CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Submission to the Senate Standing Committee on National Security and Defence regarding Bill C-59, *An Act respecting national security matters*

Canadian Civil Liberties Association
May 6, 2019

Table of contents:

Canadian Civil Liberties Association (CCLA)

The Canadian Civil Liberties Association (CCLA) is a national, non-profit, non-partisan and non-governmental organization supported by thousands of individuals and organizations from all walks of life. CCLA was constituted to promote respect for and observance of fundamental human rights and civil liberties and to defend and foster the recognition of those rights and liberties. CCLA's major objectives include the promotion and legal protection of individual freedom and dignity. For over 50 years, CCLA has worked to advance these goals, regularly appearing before legislative bodies and all levels of court.

Summary of Issues

As a defender of fundamental human rights and civil liberties, CCLA makes submissions to this Committee to express our serious concerns about several aspects of Bill C-59. While Bill C-59 makes some notable improvements to the Canadian national security landscape, it also fails to address a number of serious issues either created or exacerbated by the *Anti-terrorism Act, 2015*. Further, it introduces new provisions which may jeopardize or undermine the constitutional protections guaranteed in the *Canadian Charter of Rights and Freedoms*. CCLA made lengthy submissions on Bill C-59 to the House of Commons Standing Committee on Public Safety and National Security. Our submissions included 60 recommendations. Since we are limited to a ten page brief before this Committee, we have not exhaustively raised all of our concerns below. We have attempted to highlight in the text below our key concerns, and have included an annex with ten recommendations where we suggest language and amendments for some of the key issues we have raised. We do, however, continue to rely on the submissions and recommendations already provided to the House Committee.

1. The *National Security and Intelligence Review Agency Act*

The CCLA and others have long advocated for the creation of an integrated agency that can review the national security activities of a number of agencies and departments. The creation of the National Security and Intelligence Review Agency is a positive development and before the House Committee our recommendations sought to strengthen this agency which has a very broad mandate, including responsibilities to review a wide variety of activities and investigate complaints. We recommended that the size of the agency be increased and/or the appointments be made full-time.

We also proposed adding some detail to the legislative language describing NSIRA's activities and reporting requirements for the purposes of increased transparency. The addition of more detail in describing NSIRA's mandate seeks to ensure that the creation of a new review agency does not result in a loss of any review functions (currently carried out by SIRC, for example) and that the results of reviews are meaningfully communicated to the public to the fullest extent possible. We are also in agreement with the recommendation set out in the Annual Report of the National Security and Intelligence Committee of

Parliamentarians: that the *NSIRA Act* be amended to explicitly require an annual review of Department of Defence/Canadian Armed Forces activities related to national security or intelligence.

2. The *Intelligence Commissioner Act*

The creation of a new office known as the Intelligence Commissioner appears to be aimed at providing real-time oversight and control in relation to some of the functions of CSE and some CSIS powers that are not currently subject to oversight by the Federal Court. Independent oversight is of vital importance to ensuring that our security services act within the bounds of the law, including the *Charter*, and may help facilitate public confidence in their activities. Unfortunately, the regime established by Bill C-59 contains significant gaps that should be addressed to achieve these worthy goals.

In the proposed *CSE Act*, the Intelligence Commissioner provides an oversight function for CSE foreign intelligence and cybersecurity authorizations issued by the Minister. The government has suggested that Intelligence Commissioner approval is not required for active and defensive cyber operations authorizations because—while some *Charter* rights may be engaged by activities authorized under these provisions—the acquisition of a Canadian's or person in Canada's private information would not be authorized.[1] We reject the implicit assumption that IC approvals should only be required on the basis of concerns about individual privacy. Activities under these authorizations will be carried out in secret and may well have significant impacts on the rights and legitimate expectations of Canadians and persons in Canada; they may also have far-reaching impacts on internationally protected human rights and global security interests more broadly. Some form of independent and impartial oversight is appropriate to ensure that these powers are exercised reasonably, proportionately, and with adequate restraint, and we do not believe after-the-fact review by NSIRA is sufficient. Moreover, while independent oversight may help to provide a check on the power of these agencies that operate largely in secret, there is likely to be little impact on public confidence if the oversight process consists solely of a closed dialogue between the relevant security agency and the IC and if the outcomes of the approval process are also shrouded in secrecy. A more robust process is required to ensure that the Intelligence Commissioner hears not only from the security service seeking approval, but also from an individual or organization appointed to represent the public's interest in transparency and ensuring our national security agencies comply with the *Charter*. The Committee should consider a scheme requiring the appointment of a special advocate in relation to the IC's exercise of his/her oversight role.

