Brief on Bill C-70
The Countering Foreign Interference Act

Submitted to the
Senate Standing Committee on
National Security, Defence and Veterans Affairs

by the
International Civil Liberties Monitoring Group

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298

The International Civil Liberties Monitoring Group, a Canadian coalition of 46 civil society organizations that works to defend civil liberties and human rights in the context of national security and anti-terrorism activities.

1. Introduction

Bill C-70 has been presented as legislation to address threats of foreign interference. We recognize the importance of addressing this issue, particularly in instances where governments are threatening individuals or their close ones in order to repress their ability to exercise their fundamental rights or engage in democratic processes.

However, the changes proposed by this legislation go much further. If adopted, this bill will have wide-ranging impacts on Canada's national security, intelligence and criminal justice systems. As such, it will also have significant impacts on the lives and fundamental rights of people in Canada.

For example, providing CSIS with new forms of warrants, granting it extra-territorial reach for foreign intelligence activities, and allowing the service to disclose information to any person or entity, in order to build "resiliency," would lead to increased surveillance, diminished privacy, and racial, religious and political profiling. Powerful new offences for actions taken secretly at the behest of foreign entities, including foreign governments and terrorist organizations, punishable by up to life in prison, could infringe on freedom of expression and association, and raises questions of proportionality in sentencing. The bill would transform how federal courts handle sensitive information that can be withheld from appellants or those seeking judicial review, undermining due process in courts through the use of secret evidence.

Concerns with an expedited study

A bill of such breadth requires in-depth study. Which is why we are deeply concerned with the hastiness with which this legislation is being considered. Introduced barely a month ago, with the Foreign Interference Inquiry ongoing, it will have gone through committee study in both chambers of Parliament in approximately two weeks. This is faster than even the rushed 2001 study of the first *Anti-terrorism Act*, which studied for two months.

This expedited study means that experts and organizations with limited resources have had to rush their analysis of the bill, and has made submitting briefs and appropriate amendments nearly impossible. While we are please to be submitting this brief, and stand behiond our concerns, much of what we are recommend are preliminary suggestions that would have benefited from great time for discussion and elaboration.

Rushing the parliamentary process, supported by a state of suspicion and ardent calls to protect national security, can lead to serious, negative and long-lasting consequences. An expedited study also risks missing ways the bill could be improved to better address issues of foreign interference.

We therefore urge the committee to work with your fellow Senators to extend your study of Bill C-70 in order to hear more input and analysis and to provide the opportunity to develop, propose and debate amendments.

> **Recommendation 1:** That the SECD Committee work with colleagues in the House of Commons to extend its study of Bill C-70.

Apart from the process of this study, we have specific areas of concerns.

2. Changes to the CSIS Act

A. Dataset regime

Modifications to CSIS' dataset regime are only tangentially related to foreign interference. Many of these changes relate to significant problems the National Security and Intelligence Review Agency identified in a scathing report on the regime.[1] The necessity and potential consequences of these changes remain unclear, and should have been addressed during a statutory review of 2019's *National Security Act*. The modifications to the CSIS dataset regime should be removed until such a review happens.

Also of specific concern are proposed new rules to allow for the disclosure of datasets. The bill would establish three different thresholds for the disclosure of the three kinds of datasets:

- Publicly available datasets could be disclosed without any restriction whatsoever
- Foreign datasets could be disclosed based on terms and conditions set out by ministerial authorization
- Canadian datasets could be disclosed based on terms and conditions set out by judicial authorization

[1] See: https://globalnews.ca/news/10390622/spy-agency-big-data-law/ and https://nsira-ossnr.gc.ca/en/reviews/ongoing-and-completed-reviews/completed-reviews/nsira-review-of-csis-dataset-regime

Datasets can contain troves of data. Establishing protocols for share entire datasets, even based on conditions set out by judicial authorization, raises serious concerns about the sharing of bulk data between CSIS and not just other government departments, but with private and/or foreign entities. It is also not guaranteed that the terms and conditions set for Foreign or Canadian datasets would require specific approval each time they are shared, and could instead establish general conditions for disclosure without any further oversight. This is worsened for publicly available datasets, where no authorization is required whatsoever.

