Global Network Initiative Submission to the Government of Canada on the Proposed Approach to Addressing Harmful Content Online

Introduction

The Global Network Initiative (GNI) appreciates the opportunity to provide input in response to the Canadian Government's proposed approach to addressing harmful content online ("proposed approach"). GNI is the world's preeminent multistakeholder collaboration in support of freedom of expression and privacy in the information and communications technology (ICT) sector. GNI's members include leading academics, civil society organizations, ICT companies, and investors from across the world. All GNI members adhere to the GNI Principles on Freedom of Expression and Privacy, which provide guidance on how to navigate government demands and restrictions consistent with international human rights law and the UN Guiding Principles on Business and Human Rights.

GNI brings a unique set of perspectives and experiences to bear on the issues addressed in this consultation. Last year, GNI conducted wide-ranging research and global consultation on legal and regulatory efforts to address online harms around the world. GNI engaged in a detailed analysis of two dozen such content regulation efforts, convening six events targeting government officials and other stakeholders in Africa, the EU, India, Pakistan, and the U.K. This work culminated in GNI's *Content Regulation and Human Rights Policy Brief* (policy brief), which identifies helpful and problematic elements of emerging approaches and includes specific recommendations for how governments can address digital content-focused concerns consistent with human rights principles.

Our analysis of the proposed approach draws upon the diverse expertise of our multistakeholder membership and benefits from the analysis in the policy brief and our feedback on dozens of domestic content regulations in other countries. We stand ready to answer any questions and to continue to engage constructively with the Canadian government on the proposed approach and any other matters related to human rights in the digital age.

Analysis

1. Canada's Leadership Role in Human Rights

GNI acknowledges and is grateful for the significant role the Government of Canada has played in supporting the development of an open, interoperable, safe, and secure Internet. This includes Canada's role as a founding member and upcoming chair of the Freedom Online Coalition, leadership in the work of UN bodies and other multilateral initiatives dealing with issues of Internet governance, and active engagement in various multistakeholder processes, such as the Christchurch Call to eliminate terrorist and violent extremist content online.

As a result of this prominent leadership, the approaches Canada takes to addressing concerns about online harms will serve as a reference point for other governments and contribute significantly to global norm setting. They will also impact the ability of the Canadian government, as well as other aligned governmental and non-governmental actors, to engage with and influence similar efforts in other countries.

While we appreciate the public policy rationale for addressing online harms, we are concerned that some aspects of the proposed approach appear to be inconsistent with international human rights principles, regulatory best practice, and Canada's leadership on Internet freedom. We encourage the Government of Canada and the Canadian Parliament to ensure that its efforts are fully aligned with the country's international human rights commitments and will support, rather than hinder, its continued international leadership on these matters.

2. Focus on online harms

The proposed approach aims to address concerns about online harms in at least five areas — terrorist content, content that incites violence, hate speech, non-consensual sharing of intimate imagery, and child sexual exploitation content — all of which are illegal under the Canadian Criminal Code. We very much appreciate the commitment to focusing on areas of speech and conduct that are already defined in domestic law, rather than creating new and vaguely defined categories. However, we also note with concern the proposal's aim to "borrow" existing definitions and adapt them to the "regulatory context." Opening up these categories of prohibited speech to re-definition is likely to lead to significant controversy. Any changes made to these definitions are likely to confuse the public and create uncertainty, especially when it comes to use of humorous, satirical, and journalistic content, as well as counter-narrative efforts (e.g., CVE). In addition, such changes will weaken the value that existing jurisprudence can have in helping actors, including Online Content Service Providers (OCSPs), who will need to interpret and apply these categories.

It is critical that any further regulation avoid broadening the definitions of these existing provisions specifically for the online space. As we note in the policy brief, requiring removal of certain forms of speech that would otherwise be legal in analog form raises risks of discriminatory impacts and undermines the broad scope of the right to freedom of expression. The government's background paper states "the approach upholds and protects human rights, while also respecting fundamental freedoms, notably freedom of expression." However, it fails to sufficiently acknowledge the potential that overly broad definitions, particularly when paired with significant obligations on intermediaries and penalties for noncompliance, could contribute to invasive monitoring of users and unnecessary restrictions of their content and conduct. As just one example, the technical paper states that "[t]he concept of terrorist content, should refer to content that actively encourages terrorism and which is likely to result

in terrorism," which ignores further qualifications such as intent to intimidate the public and political and religious motivations that exist for definitions of terrorism in Canadian law.