3. The *Communications Security Establishment Act*

Bill C-59 creates for the first time a separate enabling statute for Canada's signals intelligence and cybersecurity agency, the Communications Security Establishment (CSE).

[1] Department of Justice, Charter Statement - Bill C-59: *An Act respecting national security matters* (Second Reading in the Senate, December 11, 2018), <http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html>.

The *CSE Act* is complex, and there is a great deal receiving public scrutiny for the first time. Here we focus briefly on three key concerns.

A) The addition of active and defensive cyber operations to the CSE's mandate

Section 15 (2) of the *CSE Act* adds two aspects to CSE's mandate, "defensive" and "active" cyber operations. The "active" cyber operations aspect of the mandate expands the scope of CSE powers to include offensive hacking and has received insufficient justification or analysis as part of this omnibus bill. It should be severed from the CSE Act and given independent consideration, not least because there could be serious repercussions for Canadians at home and abroad as a consequence of a decision to allow a Canadian agency to breach foreign or international law. **[See annex – recommendation 1]**

Active or defensive cyber operations are not to be "directed" at Canadians or persons in Canada,[2] or at any portion of the global information infrastructure in Canada,[3] and as amended, must not infringe the *Canadian Charter of Rights and Freedoms*.[4] However, there is no provision for independent review of these operations by the Intelligence Commissioner, leaving a notable accountability gap. Allowing CSE to assess their own *Charter* compliance in secret, with only a potential after-the-fact review by NSIRA, is insufficient. When we contrast this with the complex framework for prior judicial authorization and a list of prohibited activities for CSIS' threat reduction powers (although we do not concede the adequacy of that framework) it is notable that CSE's cyber operations activities involve no meaningful privacy protections, require only secret Ministerial authorization, and involve only after-the-fact review. **[See annex – recommendation 2]**

CCLA also shares the concern, expressed in detail in the December 2017 joint Citizen Lab/CIPPIC Analysis of Bill C-59, that putting the competing responsibility for defending Canada against security vulnerabilities while at the same time incentivizing the use of such vulnerabilities under an "active" mandate increases the tensions inherent to the CSE's multi-faceted mandate.[5] CSE's March 2019 release of a high-level summary of their equities management framework is a step towards transparency regarding the way such risk will be addressed but the Bill fails to provide statutory direction to assist in establishing priorities or managing risks.

B) The Overbroad Definition of Publicly Available Information

[2] Proposed (C-59) *Communications Security Establishment Act*, s. 22 (1).
[3] Proposed (C-59) *Communications Security Establishment Act*, s. 22 (2)(a).
[4] Proposed (C-59) Communications Security Establishment Act, s. 22(1).
[5] See Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson and Ronald Diebert, *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),* The Citizen Lab and the Canadian Internet Policy and Public Interest Clinic, online: https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf, at 62-68.

While the majority of CSE activities cannot be directed at Canadians or persons in Canada as per section 22(1), section 23 creates an exception for "publicly available information," defined in unacceptably broad terms, as information "published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase."[6] This permits a vast amount of information, including from within Canada, and/or created by or about Canadians or persons in Canada, to be collected in bulk. The breadth of the proposed definition can be contrasted with another law that creates exceptions for publicly available information: Canada's private sector privacy law. The *Personal Information and Protection of Electronic Documents Act* (PIPEDA) allows companies to use publicly available information without obtaining individual consent, but the relevant regulation defines publicly available information narrowly by specifying five categories of information that are public for the purposes of the Act.[7] Canada's other private sector privacy laws have similar, closed lists of information types considered public. The definition in the *CSE Act*, in contrast, would allow almost unfettered access to personal information online, a scope that has not been demonstrated to be necessary, even in submissions by the CSE on this Act, and which is clearly disproportionate to the needs which have been expressed publicly.[8]

