INTERNATIONAL
CIVIL LIBERTIES
MONITORING
GROUP

Submission to the federal government's consultation on its proposed approach to address harmful content online

International Civil Liberties Monitoring Group

25 September 2021

The International Civil Liberties Monitoring Group is a coalition of 45 civil society organizations from a range of backgrounds and sectors from across Canada, including leading faith-based, labour, human rights, refugee and migrant, and environmental groups. Established in 2002, our mandate is to ensure the protection of civil liberties in Canada in the context of anti-terrorism and national security laws and activities.

Over the past two decades, we have participated in various government consultations and parliamentary hearings, intervened in court cases, issued multiple reports and engaged in popular education related to anti-terrorism legislation and national security activities. Throughout, we have documented how many of Canada's anti-terrorism laws have inflicted deep damage on fundamental freedoms, including freedom of expression, assembly and movement, privacy rights, due process, and equality rights (arising from racial and political profiling). Much of this is related to issues around government surveillance and profiling, information sharing between agencies (domestic and international), the use of secret hearings and secret evidence, the development of secret lists and legal regimes, lack of rigorous review and transparency, complicity in rights abuses such as indefinite detention and torture, and the overall expansion and "mission creep" of national security and anti-terrorism laws leading to ever-growing powers and a heavy reliance on security as a solution to social problems.

Our interest in the consultation regarding the government's proposal to address online harms lies in several areas. As a coalition whose mandate is to protect civil liberties, we also recognize the need to address real threats of violence and believe it is important and urgent that action is taken to address hate-based violence, and support government efforts to do so. It is clear that in supporting various freedoms, including freedom of expression, it is not enough to simply protect against censorship, but to also address actions and environments that make it impossible for individuals and communities to fully exercise their rights. We hope that our submission helps to strengthen and support that crucial policy goal.

However, we see several worrisome and even troubling aspects to this current proposal that may in fact undermine the stated goals. These include:

- the further expansion of problematic definitions of terrorism and enforcement online, which have been shown to more often target the many of very communities which the government proposes to support with this new regime.
- a questionable conflation of efforts to address wildly different harms which need very specific solutions
- a monitoring and removal process that threatens freedom of expression and privacy rights, and which will likely have severe and significant impacts on already marginalized communities
- new obligatory reporting rules to law enforcement and intelligence agencies
- new warrant powers for CSIS
- transparency and accountability requirements that require the addition of more robust policies

In analyzing this proposal, our focus will be primarily on the interaction with anti-terrorism laws, policies and activities, as well as how they overlap and raise concerns for other areas. However, we recognize that the concerns we raise may not be applicable to all forms of "online harm" –

although concerns about impacts on civil liberties and procedural fairness would likely apply in a general way to other areas as well.

A. Concerns about the consultation itself

The proposal is meant to address five areas of harmful content:

- Child sexual exploitation content
- The non-consensual sharing of intimate images
- Content which incites violence
- Hateful content
- Terrorism content

In the discussion guide and other public statements, the government has emphasized the consultation process leading up to this proposal. However, in our discussion with other civil society stakeholders, including those who have been consulted on other aspects of the proposal as well as ICLMG coalition members, none reported being engaged in regards to the "terrorism content" aspects of the proposed legislation.

Further, as has been raised by others, the timing of the consultation has also rendered full participation difficult. While the government announced the consultation on July 29th, with a deadline of Sept. 25th, the election call resulted in the cancellation of all in-person/virtual stakeholder meetings, making it impossible to ask questions or clarify aspects of the proposal. This would have greatly benefited in helping to ensure that submissions are as accurate and constructive as possible.

The fact the consultation was held during an election also meant that resources and capacity to participate were limited. This includes that, given the issue was associated directly with party platforms and promises, any substantial public engagement during the election period would have triggered the need to register as a third-party to the election and all the regulations it entails.