3. Scope of application

In the policy brief, we call on lawmakers and regulators to ensure any restrictions on freedom of expression imposed by content regulation efforts meet the standards of necessity and proportionality. One critical way to avoid unnecessary and disproportionate impacts on freedom of expression is to focus these approaches on those services that are best positioned to identify and address the "specific concerns at issue." In this regard, we applaud the proposal's exclusion of private communications services, as well as telecommunications companies, neither of which are well positioned to implement the proposed regime in a proportionate manner.

Furthermore, we appreciate that the technical paper proposes authorities to target specific obligations to specific categories (and sizes) of companies. However, the broad definition of OCSPs in the proposal overlooks the significant disparity in capacity for certain smaller companies and companies at different layers of the ICT stack to implement the obligations outlined in the proposal — with one expert noting a particular risk for internet infrastructure providers. The apparent lack of attention to and nuanced application toward new and smaller providers could create unnecessary and unintended market consequences.

4. Breadth of obligations

The proposed approach presents a set of sweeping obligations for OCSPs in Canada that, as framed, could pose significant risks for freedom of expression and privacy. These obligations cover moderation practices around potential harmful content, transparency measures, reporting requirements to law enforcement and/or intelligence agencies, and related data preservation requirements.

Under the proposed approach, OCSPs "must take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada." The act calls on OSCPs to respond to reports of harmful content from any person in Canada "expeditiously" (currently defined as within 24 hours).

As we note in the policy brief, "by imposing strict time limits on all content adjudication, states may effectively hinder the ability of ICT companies to prioritize resources and make nuanced, content and circumstance-specific determinations. These time limits may also make it difficult for the author to contest the allegation (i.e., issue a counter-notice) or seek injunctive relief or other remedy." The proposed approach implies Canadian authorities could shorten or otherwise adjust timelines for the different forms of harms. We strongly encourage an alternative approach that provides clear guidance as to what characteristics or circumstances merit prioritization in content moderation and allows flexibility to those charged with making such determinations.

GNI appreciates the need for robust content moderation processes and believes that international human rights and due process standards should guide both these processes and any corresponding regulatory approach. In this regard, we are pleased to see proposed requirements for OSCPs to provide notice about decisions to their users, as well as opportunities for redress. As we note in the policy brief, however, outsourcing enforcement of criminal provisions to private companies, without appropriate guidance on interpretation and application (e.g., the lack of a clear definition of "reasonable measures"), raises significant concerns under the international principles of legality and necessity.

The current framing also encourages adoption of and reliance upon automated content filters, which are unlikely to serve as the least restrictive means to address the broad set of harms identified in the proposal. The biases that have been documented to feed into and be perpetuated by such automated measures can also undermine the stated aim to ensure that companies' moderation practices "do 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." As with other provisions, this reliance on filters, if enacted into law, is likely to be picked up upon and emulated by other governments.

The proposed approach also sets forth reporting obligations that pose significant risks for user privacy. The proposal sets out two different potential regulatory approaches requiring platforms to either (1) notify the Royal Canadian Mounted Police "where there are reasonable grounds to suspect the content within five categories reflects imminent risk of serious harm," or (2) report prescribed content to law enforcement and/or the Canadian Security Investigative Service (CSIS) "to allow for appropriate investigative and preventive action." Requiring platforms to proactively monitor and then share user data, without any sort of specific request, effectively deputizes non-democratically accountable providers as law enforcement and adds significant challenges for companies working to uphold commitments to user privacy.

As we describe in the policy brief, requirements for transparency by intermediaries and states can offer important safeguards to help mitigate the potential for over-removal and self-censorship. We therefore appreciate the stated commitment to require enforcement bodies to issue annual reports to the Minister of Heritage, as well as to require decisions and orders from enforcement bodies to be made public. It is important that these transparency requirements are sufficiently detailed and reviewed on an ongoing basis so that government agencies and oversight bodies can adjust for rapid changes in technology and trends. Meanwhile, company transparency reporting requirements must afford sufficient flexibility to accommodate different company size and business models, and allow companies to prioritize addressing the most salient harms on their respective platforms. It is also important that the Canadian government work with partners like Australia, the European Union, and the United Kingdom, who are also considering detailed reporting requirements, to ensure consistency in approach.

5. Enforcement

The proposed approach contemplates creating a series of new regulatory bodies, each with distinct roles and powers. These would be in addition to existing prosecutorial and judicial bodies, as well as others proposed in separate but complementary legislative proposals. The sheer number of new and newly empowered entities raises the possibility of both overlaps in authority and possible gaps in implementation.