The exclusion of information in which a person in Canada has a reasonable expectation of privacy from the definition as amended does not fully ameliorate concerns stemming from a lack of privacy protections for its acquisition or collection, particularly because the reasonableness of privacy expectations in some forms of information available on public fora remains contested, and the Intelligence Commissioner has no role in relation to publicly available information. The lack of external oversight of such collection, including CSE's (secret) assessments of when expectations are reasonable and when they are not--means that the protection provided by this provision is questionable. Post collection, privacy protections for use, analysis, retention and disclosure are similarly left to "measures" put in place by CSE which are unlikely to be subject to public scrutiny or debate.[9] The CSE should be required to publicly disclose its interpretation of what kinds of "publicly available information" attract a reasonable expectation of privacy. Further, it should be made explicit that the Privacy Commissioner of Canada has the right, as per s. 37(1) of the *Privacy Act,* to investigate to ensure compliance with sections 4-8 of that Act in relation to CSE use of publicly available personal information.

---

[6] Proposed (C-59) *Communications Security Establishment Act*, s. 2.

[7] This includes phone book information, business directory information, information in a registry collected under statutory authority, information in records of a judicial or quasi-judicial body, and information in a publication in printed or electronic form, if an individual provided it. In most cases, the overriding principle is that uses of such public information should still be consistent with the purpose for which it was collected.

[8] For example, Mr. Dominic Rochon, Deputy Chief, Policy and Communications, CSE, in response to a question from Member of Parliament Mr. Matthew Dubé, identified the need to access public information explaining "exactly how the global information infrastructure is actually set up" as a rationale for accessing publicly available information. Such information could be addressed by the ability to subscribe to public reports and academic or technical journals. Evidence, Thursday November 30, at 10:45 <http://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-88/evidence>.

[9] Proposed (C-59) *Communications Security Establishment Act*, s. 24 (b).

Finally, nothing in the definition of publicly available information precludes the acquisition of illegally obtained materials, which raises the risk of creating incentives for the acquisition and provision of questionably-obtained information, including grey and black market information from hacks and breaches, to CSE. **[See annex -recommendation 3]**

C) Gaps in CSE Oversight and Review

CCLA supports the oversight role that the Intelligence Commissioner has been positioned to play in relation to previously unexamined Ministerial authorizations. Similarly, we are encouraged that longstanding calls to provide integrated review of Canada's national security and intelligence agencies have been answered with the proposed creation of the National Security and Intelligence Review Agency. More specific public reporting requirements would similarly help to improve the transparency of CSE's activities.

4. *Canadian Security Intelligence Service Act* Amendments

A) The New Dataset Regime

The new dataset regime set out in the proposed amendments is designed in part to address the Federal Court's 2016 decision in *Re X,*[10] which determined that CSIS had been retaining certain information in the absence of a clear authority to do so, and had failed in its duty of candour to the Court in seeking approvals for certain warrants. The regime set out at proposed ss. 11.01 - 11.25 responds to the decision and takes the collection of datasets generally outside of the judicial authorization scheme. It applies to datasets that contain personal information and that *do not* directly and immediately relate to activities that represent a threat to the security of Canada. For Canadian datasets, the Minister can authorize collection of a class of datasets if the Minister concludes that querying and exploitation of *any* dataset in the class *could* lead to results that are *relevant* to the performance of the Service's intelligence, threat reduction or foreign intelligence roles. This is a low bar and does not define which datasets, if any, are clearly off the table. However, the collection of publicly available datasets and foreign datasets is not even constrained in this manner. Further, there is no meaningful definition of "publicly available dataset". It is defined in a manner that is circular and tautological. **[See annex – recommendation 4]** Finally, while there are significant record-keeping requirements in relation to all types of datasets, these requirements are carried out by CSIS and there are currently no reporting requirements regarding the rationale for collection or retention. CSIS should be required to provide this information to NSIRA and/or NSICOP.

B) Threat Reduction Powers

CCLA remains concerned about the way in which CSIS's mandate has shifted; we do not believe the case for granting threat reduction powers to CSIS has been made out by the

[10] *In the matter of an application by [redacted] for warrants pursuant to sections 12 and 21 of the Canadian Security Intelligence Act, RSC 1985, c. C-23 and in the presence of the Attorney General and Amici and in the matter of [redacted] threat-related activities*, 2016 FC 1105.