We are also concerned by the lack of supporting material explaining the necessity to implement a new regime targeting terrorism content online. We support the need to regulate online content which incites violence, including content linked to terrorism. However, there are already multiple international efforts to do so that focus on the obligations of platforms overall. It is unclear from the consultation documents what the scope of the problem is in Canada, whether or not other efforts are succeeding or failing, and what would be judged a successful outcome of the new regime. These are issues which may have become clear if the consultation process had not been limited due to the elections; either way, the online materials would have benefited from such materials.

This is why we have joined with others in asking that the government extend the consultation process and delay tabling this proposal as a bill in Parliament until after this consultation process has concluded.

B. Inclusion and impact of “terrorism content”

Conflation of issues

We share the concerns raised by others that attempts to regulate multiple forms of harm under one overarching regime raises questions of effectiveness and appropriateness.[1] As we will discuss later, there is a lack of detail in regard to how the regime may be adapted to address the various types of harms. While we recognize that there are policy rationales for including various harms under one regime, it gives rise to various concerns.

First, it pre-supposes that a common approach on unrelated harms will effectively address each harm. As others have also argued, we believe that a more specific approach is necessary in order to adequately address each harm. By including these five harms together in one proposal, it is difficult to ensure that each area is dealt with appropriately. What is effective for one area may be unnecessary, or even detrimental, to another.

Second, we are concerned by the potential for “policy laundering,” that is, using one policy goal in order to substantiate another, unrelated goal. By including new powers to monitor and report terrorism-related content in a proposal that also includes addressing child sexual exploitation content and the non-consensual sharing of intimate images, for example, renders it more difficult to question aspects of the bill because to do so would weaken regulation in other areas. We have seen this before in regard to proposals regarding lawful access and encryption, for example. It is essential that, when addressing such important and sensitive policy areas, that we are able to address them one by one. This proposal renders this kind of nuanced discussion difficult, if not impossible, and raises the possibility that tools that would not be acceptable if the proposal was related to terrorism alone will be more easily adopted. This issue could perhaps have been resolved with a more in-depth consultation process, but would have been better resolved by crafting a proposal that addressed the nuances of each harm separately.

Definition of “terrorist content”

As mentioned above, we recognize the need to regulate content that incites violence, including content related to terrorism, in order to avoid real-world harms.

However, such efforts must be targeted, clearly defined and demonstrate necessity and proportionality. Research, including our own, has demonstrated that terrorism is an incredibly difficult term to define.

The definition itself of “terrorism” is subject to controversy. It is almost impossible to reach consensus on it precisely because to say that some crimes are terrorist acts and some not is to make a judgment about the motive behind a crime. And that judgment will necessarily depend on the social, racial, religious, political or historical perspective of the people making the judgment. Using motive in this manner, as an essential element in defining and identifying a

[1] See, https://internetsociety.ca/submission-to-the-department-of-canadian-heritage-consultation-on-internet-harms/; https://ablawg.ca/2021/09/13/the-federal-governments-proposal-to-address-online-harms-explanation-and-critique/; https://www.michaelgeist.ca/2021/08/law-bytes-podcast-episode-99/

crime, is foreign to criminal law, humanitarian law, and the law regarding crimes against humanity. While a hate motive may be an aggravating factor at sentencing in the traditional criminal law, motive neither establishes nor excuses a crime.[2]

It is, therefore, never possible to create a definition of "terrorism" that is not either over-inclusive or under-inclusive. It can be over-inclusive in that it captures ordinary crimes, civil disobedience, or the justified use of force against oppressive governments and occupations. It can be under-inclusive in that it excludes serious crimes and attacks against civilians that ought logically to be included, but are not, on purely political grounds.[3]

For instance, the definition fails to distinguish between criminal terrorist entities and liberation movements or groups opposing tyranny, whose legitimacy can shift depending on the time period and the dominating political interests at stake. Under this definition, Nobel Prize recipients Nelson Mandela and Rigoberta Menchu would be considered terrorists. Members of the French resistance fighting against the Nazi occupation were branded as "terrorists" by the Vichy authorities. More recently, participants in the 2011 Arab Spring protest movements against Egyptian dictator Hosni Mubarak have also been accused of being members of a "terrorist group" and deemed inadmissible due to security concerns, without evidence that they did more than engage in their right to freedom of expression and assembly.[4]

The definition does capture violent white supremacist groups, but we have seen how it also captures Palestinian and Kashmiri groups – as well as charities like IRFAN, proscribed for donating medical equipment to the Gaza Strip – conflating groups originating under or responding to long-term military occupation, with white supremacists and neo-Nazis, all under the rubric of a broad and inconsistent concept of "terrorism."