Beyond these operational concerns, GNI is also worried that the proposed approach does not provide sufficient mechanisms for ensuring oversight and accountability of these bodies, including by democratically elected bodies like Parliament. As we set out in the policy brief, "[t]o the extent that substantial rulemaking authority and discretion is delegated to independent bodies, the scope of the regulator's duties and corresponding legal safeguards must be set out in primary legislation. States must create robust oversight and accountability mechanisms to ensure that those bodies act pursuant to the public interest and intervene in markets in a non-arbitrary way, consistent with the state's obligations." Transparency requirements, while laudable, are not likely to sufficiently safeguard against potential abuse or scope creep.

Of the new entities contemplated, the Digital Safety Commissioner appears to be the most formidable. The proposed approach would give significant powers to administer and enforce the proposed obligations, including a novel "complaints regime" focused exclusively on complaints of "non-compliance." While the proposal acknowledges the likelihood of complaints being received that are "trivial, frivolous, vexatious, made in bad faith," it provides no mechanism to punish or otherwise disincentivize such misuse. Without such measures, and combined with the significant penalties contemplated for non-compliance, we are concerned that this complaints mechanism could turn into a megaphone to amplify the impact of the "heckler's veto."

In addition, the proposal to empower the Commissioner to conduct inspections of OCSPs, including physically accessing "any place" or "any thing," at any time, for any reason (not to mention the contemplation of the possibility of the use of force in such inspections), is incredibly broad and inviting of abuse and should be significantly circumscribed. While audits can be a useful enforcement tool, these powers create the potential for overly intrusive and potentially coercive inspections, as well as a possible backdoor for unauthorized surveillance. There are ample examples of how such broad and unchecked authorities have been abused in other countries. In short, this aspect of the proposed approach would be an unnecessary and unfortunate precedent.

We welcome acknowledgement of the need for and resourcing of bodies such as the proposed Digital Recourse Council that can empower and educate users. The parallel "complaints regime"

set up to allow this Council to review and reverse content moderation decisions could also have some merit. While we appreciate any efforts to enhance access to remedy for individuals who feel their rights may have been violated, the proposed regime suffers from the same lack of consideration noted above about how to mitigate against abusive or inappropriate complaints. It is also important to ensure that individuals impacted by the Council's determinations will continue to have recourse to traditional judicial processes, where appropriate.

In addition, we welcome the possibility of establishing an "Advisory Board" to allow for diverse, non-governmental expert advice, but are confused by the lack of clarity in the proposal as to the specific functions contemplated for such a Board.

6. Changes to the Existing Legal Framework

The proposal also suggests modifying the existing legal framework for data retention and for authorities to access data in certain circumstances. The first would amend the Mandatory Reporting Act to require reports of child pornography by covered entities to include transmission data, as well as possibly basic subscriber information (BSI), without judicial authorization. GNI appreciates the importance of addressing internet child pornography and supports collaborative efforts to identify and remove such content. Because of the proactive and mandatory nature of this reporting, GNI has concerns about the extent to which such reporting may include false positives, and therefore the impact that requiring any additional personal identifying information could have on innocent users. Of the options under consideration (to require reporting of transmission data, or to also require BSI), the former would best serve the government's stated purposes of "expediting the police response," "while respecting freedom of expression, privacy protections, and the open exchange of ideas and debate online."

The proposal also contemplates amending the Canadian Security Intelligence Service Act to allow CSIS to access BSI information held by OSCPs "more quickly" in order to "investigate and mitigate the spread of violent extremist narratives that may inspire real-world acts of violence." Lowering the legal threshold and associated due process for intelligence services to access BSI could have result in significant privacy infringements and chilling effects on expression. History illustrates that the enforcement and associated impacts of such investigations often fall disproportionately on groups who hold dissenting views, minorities, and those who are least empowered to exercise and defend their rights. Before enacting any such authorities, the government should provide clear evidence of both why such new authorities are necessary, and what additional safeguards and oversight could be effective in mitigating such concerns (beyond existing review by the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians).

Finally, in order to avoid extraterritorial impacts and conflicts of law, any expansions of authority to compel production of transmission data or BSI should be focused clearly and narrowly on content that has an appropriate jurisdictional nexus to Canada.

Conclusion

The proposed approach puts forward a vast array of new obligations on OCSPs, new enforcement bodies, and new powers and authorities. While there is no doubt that new regulatory attention and approaches are needed, the burden is on the government to make a clear case for why so much is required to be implemented so quickly. Without further articulation of both the specific challenges that the government intends to address, and clear evidence for why the proposed changes are required and well-tailored to address those, the government risks creating confusion and unintended consequences at home. It also risks undermining the critical and well-deserved reputation and influence that it has on internet policy and governance abroad.

The GNI and its members are ready to continue to engage with the government on its concerns and to work constructively to shape proportionate and effective regulatory approaches that will strengthen freedom of expression and privacy in Canada, and provide a model truly worthy of emulation by other countries.