government or that it has been demonstrated why better communication and cooperation between CSIS, the RCMP, and other law enforcement bodies is incapable of achieving the same goals. If CSIS is to continue to have these powers (a point we think has not been the subject of adequate debate), the scheme can and should be improved further. In particular, changes should be made to: (1)clarify that threat reduction by CSIS is a last resort; (2) narrow the threat reduction measures available to the Service; and (3) ensure that questions of compliance with the law and the *Charter* are not left solely to CSIS. In particular, warrants should be obtained in all cases where threat reduction measures will be pursued in accordance with s. 21.1(1.1). **[See annex – recommendations 5 & 6]**

5. *Security of Canada Information Disclosure Act* Amendments (SCIDA)

The *Security of Canada Information Sharing Act* ("SCISA") was one of the most profoundly flawed sections of Bill C-51. CCLA argued at that time, and continue to argue, that it is essential that the lessons of the Air India and Arar Inquiries are acknowledged, and that Canada's information sharing/disclosure practices are guided by principles of necessity, proportionality, and accountability. The amendments made in Bill C-59 fail to fully live up to these principles, although there is progress in some respects towards this goal. CCLA's critique centres on three critical flaws, addressed below.

A) Overbroad Definition of "activity that undermines the security of Canada"

The definition of "activity the undermines the security of Canada" is excessively broad, encouraging proactive disclosure across a range of activities that go well beyond the range of threats identified in the CSIS Act as threats to Canada's national security. When a broad range of actors are asked to interpret a broad set of provisions, it is inevitable that a broad range of information about Canadians will end up being disclosed among recipient institutions--raising both privacy concerns, and also concerns that vital information will get buried.

Furthermore, the essential exception for acts of advocacy, protest, dissent or artistic expression from this definition is newly qualified in C-59 by the phrase "unless carried on in conjunction with an activity that undermines the security of Canada."[11] Given the overbroad list of such activities, this qualifying clause raises the risk that the exception can be interpreted inappropriately narrowly. We are concerned that constitutionally protected acts of advocacy, protest, dissent or artistic expression—particularly by environmental and Indigenous activists—will continue to be subject to information disclosures because some of their activities might be speculatively (and wrongly) believed to be captured. For example, despite the addition of the (undefined) qualifiers "significant or widespread" to paragraph 2(f), which addresses interference with "critical infrastructure," it remains unclear whether a non-violent, long-term occupation of a resource extraction site might be considered significant. Might a protest in front of a foreign embassy be "conduct that takes place in Canada and that undermines the security of another state"? How about a civil society letter writing campaign criticizing, for example, foreign legislation mandating

[11] Proposed (Bill C-59) *Security of Canada Information Disclosure Act*, s. 2(2).

encryption backdoors for national security agencies? Limiting the exception for legitimate acts of dissent or expression in this manner makes the exception subject to interpretation and renders it difficult for members of the public to predict its effects in relation to their constitutionally protected rights.

While some commentators, including the influential Professors Roach and Forcese, expressed an opinion that violent forms of protest or dissent should be excluded from an exception for these activities, their explicit concern was with protest activities "intended to cause death or bodily harm, endanger life, or cause serious risk to health."[12] Any exception to the exemption from information sharing for protest and related activities should only be in cases where there is substantiated reason to believe such serious harms are likely. **[See annex – recommendation 7]**

B) Insufficiently High Thresholds for Disclosure and Retention

SCISA was soundly criticized for failing to set sufficiently high thresholds for information sharing; the standard in section 5(1) of *SCISA* required only that information be "relevant to the recipient institution's jurisdiction or responsibilities." *SCIDA* has altered this threshold but it remains short of what CCLA believes is the appropriate standard for disclosing and recipient institutions, which is that information should be *necessary* for the exercise of the recipient's jurisdiction in respect of activities that undermine the security of Canada. Tightening this threshold is made all the more important by the exceptional breadth of activities captured by the definition of activities that undermine the security of Canada, as discussed above. Privacy rights are not the only rights at stake if thresholds are permissive. Equality rights, in particular, those related to discrimination or bias against particular religious, ethnic, or racial groups, are also at risk when there is broad scope to make choices about who might be a threat. We do appreciate that in the Bill as amended, under s. 5.1(1) recipient institutions are required to return or destroy *personal* information disclosed to them that is not necessary but the necessity threshold that triggers return or destruction for recipient institutions should cover all information, not just personal information.