Instead, disclosure of datasets should be greatly restricted, with provisions for, at a minimum, authorization by the Intelligence Commissioner for each specific instance of sharing, record keeping, and reporting to the National Security and Intelligence Review Agency.

> **Recommendation 2:** The modifications to the CSIS dataset regime should be removed until a thorough review of the regime is completed as part of the statutory review of the *National Security Act, 2017*.

> **Recommendation 3:** The committee should implement strict safeguards around the disclosure of datasets, ensuring appropriate authorization for any instance of disclosure. For example, authorization of each instance of disclosure by the Intelligence Commissioner, based on criteria established by judicial or ministerial authorization (as the case may be), along with detailed record-keeping and reporting to the National Security and Intelligence Review Agency.

B. Disclosure of information:

Changes proposed in Bill C-70 to disclosure powers in s. 19 of the CSIS Act also raise significant concerns. While we understand the goal of ensuring appropriate information can be shared, there are several grounds that give rise to concerns about whether the envisioned changes are appropriate.

Journalists and NSIRA have raised serious questions about how CSIS has handled the disclosure of sensitive information in the past. This includes, for example, participating in private information sharing sessions with natural resource companies which framed Indigenous land defenders as "extremists" and prioritized economic interests over Indigenous rights, as well as Charter protected rights of free expression. In another example, NSIRA found that when disclosing information under its threat reduction powers, CSIS failed to account for ways in which third parties could take actions that violate the rights of individuals. This is particularly important, as the changes proposes in subsections 34(2) and 34(3) would grant CSIS the ability to share information with a significantly broader array of entities and individuals.

In addition to these concerns, there is also the challenge of ensuring that information shared in secret is accurate. There have been multiple instances in the past of CSIS sharing either inaccurate or unsubstantiated information, resulting in harm to individuals' rights. During the federal inquiry into foreign interference itself, it was revealed that CSIS at times was required to revisit and recall intelligence reports. While this cannot be completely avoided, it raises questions of whether intelligence shared with a broader audience that is found later to be inaccurate may have already caused irreparable harm.

This potential for harm and the need for accountability and record-keeping around information sharing is reflected in the important rules around record-keeping, reporting and destruction of information inappropriately shared contained in the *Security of Canada Information Disclosure Act.*

We would recommend several amendments:

> **Recommendation 4:** Remove s. 34(2) of Bill C-70, which would amend s. 19(2)(d) to allow the Minister to authorize disclosure to any person or entity. This is much too broad. Alternatively, any authorized disclosure should be limited to entities or persons within Canada. A further protection would be to allow sharing with a closed list of types of entities established by regulation (again, restricted to people and entities within Canada).
>
> **Recommendation 5:** Revisit s. 34(3) of C-70, which would allow for information, excluding personal information, to be disclosed by CSIS to any person or entity for the purpose of building resiliency against threats to the security of Canada.

- Resiliency should be defined in the legislation
- The government should consider creating a separate office, apart from CSIS, to organize and arrange briefings with non-governmental entities to avoid a bias towards securitization and to ensure a holistic approach to protecting against interference with the exercising of fundamental rights or participating in democratic processes
- Add transparency and accountability requirements for CSIS, including, for example:
  - Public sharing of documents and information disclosed, where possible

- Internal documenting of what information was disclosed to whom and why
- Reporting all instances of information disclosure to the NSIRA, similar to the existing requirement in s. 19(3) of the CSIS Act, regarding reporting of information disclosed with Ministerial authorization.

C. Warrant and production order powers

Bill C-70 also grants CSIS significant new production order and warrant powers. It comes after years of courts admonishing CSIS for misleading them in their warrant applications. Warrant requirements exist to protect our rights - they shouldn't be lessened; and especially not while CSIS' problem of breaches of duty of candor to the courts has not been resolved.