This is why there is no international consensus in multilateral forums for a workable definition of terrorism.[5]

Beyond the application of terrorism laws by the justice system, the use of accusations of terrorism by bad actors to target political opponents and marginalized communities is also well-documented. For example, proponents of the non-violent Boycott, Divestment and Sanctions movement in support of Palestinian human rights have been accused of both supporting terrorism and engaging in anti-Semitism.[6] Similarly, Indigenous land defenders have been accused by political opponents of engaging in or supporting terrorism for simply exercising their territorial

[2] Canadian Association of University Teachers (CAUT), "Submission to the House of Common, Subcommittee on public safety and national security, regarding the *Anti-Terrorism Act*," February 28, 2005, p.31. Compulsion and necessity can be a defence, but under rare circumstances.

[3] *Ibid.*

[4] Nicolas Keung, "Egyptian asylum seeker with rights breached faces deportation," *The Toronto Star*, 21 April 2021. Online: https://www.thestar.com/news/canada/2021/04/21/egyptian-asylum-seeker-with-rights-breached-faces-deportation.html

[5] See, for example, Wesley S. McCann & Nicholas Pimley, "Mixed Mandates: Issues Concerning Organizational and Statutory Definitions of Terrorism in the United States," *Terrorism and Political Violence* (2020) 32:4, 807-830, DOI: 10.1080/09546553.2017.1404457

[6] https://www.aljazeera.com/opinions/2016/2/28/canada-jumps-on-the-anti-bds-bandwagon

rights[7]. Black Lives Matter activists have similarly seen accusations lobbed at them, leading to removal of content and suspension of social media accounts.[8]

Other examples could include:

- Academic work and reports on Palestinian human rights have been labelled as anti-Semitic and supporting terrorism, and could be made inaccessible based on automatic moderation or complaints.
- Calls for non-violent civil disobedience in support of Indigenous rights have been labeled by some Canadian politicians and media outlets as "terrorism." Would such postings be made inaccessible based on automatic moderation or complaints?
- Groups engaged in conflict often paint one or the other as "terrorist," particularly when one is a non-state actor and the other is a state actor. How will a platform decide what should be included as "terrorist" content, especially given the global application of the proposed regime?

The proposed system would allow for vague definitions of terrorism to be weaponized against those very groups that proposed legislation aims to support.

This renders both the proposed content moderation and reporting processes open to political arbitrariness and potentially vulnerable to manipulation for specific political interests.

Determining whether or not something consists of "terrorist content" is therefore already incredibly difficult to ascertain, even within the justice system. Adapting the current criminal code definition of "terrorism" to a regulatory framework, as proposed, would almost certainly mean an expansion of what content would fall under the definition. Social media companies would then be asked to develop both an automatic moderation system to make terrorism content inaccessible on their platforms as soon as possible, as well as to have staff not specifically trained in terrorism law to adjudicate, in a very short time frame, and under threat of financial penalty, what consists of terrorism content and what does not. The result will almost certainly be the over-moderation of content, impacting not just freedom of expression, but also targeting the views of those communities that the proposal sets out to protect.

To inject an essentially political concept like "terrorism" into a legal framework is to ensure that politics, not law, determines culpability. If we are truly interested in condemning and prosecuting these crimes, it must be the act, not the motive that is determinative.[9]

Content that incites violence, whether terrorist or otherwise, would seem to be clearer and more precise.

[7] https://www.ctvnews.ca/politics/conservative-mp-questions-whether-rail-blockades-constitute-terrorism-1.4830220

[8] https://www.usatoday.com/story/news/2019/04/24/facebook-while-black-zucked-users-say-they-get-blocked-racism-discussion/2859593002/

[9] Canadian Association of University Teachers, *supra* note 2, at 32.