C) Accountability Measures Must be Stronger

Sections 9 and 10 of the *SCIDA* add record keeping requirements to the legislation for the disclosing and, as amended, receiving institution, and provide for NSIRA to receive copies of those records. This goes some way to address recommendations CCLA made regarding *SCISA* and the initial version of *SCIDA*. Recipient institutions, however, should have a requirement, parallel to that of disclosing institutions, to describe the information they relied upon to satisfy themselves that the information they have received and retained, personal or non-personal, is necessary for the exercise of its jurisdiction in respect of activities that undermine the security of Canada.

[12] Craig Forcese and Kent Roach, Analysis and Proposals on the S*ecurity of Canada Information Sharing Act* (3 November 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2863364> at 4.

While CCLA believes the mandate of the Privacy Commissioner of Canada does, and should, allow him to investigate disclosures under *SCIDA*, and indeed, he has done so for *SCISA*,[13] we would like to see explicit provision for the Privacy Commissioner of Canada to also receive records created under section 9 of *SCIDA*.

6. *Secure Air Travel Act* Amendments

While Bill C-59 makes a number of positive changes to the *Secure Air Travel Act* which may better protect children placed on the list, and which may help to reduce the number of "false positives," these fixes are ultimately minor in comparison to larger problems raised by the no-fly list. We support the bill's reversal of the rule for applications for administrative recourse, so that the Minister is no longer deemed to have decided against removal of a name from the list in situations where the Minister does not have sufficient information to make a decision, or simply fails to make a decision for other reasons.[14] However, the standard for adding an individual's name to the list—"reasonable grounds to suspect"[15]—remains low given that listing may result in a severe restriction of the mobility rights guaranteed under section 6 of the *Charter of Rights and Freedoms*. Further, the Minister's ability to delegate her or his authority to limit these rights is far too broad.

A) Dangerous lack of Due Process in the Appeal Framework

The *Secure Air Travel Act*'s remedial mechanisms remain similarly defective. Even if denied travel, individuals may never be explicitly informed that they are a listed person, which can frustrate their ability to seek recourse within the narrow window available to do so.[16] This is because the 60-day period begins on the day on which they were denied transportation, rather than the day on which they became aware of their status on the list.[17] There are also more fundamental problems with the appeal mechanism, which replicates many of the same issues present in the security certificate context prior to 2008.[18] Proceedings may take place in secret,[19] appellants are only provided a discretionary summary of the intelligence and evidence used against them[20] (which may include hearsay[21]), and the judge is empowered to rely on evidence and information which has not been provided in that summary.[22] The appellant's right to be heard is not meaningful if she or he does not

[13] Office of the Privacy Commissioner of Canada, 2015-2016 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*, September 2016, at 16-21, online: https://www.priv.gc.ca/media/4516/ar_201516_eng.pdf.
[14] Proposed (Bill C-59) *Secure Air Travel Act,* s. 15(6).
[15] Proposed (Bill C-59) *Secure Air Travel Act,* s. 8(1).
[16] The 60-day window is subject to the Minister's discretion to extend based on "exceptional circumstances that warrant it," see *Secure Air Travel Act,* s. 15(2).
[17] *Secure Air Travel Act,* s. 15(1).
[18] See *Charkaoui v Canada (Minister of Citizenship and Immigration)*, 2007 SCC 9 [*Charkaoui I*].
[19] *Secure Air Travel Act,* s. 16(6)(a).
[20] *Secure Air Travel Act,* s. 16(6)(c).
[21] *Secure Air Travel Act,* s. 16(6)(e).
[22] *Secure Air Travel Act,* s. 16(6)(f).

know the case to meet.[23] Moreover, the appellant is not afforded a special advocate with the ability to review and test the government's case. In addition to the clear issues with regard to due process and fundamental justice, these provisions also erode the separation of functions between judge and counsel in an adversarial system. **[See annex – recommendation 8]**

While being placed on the no-fly list undoubtedly comes with a different set of consequences than being named in a security certificate, both have the ability to substantially interfere with the constitutionally protected rights and liberties of an individual, including those protected under sections 6 and 7 of the *Charter of Rights and Freedoms* in a manner that cannot be saved by section 1. A no-fly list designation can also result in very serious practical costs to an individual's relationships and family life, compromise their employment, limit the professional opportunities available to them, and damage their reputation and community standing. The SECU Committee of Parliament previously recognized these profound issues in May 2017 when it recommended the use of special advocates in no-fly list proceedings, among other safeguards—and yet Bill C-59 does not address these concerns. It should do so by ensuring full disclosure of all information in the government's possession which is relevant to the listed individual's case, including exculpatory evidence, and by creating a mechanism for the appointment of a special advocate to protect the interests of the person who has appealed to have their name removed from the Specified Persons List, with the same powers and responsibilities to test and challenge that evidence as special advocates in the security certificate context.[24] **[See annex – recommendation 9]**

