CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Submission in relation to the consultation on addressing harmful content online

September 25, 2021

Cara Zwibel, Director, Fundamental Freedoms Program

Canadian Civil Liberties Association
90 Eglinton Ave. E., Suite 900
Toronto, ON M4P 2Y3
Phone: 416-363-0321
www.ccla.org

I. Introduction

The Canadian Civil Liberties Association ("CCLA") is an independent, national, nongovernmental organization that was founded in 1964 with a mandate to defend and foster the civil liberties, human rights, and democratic freedoms of all people across Canada. Our work encompasses advocacy, research, and litigation related to the criminal justice system, equality rights, privacy rights, and fundamental constitutional freedoms.

We recognize the public pressure on governments to "do something" about the Wild West of online content. With this proposal, however, the Heritage Ministry is addressing areas far outside its core expertise; it ought not to be stewarding legislation that so impacts Canada's foreign affairs, anti-terrorism and criminal laws. Consulting with other Ministries and other jurisdictions and stakeholders will not suffice, any more than one would want Foreign Affairs to regulate the radio broadcast industry. This may explain the proposal's over breadth.

The CCLA has several concerns about the government's proposed approach to "online harms" as well as concerns about the way this consultation is being undertaken. Considering the timing of this consultation process (discussed briefly below), our submissions on the substantive concerns about the proposal are set out in brief and are not exhaustive. This should not be misinterpreted to suggest that CCLA has little to say about the proposal. To the contrary, we believe a policy issue of this level of importance, and a proposal with such novel elements, must be subject to more rigorous scrutiny. We welcome the chance to be part of more meaningful discussions in the future; we will strongly resist attempts to push through legislation on this issue in the absence of truly inclusive and substantive consultations with Canadians.

The proposal is a radical policy change, in our view. It is excessive in scope, effect and purpose. CCLA's substantive concerns about the proposal include the following:

1) **The scope of the proposal problematically attempts to deal with a variety of different "online harms" and not solely unlawful content.** This amounts to significant regulation of the ways in which Canadians communicate. The proposal also fails to appreciate how different the content categories are and the possibility that they may need to be addressed using different policy tools.
2) **The proposal merges communications policy/regulation with public safety, national security and law enforcement concerns in a way that is quite troubling.** Mandatory reporting by online communications service providers (OCSPs), as tentatively defined in the proposal, give rise to significant questions about the use of artificial intelligence and over-reporting, as well as state surveillance and the role of large platforms in its facilitation. The law enforcement proposals would also leave a great deal of detail to be decided by regulation, leading to concerns about political interference and the absence of meaningful democratic debate.
3) **The proposal includes 24-hour takedown requirements for platforms for a wide variety of content and fails to consider the significant risk to lawful expression posed by this requirement.** There are few meaningful due process protections built into this scheme.

4) **The proposal includes a power to seek website blocking orders. Although this is touted in this context as a means of making the internet safer, site blocking presents a real threat to an open and safe internet.** Clear and meaningful safeguards are required if such a power is deemed necessary in extraordinary circumstances.

CCLA does **welcome the proposal's inclusion of new transparency obligations** for online communication service providers (OCSPs), although care should be taken to ensure that a push for transparency from platforms doesn't inadvertently impinge on user privacy by requiring platforms to collect more information from users in order to fulfill their statutorily-mandated reporting requirements.

With respect to process, we note that the government's proposal for addressing harmful content online was released on July 29, 2021 and the closing date for submissions is September 25, 2021. A federal election was called on August 15 and voters cast their ballots on September 20, 2021. Thus, throughout much of the consultation period, it was unclear whether the government that undertook it would be elected and form a government. As noted in an open letter to individuals in the Privy Council Office and to which CCLA was a signatory, guidance on the activities of government after Parliament is dissolved states that policy work should be limited to routine, non-controversial or urgent areas, or where there is agreement by opposition parties. The online harms policy question falls into none of these categories. It is a complex area that raises fundamental questions about communications in Canada, human rights, corporate social responsibility, and the role of the state in regulating and monitoring Canadians' expression.

This issue deserves careful consideration and meaningful engagement with Canadians. To ask civil society to provide feedback to a government proposal when it is unclear if that government will return to govern is insufficiently respectful of the time and efforts that civil society organizations expend on these kinds of consultations. It is also likely to diminish the breadth and depth of submissions the government receives. Further, the government's proposal in this case is very detailed and in fact asks very few questions of those interested in participating in the consultation process, suggesting that the government has largely already decided what it intends to do. **We strongly believe that a much more robust consultation process should be undertaken as soon as possible.**

II. The Scope of "Online Harms"

Throughout the consultation documents and in messaging from the government, the focus of the proposal has been on tackling "online harms". This suggests that it targets content that is *harmful* but not necessarily *unlawful*. This is inappropriate. The focus of any legislative proposal should be on illegal content. Although the government's technical document notes that the content categories will use definitions that borrow from the *Criminal Code*, it also states that these categories will be adapted to the "regulatory context". It is not clear what exactly this language means, or how it will apply to the different types of content. The proposal also notes that there will be authority for the Governor in Council to, by regulation, define certain specific terms used in the definitions of harmful content. Thus the scope of the law, and the kinds of content it may capture, can be expanded without any meaningful democratic oversight. The expressive freedom guaranteed by the *Charter* dictates that lawful communications should not be the subject of

government restrictions, but the proposal could be used to restrict the so-called "lawful but awful" content online.