C. Moderation & appeal process

Our concerns around the application of "terrorist content" are exacerbated by the proposed moderation obligations and associated appeals process being put forward, particularly in combination with the proposed monetary penalties.

The proposal suggests that moderation would be carried out in two distinct ways in order to render harmful content inaccessible to people in Canada: via automatic moderation and complaints-based moderation. Both of these approaches carry with them distinct concerns.

Before addressing the specifics, there is an overarching concern about placing the determination of harmful content in the hands of private entities. The "privatization" of the decisions regarding discourse and public speech raises very specific concerns. As explained by Cynthia Khoo in "Deplatforming Misogyny," these kinds of questions should generally be considered by public institutions, and not private entities, particularly given that companies motivated by profit should not be relied upon to protect or advance issues of human rights or public good.[10]

To protect against this, we would argue that any policy proposal must include clear, restricted definitions of the content in question and strict reporting and enforcement rules, which we do not feel this proposal adequately contains in relation to terrorism content (and arguably other forms of content as well).

Automatic moderation

The proposal would oblige included platforms to "take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS [Online Communications Service] and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada." It is likely that such automated systems would be powered by algorithms developed by platforms or third parties to identify and render inaccessible the targeted content.

This obligation goes much further than other comparable harmful content moderation regimes, including those in Germany, France and the UK, which purposefully do not include automated moderation of all content. While this is partially because of the restriction on doing so in the EU's e-Commerce Directive, it is primarily in recognition that such automated moderation of all content violates fundamental aspects of free expression by surveilling and monitoring all content for violations.[11] While the proposed system has been defended as being based on systems adopted in like-minded, rule of law countries, the fact that this proposal goes further than what has been accepted in those jurisdictions is often excluded from the conversation.

This filtering of content as it is published also raises a practical question: it would require all content accessible by Canadians – and therefore all content published on, for example, Facebook

[10] https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[11] https://www.eff.org/deeplinks/2021/07/uks-draft-online-safety-bill-raises-serious-concerns-around-freedom-expression; https://www.counterextremism.com/sites/default/files/CEP-CEPS_Germany%27s%20NetzDG_020119.pdf

– to undergo moderation. This would mean that content in a variety of languages and from a variety of political and social contexts would need to be evaluated based on the Canadian government's definition of terrorism (and other harms). Therefore, any individual in the world posting to Facebook could be impacted by Canada's regulatory scheme. This could implicate large amounts of resources, and would possibly limit the access of people in Canada to important and relevant content that, due to cultural or linguistic differences, would be automatically made inaccessible. As will be discussed later, it also raises questions about access and fairness in any appeals process.

Filtering by algorithm also raises concerns about effectiveness and bias. As we have seen in multiple other contexts, reliance on algorithms to identify harmful language or content has led to disproportionate impacts on Black, Indigenous and people of colour (BIPOC), women and gender-diverse people.[12] There is no reason to expect a different result in the context of the proposed framework. In fact, we may expect even greater difficulty, as problems with algorithmic monitoring have been identified in more straightforward situations and with clearer definitions than that of "terrorist content."

While there are provisions in the proposal that such automatic moderation must "not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act," it is not clear that there would be proactive inspection of such algorithms (for example, via an initial review by the proposed Digital Safety Commission). It is also unclear to what degree or under what circumstances a member of the public could make a complaint if they believe that algorithms, overall, are resulting in "differential treatment of any group based on a prohibited ground of discrimination," particularly in the context of over-moderation which we imagine will be more difficult to monitor than, for example, under-moderation.

Finally, issues with an algorithm could conceivably be based on a characteristic other than a "prohibited ground for discrimination." For example, there could be unintended consequences of media or academic content not created by a member of a protected group being overly-moderated because of subject matter or language used. Would there be grounds for recourse?

Complaint-based moderation

The proposed framework would allow for a new reporting system for people accessing a platform in Canada in order to signal harmful content, including terrorism content, to the platform in order to render it inaccessible. The platform would be required to act within 24 hours, informing the complainant whether they are taking action on the piece of content flagged and what action that is. If the piece of content is deemed harmful and is rendered inaccessible, the individual who posted the content would also be contacted. In both instances, the individual would be informed of the process for appealing the platform's decision.