> **Recommendation 6:** That new production order and warrant powers be suspended until there is independent reporting that CSIS has addressed concerns around breaching of duty of candour towards the courts.
>
> **Recommendation 7:** That the newly proposed s. 20.4(5) of the CSIS Act (in clause 37 of Bill C-70) include more specific parameters to restrict the reasons a judge may order the non-disclosure of productions orders, including timeframes for automatic disclosure.
>
> **Recommendation 8:** That the newly proposed s. 20.6(1) of the CSIS Act (in clause 37 of Bill C-70) be amended to require CSIS to document and report any requests for a person or entity to voluntarily preserve or produce any information, record, document or thing.
>
> **Recommendation 9:** That the newly proposed s. 22.21(2) of the CSIS Act (in clause 39 of Bill C-70) be amended to add after (a):
>
> > (a1) why other investigative procedures would be unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (a) would not be obtained;

3. Security of Information Act:

Bill C-70 also changes the *Security of Information Act*, including a new indictable offense for the carrying out of *any* indictable offense - including relatively minor transgressions - if done for the benefit of a foreign entity. This, along with other new or modified offenses, would be punishable by either life in prison, or consecutive sentences that could amount to life in prison, provisions that are normally reserved for the worst forms of crimes and raise concerns of proportionality in sentencing.

> **Recommendation 10:** Remove "intimidation" throughout clause 53 of Bill C-70; alternatively, clause 53 should be amended to include a specific definition of "intimidation."
>
> **Recommendation 11:** Remove the undefined criteria of "association" with a foreign entity throughout clause 53 of Bill C-70.
>
> **Recommendation 12:** Proposed s. 20(3), 20.1(3), 20.2(1), 20.3(2) and 20.4(2) of the SOIA (in clause 53 of Bill C-70) should be amended to either provide incremental sentencing provisions, or to impose a sentence equal to the maximum of the underlying offense, as opposed to simply "liable to imprisonment for life."
>
> **Recommendation 13:** Proposed s. 20(4). 20.1(4), 20.2(2), 20.3(3) and 20.4(3) should be amended to read:
>
> > (4) A sentence, other than one of life imprisonment, imposed on a person for an offence under subsection (1) ~~is to~~ may be served consecutively to…
>
> **Recommendation 14:** Proposed s. 20.2, which would make it that, "Every person who commits an indictable offence under this or any other Act of Parliament at the direction of, for the benefit of or in association with, a foreign entity is guilty of an indictable offence" should be revisited, as it creates a doubling of offenses. Instead, this should be considered as a sentencing provision by the presiding judge.
>
> **Recommendation 15:** Proposed s. 20.3 should be amended as follows:
>
> > 20.3 (1) Every person commits an indictable offence who, at the direction of, for the benefit of ~~or in association with,~~ a foreign entity, knowingly engages in surreptitious or deceptive conduct or omits, surreptitiously or

> with the intent to deceive, to do anything if the person's conduct or omission is for a purpose prejudicial to the safety ~~or interests of the State~~ of Canadians or people in Canada ~~or the person is reckless as to whether their conduct or omission is likely to harm Canadian interests.~~

Proposed s. 20.4 - *Influencing political or governmental process* – should be revisited to include more specific definitions and introduce safeguards against infringing on participation in the democratic process.

This section is particularly problematic, given the ease with which unsupported or baseless accusations are made that protest movements, that seek to influence public policy, are influenced or acting at the behest of foreign actors. This includes, for example, on campus protests in support of Palestinian rights, that could be viewed as disrupting or influencing educational governance.

> **Recommendation 16:** Amend s. 20.4 - *Influencing political or governmental process* – to include more specific definitions and introduce safeguards against infringing on participation in the democratic process.
>
> **Recommendation 17:** The term "in association with" in 20.4(1) should be removed.
>
> **Recommendation 18:** Offences should be tied not just to influence but to demonstrable harm.
>
> **Recommendation 19:** The definition of "educational governance" in s. 20.4(4) must be clarified, or should be removed.

4. Canada Evidence Act

We have significant concerns regarding changes to the Canada Evidence Act contained in Bill C-70. Our coalition is fundamentally opposed to expanding the use of secret evidence in Canada's courts under the guise of protecting national security, national defense and international affairs. Introducing a standardized system for withholding information from those challenging government decisions that have significant impacts on their lives will normalize this process and is likely to facilitate the spread of the use of secret information further into our justice system.