Finally, section 16(5) of the Act is drafted so that, after having found the decision to list an individual under section 15 unreasonable, the judge "may order that the appellant's name be removed from the list." This unusual discretionary power should be removed.

7. *Criminal Code* Amendments

The proposed amendments to the *Criminal Code* in Bill C-59 give rise to a number of civil liberties concerns related to: the terrorist entities list; the "terrorist speech" offence; the definition, seizure and deletion of "terrorist propaganda;" investigative hearings; warrantless arrest and recognizance with conditions; and terrorism peace bonds. These were canvassed extensively in our submissions to the House Committee and we make only a few brief comments here.

With respect to the proposed changes to the terrorist entities list, we note that the process for judicial review in the context of listed entities replicates many of the due process and procedural fairness concerns associated with the no-fly list, the pre-2008 security certificate regime, and the security certificate process following the changes made in the -

[23] See *Charkaoui I* supra note 18, e.g., at paras 29, 53; *Singh v. Minister of Employment and Immigration*, [1985] 1 S.C.R. 177 at p. 213; *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1 at para 123.
[24] See also House of Commons, Standing Committee on Public Safety and National Security. *Protecting Canadians and their Rights: A New Road Map for Canada's National Security*. 42nd Parliament, 1st Session (May 2017) at Recommendation 37.

Anti-terrorism Act 2015. The Minister has extraordinary discretion to withhold evidence and information from the judge, the applicant and the applicant's counsel. At a minimum, these proceedings should require the appointment of a special advocate with the ability to review and test all relevant evidence.

We continue to have concerns about the terrorist speech and terrorist propaganda provisions. The provisions regarding the seizure and deletion of "terrorist propaganda" allow the government to censor and de-anonymize expressive content, and thus should be accompanied by robust reporting and accountability requirements. **[See annex – recommendation 10]**

8. Need to Amend the *Immigration and Refugee Protection Act*

In the *Anti-terrorism Act, 2015*, the former government introduced a series of changes to the *Immigration and Refugee Protection Act* which removed important protections for named persons in security certificate proceedings. Those protections were adopted in 2008 following the Supreme Court's 2007 ruling in *Charkaoui v. Canada (Citizenship and Immigration)*,.[25] wherein the Court affirmed that the individual named in a security certificate "must be given an opportunity to know the case to meet, and an opportunity to meet the case," an impossible exercise in the absence of a coherent framework for the disclosure of relevant evidence. Yet as of 2015, sections 83(1) and 85.4(1) of the *Immigration and Refugee Protection Act* have allowed the Minister to withhold information from a special advocate appointed to protect the interests of the person named in a security certificate, including information relevant to the government's case against the named person. These provisions are at odds with the Supreme Court of Canada's ruling in *Charkaoui I, Charkaoui II,*[26] and *Canada (Citizenship and Immigration) v. Harkat.*[27] The 2015 changes also gave rise to a number of other defects of due process and procedural fairness, affording the Minister virtually unfettered interim rights of appeal regarding orders made for disclosure of information.

The preservation of Canada's national security interests is of critical importance. At the same time, the *Charter's* guarantee of a fair hearing and due process before an independent and impartial tribunal is a non-negotiable condition of a free and democratic society. The delicate balance struck by the courts to protect those rights prior to the *Anti-terrorism Act, 2015* should be restored. In our constitutional challenge and elsewhere, CCLA has argued that the *Anti-terrorism Act, 2015* amendments to the *IRPA* are an unconstitutional violation of the section 7 guarantee to a fair hearing before an independent and impartial tribunal. The security certificate regime has already been the subject of significant litigation, and this committee now has the opportunity to repeal those provisions as part of Bill C-59.