[12] See notes 6, 7, 8 & 10

This system is more widely used among jurisdictions similar to Canada's, including the UK and Germany. However, it has also met considerable opposition in those countries, and was even deemed largely unconstitutional in France.[13]

Concerns also exist around the short time period in which platforms must render a decision. It is clear that some forms of harmful content are readily identifiable as illegal, and would not be impacted by a mandatory 24-hour response time. However, large amounts of content including in regard to "terrorist content" will likely fall in a grey area of lawfulness or harmfulness, requiring examination of context or seeking out further information. To expect a decision within 24 hours, under penalty of non-compliance, would likely force a "render inaccessible first, ask questions later" approach. While the proposal makes explicit mention of setting different time periods by regulation (including shorter time periods), it positions 24 hours as the standard by which to decide all moderation decisions; it will be necessary to justify going forward why there should be longer time frames, rather than needing to justify a short time frame such as 24 hours. For example, in Germany, for grey area content, platforms have up to a week to make a moderation decision, and are able to request a further extension if necessary.[14] If this is the ultimate goal for the Canadian system, presenting these options clearly would have ensured a more comprehensive consultation and understanding of the moderation process.

Finally, while reports in Germany ostensibly point to fears of over-moderation of content having not played out, others have pointed out that a lack of clear and uniform reporting from platforms has made it difficult to ascertain the true impact (either positive or negative) of the system.[15] Once again, it is also important to bear in mind that this comparison is with a system based only on report-driven moderation, not automatic moderation as considered in the Canadian proposal.

Appeal process

The proposal would allow an individual who disagrees with either the decision to leave a piece of content accessible, or to make it inaccessible, to appeal it to the platform (which, under the new framework, would be obliged to create an appeal process). Our understanding is that this is true whether the content is made inaccessible based on automatic moderation or through a user report; however, this must be further clarified.

If the individual is not satisfied with the platform's decision of their appeal, and has exhausted all avenues for appeal with the platform, they may appeal it to the newly proposed Digital Recourse Council of Canada (the Council). In the case of a complaint about content **not** being made inaccessible, and the Council rules that the platform erred, the Council can **order** the platform to make the content inaccessible. In the case of a complaint about content that **was** made inaccessible (asking that it should be restored), if the Council finds the platform erred, it can only **recommend** that the content be restored, but the platform has the final say based on its own community guidelines. This is clearly problematic, as it reduces the ability of individuals whose content has been removed to seek adequate recourse.

[13] https://www.politico.eu/article/french-constitutional-court-strikes-down-most-of-hate-speech-law/

[14] https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

[15] https://policyreview.info/pdf/policyreview-2019-2-1398.pdf

Also missing from the appeal process is clarity around timelines and accessibility. For example, a film festival specializing in Palestinian films is accused, unjustly, of programming content that supports terrorism. The festival's online event postings are either made inaccessible because of an algorithm or because of bad-faith reporting. The content is made inaccessible because of error in the algorithm or the need to adjudicate within 24 hours. The film festival appeals, and is eventually proven correct. The platform renders the content accessible, but the weeks-long process results in the content becoming no longer relevant, harming the festival and possible attendees. Arguably, the pursuit of reducing online harms is more important than access to a film festival; however, the impact is felt most strongly by a community that should ostensibly be protected by the new system rather than penalized.

Similar scenarios are possible when considering protests in support of Indigenous rights, given that Instagram has already removed content related to Missing and Murdered Indigenous Women and Girls, or acts in support of Black Lives Matter, which has also seen their content more heavily censored on social media platforms.[16]

While the appeal process is one of the more positive portions of this proposal, there are several outstanding concerns, particularly in relation to other aspects of the proposal. For example, the regime is global in scope, meaning that content posted from anywhere in the world is implicated, so long as it is accessible in Canada. It is likely, then, that individuals not in Canada will see their content removed and therefore need to engage in the Canadian appeal process. This is particularly true for automated moderation, since it can be assumed that most people in Canada will be engaging with content that is in a language they comprehend, shared in networks of their contacts, or referred to them by the platform itself.