As we have previously explained:

> The use of secret intelligence in diverse proceedings before tribunals and courts has been criticized, as Canada and other states – likely in consultation with each other – appear to be normalizing what was meant to be an exceptional procedure, expanding its use in other areas, including in criminal trials. While it is perhaps trite to reference the 'slippery slope,' there are real dangers. Canada is not at war; there is no national emergency. The normalization of secrecy as part of the decision making process, in addition to the human rights issues raised, undermines democratic principles and public confidence, not just in the government, but in the judiciary itself. Secrecy feeds the perception that the government is seeking to immunize itself from public censure for the wrongdoing of its officials and to shield from scrutiny information obtained from questionable sources. It contributes to the politicization of intelligence. Regardless of the merit of a decision that a refugee is involved in terrorism, non-disclosure of the underlying evidence undermines confidence in the result, and gives rise to the perception that the person has been wrongfully sanctioned – especially where the evidence could have been challenged if it had been disclosed. The end result may well be the alienation of entire communities whose cooperation is critical to the fight against terrorism."[2]

While the context of this was the challenge to security certificate regimes in the *Harkat* case, "terrorism" could easily be substituted with "foreign interference" and the arguments would remain salient.

As we also argued, there are inherent defects in these secret processes that serve to undermine the fundamental principles of justice, including:

- The difficulty of defining the amorphous and elastic concept of national security, which is nevertheless necessary in order to ensure that the grounds for non-disclosure can be limited and consistently applied;
- Constant pressure on state officials to over-claim on national security grounds as a matter of prudence or because of a perceived need to protect officials from public criticism, and on the Court or tribunal to over-redact as a matter of caution;
- The existence and development of a closed body of jurisprudence available only to the court and the Minister, but not to the special advocates or to public counsel;

[2] CCR & ICLMG MEMORANDUM OF ARGUMENT, Canada (Citizenship and Immigration) v. Harkat, 2014 SCC 37, [2014] 2 S.C.R. 33. Online: https://www.scc-csc.ca/WebDocuments-DocumentsWeb/34884/FM080_Intervener_Canadian-Council-for-Refugees-etal.pdf

- The absence of an "effective means of keeping this process under independent scrutiny and review" by "legal practitioners, the media and other civil society organizations which seek to hold executive government and its agencies accountable and answerable for their actions."[3]

We therefore oppose the creation of a standardized Secure Administrative Review Proceeding, as it would serve to further normalize secret proceedings. Once an "acceptable" template has been established, it can be more easily tacked on and presented as uncontroversial – when such proceedings should always be viewed as controversial and exceptional.

Instead, the government should review the areas of legislation that already allow for similar regimes to remove provisions for the non-disclosure of information to appellants and those seeking judicial review.

> **Recommendation 19:** Remove provisions for a new Secure Administrative Review Proceeding and instead review the areas of legislation that already allow for similar regimes, in order to remove provisions for the non-disclosure of information to appellants and those seeking judicial review.

Finally, we are opposed to the proposal in Bill C-70 to add "international affairs and national defence" to the grounds on which the minister may oppose disclosure of information, or on which a judge may decide against disclosure of information, in the security certificate provisions of the *Immigration and Refugee Protection Act*. This should be removed from the bill. Instead, consideration should be given to removing the entirety of the security certificate regime.

> **Recommendation 20:** Remove all provisions in Bill C-70 to add "international affairs and national defence" to grounds for barring disclosure of information in *IRPA*.

5. Sabotage and the Foreign Influence Transparency Registry Act

We also have concerns about new sabotage offenses and the proposed foreign influence registry, but defer to concerns shared by the Canadian Civil Liberties Association among others.[4]

---

[3] Ibid.
[4] See: https://www.ourcommons.ca/Content/Committee/441/SECU/Brief/BR13166758/br-external/CanadianCivilLibertiesAssociation-REV-67-240606-006-e.pdf

However, we would note our specific concern around the amendment passed by the House of Commons to extend the sabotage provisions to include essential infrastructure "under construction" and "is intended to provide or distribute" services that are essential to people in Canada.[5] To include infrastructure that has not been completed and whose essential nature is only speculative, only serves to exacerbate the problems identified in the original proposal.

> **Recommendation 21:** Rescind the amendment to Clause 61 of Bill C-70 adopted by the House of Commons.

[5] See: https://www.ourcommons.ca/documentviewer/en/44-1/SECU/report-13