---

[25] *Charkaoui I* supra note 18, at para. 69 et seq.
[26] *Charkaoui I* supra note 18; *Charkaoui v. Canada (Citizenship and Immigration)* [*Charkaoui*, 2008 SCC 38; see also *Almrei (Re)*, 2009 FC 240 at para 43: "Such disclosure, it is to be remembered, consists of disclosure to the designated judge and the special advocate of all of the information in the possession of the Service concerning the named person."
[27] *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37.

Annex – Recommendations

1. Do not adopt the provisions in the *CSE Act* related to active cyber operations, and refer the issue for further study to evaluate the necessity and proportionality of these powers.

2. Amend the *CSE Act* and the *Intelligence Commissioner Act* to require Intelligence Commissioner approval of active (if active operations are maintained in the Bill) and defensive cyber operation authorizations granted by the Minister pursuant to sections 30 and 31 of the *CSE Act*.

3. Amend the definition of "publicly available information" in section 2 of the *CSE Act* to:
    a) specify that it only includes information that has been published or broadcast for public consumption without restriction;
    b) limit the ability to purchase or subscribe to information from the definition, to specify that information for which remuneration is provided must be legally available to the general public, and have been legally obtained or created by the vendor (i.e. limit the purchase of information to "commercially available publications and broadcasts").

4. Amend section 11.01 and paragraph 11.07(1)(a) of the *CSIS Act* such that "publicly available dataset" is clearly and narrowly defined to cover statistics and data readily available from a source without payment, explicitly exclude any data in which an individual may have a reasonable expectation of privacy, and require CSIS to disclose its determination of which publicly available datasets do not give rise to a reasonable expectation of privacy.

5. The committee should carefully scrutinize the measures set out in subsection 21.1(1.1) of the *CSIS Act* to determine if any of them can be narrowed or refined. For example, paragraph (g) allows CSIS to personate a person, other than a police officer, in order to take a measure referred to in any of paragraphs (a) to (f). At a minimum, CSIS should also be prohibited from personating a lawyer, a judge, a religious official, or a member of the press.

6. Amend the warrant scheme in the *CSIS Act* to require a warrant in *any* case where the measures set out in proposed s. 21.1(1.1) will be pursued by CSIS, regardless of CSIS's opinion on whether the measures would violate the law or *Charter.*

7. Amend section 2(2) of *SCIDA* to read, "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 <u>intended to cause death or bodily harm, endanger life, or cause serious risk to health or public safety</u>."

8. Amend the *Secure Air Travel Act* to create a system for prompt and effective notice to individuals who have been denied air travel that they are, or are not, on the Canadian

Specified Persons List, and that they do, or do not, share a name with an individual on the Canadian list. In the alternative, amend the *Secure Air Travel Act* to allow an individual who has been denied air travel to confirm the above with the Passenger Protect Inquiries Office, and amend subsection 15(1) such that the 60-day window only begins on the date the individual is made aware of their placement on the list.

9. Replace the appeals mechanism in section 16 of the *Secure Air Travel Act* with a system that:
   a) ensures full disclosure of all information in the government's possession which is relevant to the listed individual's case, including exculpatory information; and
   b) creates a mechanism for the appointment of a special advocate to protect the interests of the person who has appealed to have their name removed from the Specified Persons List, with the same powers and responsibilities to test and challenge that evidence as special advocates in the security certificate context.

10. Introduce a requirement for the Attorney General of Canada to prepare a report to Parliament and to the public on the operations of sections 83.222 and 83.223 of the *Criminal Code* on an annual basis that includes:
    a) The number of applications sought for the seizure of "terrorist propaganda," and the number obtained, by virtue of section 83.222;
    b) The number of applications sought to order a custodian of a computer system, and the number obtained, by virtue of section 83.223. The report should be separated by type of order, whether production (s. 83.223(1)(a)), removal (s. 83.223(1)(b)) or identification (s. 83.223(1)(c)) respectively. It should also include the number of individuals implicated in identification orders and the number of instances of terrorist propaganda removed (assuming one order may comprise multiple instances of offending content).
    c) The number of orders for deletion of "terrorist propaganda or computer data that makes terrorist propaganda available" made under subsection 83.223(5);
    d) The number of orders to delete "terrorist propaganda or computer data that makes terrorist propaganda available" in the court's possession by virtue of subsection 83.223(6), if that subsection is not repealed;
    e) A general description of each instance of "terrorist propaganda" subject to the aforementioned orders in the preceding year.