It is unclear whether an individual who is not in Canada will be familiar enough with the Canadian appeal process to engage with it, or be able to go through the process in one of Canada’s major languages (platforms may specialize in providing service in a broad range of languages, but the Digital Recourse Council may not). They may also simply not care whether their content is available to people in Canada. The result could be that content that should otherwise be accessible to people in Canada would remain inaccessible. This would be a problem for content overall, but is even more important when such information may be necessary for research, journalistic or other purposes. For example, if foreign language posts about a conflict in another region of the world were to be made inaccessible without cause due to over-breadth of automated moderation. Because the primary audience is not Canada, and because they do not speak a language commonly used in Canada, they decide not to appeal. Canadian audiences on social media would remain unaware of what content they do not have access to. This may seem far-fetched, but it could be possible that access to important and relevant information related to the Rohingya genocide, or the Arab Spring could have been blocked to Canadians.

[16] See note 12

Monetary penalties

If a platform does not comply with their obligations, they face significant monetary penalties, ranging from $10 million or 3% of income (whichever is higher), and $25 million or 5% of income in cases of non-compliance with sanctions. While financial penalties on their own are not necessarily problematic, in conjunction with short take down windows, they could provide yet another incentive for platforms to remove content in order to remain compliant. While in theory, sanctions could also be brought due to over-moderation it is likely that this would be much rarer than sanctions for lack of moderation.

D. Information sharing with law enforcement and intelligence agencies

The framework proposes two options for sharing information with law enforcement and national security agencies. The first would "require that a [platform] notify the RCMP in circumstances where the [platform] has reasonable grounds to suspect that content falling within the five (5) categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property."

The other is that a platform "must report prescribed information in respect of prescribed criminal offences falling within the five (5) categories of regulated harmful content to prescribed law enforcement officers or agencies, as may be prescribed through regulations established by the Governor in Council."

Both proposals would create new obligations to automatically report content to law enforcement and intelligence agencies, raising questions about the dangers of proactive reporting requirements, especially in light of "automatic moderation."

While the first appears more restrictive, requiring platforms to determine what constitutes "reasonable grounds to suspect" imminent risk of serious harm would likely result in over-notification. An automated system would also see such content shared with the RCMP without review, possibly sharing information that, after further appeal, is not considered as presenting "imminent risk of serious harm". It is also unclear why, if the goal is to oblige platforms to notify the RCMP in cases of imminent risk of serious harm, why that would be restricted only to risks that fall under the five categories. This is not an argument for expanding reporting obligations, but an example of how this approach fails to address the issue at hand.

The second proposal is the more troubling of the two. It creates an open-ended system of information sharing with many more law enforcement and intelligence agencies. In fact, the second proposal explicitly contemplates that any content related to terrorism or incitement to violence be shared immediately with CSIS.

Both proposals also require the platforms to not disclose either notifications or reports "if the disclosure could prejudice a criminal investigation, whether or not a criminal investigation has begun" or "if the disclosure could be injurious to national security." This could mean that an individual would see their online content reported to law enforcement or national security agencies and never be informed, including if a criminal investigation never begins or on the incredibly broad grounds of "injurious to national security."

There is an attempt to mitigate this issue by including the following section:

> Retention period and use:
> 32. The Act should provide the Governor in Council with the authority to make regulations with respect to the use and subsequent disclosures of information provided to (a) the RCMP or (b) law enforcement and CSIS under part [E], **depending on the privacy interests engaged by that information.** [emphasis added]

Here, though, the relevant phrase is "depending on the privacy interests engaged by that information." It is likely that content posted on social media platforms would have a low-level privacy interest, although this is currently disputed by privacy advocates given that content posted on social media platforms, while accessible, may still retain some expectation of privacy from government agencies. Further, since this system would be applicable to non-Canadians outside of Canada, they would not be granted the same privacy interests as Canadians or people in Canada.