The government's proposal also groups together five quite different types of "harmful" content: child sexual exploitation content, terrorist content, content that incites violence, hate speech and the non-consensual sharing of intimate images. Not only are these content categories very different, but the types of harms to which they give rise also vary considerably. For example, while hate speech may constitute a criminal offence in some contexts (e.g. where the communication is willful and intended to promote hatred and where the hallmarks of hate identified by the Supreme Court are present), the acts that result in visual depictions of child sexual exploitation are themselves criminal in almost any circumstance and there are offences not only for creating and distributing this material, but also for accessing it. As a result, some of the categories of content will require a greater understanding of context to assess legality, while others will be more obvious and easier to identify either using automation or manual human review. The types of content have little in common with one another except that they may be communicated in the same type of online space, through OCSPs. Given these differences, it is questionable whether these diverse types of content should be addressed using identical policy tools.

III. Public Safety and State Surveillance

The CCLA has significant concerns about the proposal's plans to leverage OCSPs as agents of law enforcement, creating mandatory reporting and preservation obligations that may expand over time and significantly impact the privacy rights of Canadians. The involvement of CSIS is of particular concern.

Further, while we appreciate that adequately addressing some of the harms identified in the proposal will require the assistance of law enforcement, the feasibility of mandatory reporting on this scale is far from evident. The sheer volume of content that some OCSPs would have to proactively review and potentially report suggests that the use of artificial intelligence is inevitable. It is likely that some content will be assessed and reported to law enforcement based exclusively on algorithms that will have a rate of false positives. The consequences to an individual of being flagged for police investigation are significant. The proposal contains no consideration of these consequences or the due process protections that might mitigate them.

The two options proposed in the government's technical document each have serious flaws. The first option is focused on reports where the OSCP has reasonable grounds to suspect there is an imminent risk of serious harm to any person or to property. However, the focus on imminent harm suggests that OCSPs are expected to proactively review and report content in real-time, something that is not feasible for the reasons outlined above. The second option requires OCSPs to 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." It is difficult to comment on a proposal that leaves so many details to regulation. The question of when online communications should be turned over to law enforcement officials is something that should be the subject of debate in Parliament.

IV. Twenty-Four Hour Takedown

The government's proposal creates several new obligations on OCSPs including responding to individuals who flag content as falling within one of the prohibited categories within twenty-four hours of the flagging taking place. If the OCSP finds that the content does fall into one of the categories, it is to be made inaccessible to individuals in Canada within that twenty-four-hour period, although the Governor in Council may both extend that period or shorten it in respect of certain types of content.

The diverse types of content that the proposal targets each have their own unique characteristics and while some may be easy to identify, others will be much more difficult, particularly under severe time pressure and where the volume of content is large. Identifying *illegal* hate speech and terrorist content, for example, is not an easy task if one takes seriously the obligation to interpret these terms narrowly to avoid unreasonably restricting freedom of expression. Even judges who are trained in statutory interpretation and constitutional law may disagree about what falls on the right or wrong side of the line with respect to these types of content, yet the proposal imagines that OCSPs will be able to make these determinations for potentially huge volumes of content within 24 hours. There is no requirement in the proposal that these providers receive any training or have any background understanding of Canadian law. If OCSPs are going to be the "front line" when it comes to policing Canadians' communications online, it is important that they understand the proper scope of the law, and its constitutional limits.

Further, experience in other jurisdictions and the sheer scale of content on some OCSPs strongly suggests that content will be removed when there is any doubt about its legality, and not solely when its illegality is plain and obvious. Rather than erring on the side of caution, platforms have incentives to remove content quickly where judgments are difficult to make. It is worth noting that the Canadian Commission on Democratic Expression rejected the idea of 24-hour takedowns for content, except for the narrow category of content that presents an imminent threat to a person. CCLA believes this standard is more in keeping with Canada's commitments to freedom of expression and deals appropriately with the most egregious and potentially dangerous forms of online content. The government should eliminate the 24-hour takedown or to dramatically reduce the scope of content to which it applies.

V. Website Blocking

The proposal seeks to establish a scheme to apply to a court for a website blocking order. Although the suggestion is that this would be used in exceptional circumstances for repeat offending conduct by OCSPs, it is worth emphasizing that website blocking is a truly extraordinary remedy when imposed by a state body. This tool will often be both inefficient and ineffective, resulting in a game of whack-a-mole as repeat offenders move to new online spaces to engage in the targeted conduct. There are also technical concerns about website blocking and how it will impact the online ecosystem as a whole.

VI. Transparency Obligations

Finally, we welcome many of the proposals to increase the transparency required from OCSPs. This information is vitally important for any regulatory efforts and can help encourage responsible

corporate behaviour. However, many of the reporting requirements call for a significant amount of detail from service providers which may impact the information they, in turn, have to collect from their users. This is not a trivial concern. We already have significant experience and concerns about the way in which some platforms collect and utilize user information. When paired with the transparency obligations and the mandatory reports to law enforcement, user privacy is at significant risk from this proposal. The transparency obligations should be crafted in a way that does not have unintended consequences for user privacy.

VII. Conclusion

As noted above, the CCLA is concerned about the substance of the government's proposal to address online harms, and about the manner in which the government has treated this issue and public consultation. Regulating the way in which Canadians communicate online – including the content that they may access from locations all around the globe – is a significant public policy project that merits broad participation and involvement from Canadians. Further, many countries look to Canada as a mature liberal democracy and may seek to emulate the tools developed for tackling online harms here. Twenty-four-hour takedown requirements and website blocking orders are dangerous tools anywhere, but may be of heightened concern in the hands of regimes that have a lesser commitment to democracy. Given the truly global nature of the internet, this is a concern that the government should take seriously.

This submission is brief given the inadequate time provided for consultation; we have highlighted some of our core concerns but have others that are not addressed herein. The government should not introduce legislation in this policy area until a more fulsome consultation process has taken place. We look forward to participating in that process.