While platforms are also obliged to ensure that the reporting to law enforcement / security agencies does not result in "differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act and in accordance with regulations," we have seen how agencies defend surveillance and profiling of specific communities on the basis of national security in order to avoid accusations of "differential treatment."

Finally, the framework proposes that platforms who report to CSIS and the RCMP or other agencies in good faith pursuant to the act would be immune to civil or criminal proceedings. So, for example, if a platform's auto-reporting system accidentally sends information that results in the violation of an individual's rights, including surveillance or possible detention, they cannot hold the platform accountable for that action.

Again, all the issues above are exacerbated by the underlying problems in identifying terrorist content highlighted earlier.

The result is that social media platforms would essentially be recruited and turned into extensions of the surveillance tools already at the disposal of Canada's law enforcement and intelligence agencies.

E. New CSIS warrant

The proposal also makes the extraordinary argument that CSIS be granted a new form of warrant. Arguing that CSIS is currently limited to one kind of warrant that takes several months to process, the proposal suggests a new "simplified" process for seeking out a judicial authorization for obtaining identifying information (basic subscriber information, or BSI) in order to aid with the investigation of online harms.

While it may be true that the current judicial authorization process is not adequate for CSIS to assist in the investigation of online harms, this is a secondary issue. The first is whether CSIS should be recruited into this form of investigation in the first place. While action must be taken to address threats of white supremacist and hate-based violence, this should not be used to justify the further granting of police-like powers to an intelligence agency that operates in secret. We have already seen CSIS granted threat-disruption powers that mimic those of the police. This new form of warrant would further entrench the idea of CSIS investigating criminal activity akin to law enforcement, well beyond its role as an intelligence agency.

If there is a problem with CSIS not being able to carry out its intelligence work regarding threats to national security, it should be addressed in a stand-alone bill and justified on those grounds.

Finally, any new warrant power would not be limited to investigating online harms, but could be harnessed in other areas of CSIS' work as well. At a time where there are serious questions before the court about CSIS' breach of its duty of candour in warrant applications, it is concerning that the government would be proposing to create a new, simplified and flexible process for obtaining judicial authorization to collect information about individuals.

F. Transparency and accountability

As mentioned above, there are certain requirements placed upon the platforms to report to the Data Commissioner annually. This is an important and positive part of the proposal, especially in terms of integrating concerns that have been raised in other jurisdictions about problems with reporting. However, it is crucial that this reporting be strengthened in several ways:

1. Other jurisdictions require platforms to publish publicly available transparency reports on a regular interval (for example, every six months in Germany). The Canadian proposal should include similar requirements.
2. While the Digital Safety Commissioner and Recourse Council are required to make extensive reports to the Minister, there are no provisions that such reports will be tabled in Parliament. It is crucial that such reports be made public.
3. Given the role of the RCMP and/or CSIS, they should be required to report separately to the Minister of Public Safety. Those reports should be tabled in Parliament, and proactively shared with the Privacy Commissioner, CCRC and NSIRA.

Conclusion

Our coalition has not taken a position on the need for new regulations related to online harms. Indeed, in much of our recent work we have taken the position that more needs to be done to protect various communities, including BIPOC, women and gender diverse people, from growing violence and threats from white supremacist, far right or misogynist organizations. The lack of action in this area by social media platforms has been well documented by groups including LEAF and Amnesty International Canada[17].

However, over the past two decades, we have seen the impacts that expanding national security and anti-terrorism laws have had on the rights of people in Canada, and internationally. This is particularly true for Muslim, Arab, Indigenous and other racialized communities and their allies who have faced profiling, disproportionate policing and other human rights abuses. Moreover, growing surveillance predicated on countering terrorism has overarching impacts on privacy, freedom of expression, freedom of association and freedom of movement.

We believe that in order to achieve the stated goals of the government's proposal - to counter real world harms faced by protected classes of individuals as defined in the Canadian Human Rights Act - that it must be reviewed with the issues we lay out above in mind, particularly in regard to the inclusion of "terrorist content" and the involvement of law enforcement and national security agencies in any new regime.

[17] https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-1/; https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf