Overhauling the Online Harms Proposal in Canada: A Human Rights Approach

Yuan Stevens & Vivek Krishnamurthy

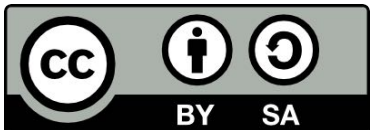
September 2021

cippic Samuelson-Glushko **Canadian Internet Policy and Public Interest Clinic**
Clinique d'Intérêt publique et de politique d'Internet du Canada Samuelson-Glushko

uOttawa

ABOUT CIPPIC

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) is Canada's first and only public interest technology law clinic. Based at the Centre for Law, Technology and Society at the University of Ottawa's Faculty of Law, our team of legal experts and law students works together to advance the public interest on critical law and technology issues including privacy, free expression, intellectual property, telecommunications policy, and data and algorithmic governance.



The authors wish to thank Tamir Israel for his feedback and input on this submission.

TABLE OF CONTENTS

INTRODUCTION: A NEW APPROACH IS NEEDED ____ *1*

THE DEFINITION OF SERVICE PROVIDERS IS IMPRECISE ____ *2*

Recommendations ____ 4

THE 24-HOUR BLOCKING REQUIREMENTS MUST BE SCRAPPED ____ *4*

Recommendations ____ 6

PROACTIVE CONTENT MONITORING AND FILTERING IS UNDEMOCRATIC ____ *6*

Recommendations ____ 8

MANDATORY REPORTING TO LAW ENFORCEMENT MUST BE NARROWED ____ *8*

Recommendations ____ 10

CONCLUSION ____ *11*

INTRODUCTION: A NEW APPROACH IS NEEDED

Canada has long been a champion of human rights, democratic values, and internet freedom.[1] Canada co-founded the Media Freedom Coalition, which advocates for media freedom online and offline,[2] and next year Canada will chair the Freedom Online Coalition.[3] Canadians pride themselves on supporting internet freedom, protecting free expression, and serving as a leader in the protection of the freedom of association and assembly online worldwide.[4]

In this context, the government's proposed legislation to regulate online harms seriously undermines claims that Canada is a leader in human rights. By raising the spectre of content filtering and website blocking, the current proposal threatens fundamental freedoms and the survival of a free and open internet in Canada and beyond. In an effort to combat hate speech and other ills, the proposed law threatens the free expression and privacy rights of the very equality-seeking communities that it seeks to protect.

The online harms proposal combines some of the worst elements of other laws around the world.[5] This is why CIPPIC believes that the Department of Canadian Heritage needs to overhaul its current approach to addressing the problems caused by unlawful online content. We are seriously concerned about numerous elements of the proposed law — such as the lack of adequate transparency requirements, the loosened requirements for the Canadian Security Intelligence Service (CSIS) to obtain basic subscriber information, the various jurisdictional issues raised by the law, and whether an administrative body like the Digital Recourse Council should be able to determine what speech is legal under Canadian law.

The feedback we provide is focused on other key areas of concern. First, we focus on the need for increased clarity regarding which services or platforms are covered by the law. Second, we explain why the proposed 24-hour blocking requirement needs to be scrapped. Third, we demonstrate why the proposed proactive monitoring requirements need to be reined in. Finally, we advocate against the general requirement to identify and funnel

---

[1] "Reports on United Nations human rights treaties" (23 December 2020), *Government of Canada*, online: https://www.canada.ca/en/canadian-heritage/services/canada-united-nations-system/reports-united-nations-treaties.html.

[2] "Media Freedom Coalition ministerial communiqué" (14 December 2020), *Government of Canada*, online: https://www.canada.ca/en/global-affairs/news/2020/11/media-freedom-coalition-ministerial-communique.html.

[3] "Freedom Online Coalition", *Freedom Online Coalition*, online: https://freedomonlinecoalition.com/.

[4] "Internet freedom" (5 November 2020), *Government of Canada*, online: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/internet_freedom-liberte_internet.aspx.

[5] "Have your say: The Government's proposed approach to address harmful content online" (29 July 2021), *Government of Canada: Canadian Heritage*, online: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html; Michael Geist, "Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation" (30 July 2021), *Michael Geist (blog)*, online: https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/; Daphne Keller, "Five Big Problems with Canada's Proposed Regulatory Framework for 'Harmful Online Content'" (31 August 2021), *Tech Policy Press*, online: https://techpolicy.press/five-big-problems-with-canadas-proposed-regulatory-framework-for-harmful-online-content.

profiling information to law enforcement about people's online activity, in view of the chilling effects this will have on people's online behaviour.[6]

Canada is well-positioned to maintain its role as a global human rights leader and advocate for maintaining an internet that is open and free to all. A first step to preserving our role as a leader in this space involves an overhaul of this proposed law so that it is consistent with our democratic values.

THE DEFINITION OF SERVICE PROVIDERS IS IMPRECISE

The proposal's definition of "online communication services" (OCSs) and "online communication service providers" (OCSPs) are imprecise and ill-suited to respond to the challenges posed by various kinds of unlawful online content.

Other countries have followed one of two options in defining to whom similar laws apply. Some countries' legislation goes broad and defines applicable services in a technologically neutral way, as has been done in Germany,[7] the EU,[8] and the US.[9] This approach involves crafting definitions that are malleable given technical developments. Others limit the scope to defined categories of service providers, as has been done in the UK[10] and Australia.[11] This approach involves setting out a taxonomy of services in light of the purposes they serve.

The government's proposal follows neither of these two dominant approaches. This is a problem as it renders the proposal's definitions of OCSs and OCSPs impermissibly vague. OCSs are defined as services accessible in Canada that have the "primary purpose" of allowing users of the service to "communicate with other users of the service, over the internet."[12] OCSPs are defined as "person[s] who provides an OCS."[13] With these definitions

---

[6] Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31:1 *Berkeley Tech LJ* 117, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

[7] *Act to Improve Enforcement of the Law in Social Networks*, 12 July 2017, § 2, 3 (2017) [NetzDG].

[8] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* [Directive on E-Commerce], at art. 1(2); *Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services* [Digital Services Act], at art. 1(1)(b).

[9] *Title 47 U.S. Code §230* – Protection for private blocking and screening of offensive material [Section 230]; *Digital Millennium Copyright Act*, Public Law 105-304, Oct. 28, 1998 [DMCA], at s. 512(k)(1)(A).

[10] *Draft Online Safety Bill*, (May 2021), online: https://www.gov.uk/government/publications/draft-online-safety-bill [Draft Online Safety Bill], at ss. 2 and 3.

[11] *Online Safety Act: An Act relating to online safety for Australians, and for other purposes*, No. 76, 2021, online: https://www.legislation.gov.au/Details/C2021A00076 [Online Safety Act], at ss. 13, 14, and 17.

[12] "Technical paper" (29 July 2021*), Government of Canada: Canadian Heritage*, online: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html at para 2. Excluded from this definition are services that "enable persons to engage only in private communications."

[13] *Ibid* at para 4. The term "person" here presumably captures legal persons such as corporations. OCSPs exclude telecommunications service providers defined in the *Telecommunications Act*. OCSPs also exclude a person who indicates the "existence or location of content or hosts or caches the content or information about the location of the content, by reason only that another person who uses their services to provide an OCS."

a huge swath of the internet could qualify as an OCSP — including forum-based websites, dating platforms, blogs or news outlets with comment sections, and much more.

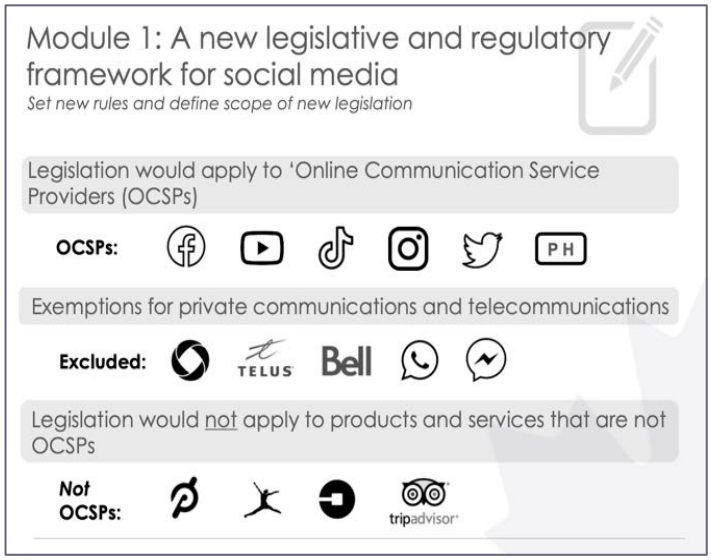


Figure 1: Slide 8 of Technical Discussion Paper presentation from Canadian Heritage officials

Canadian Heritage (PCH) officials attempted to clarify the meaning of these terms at an invite-only presentation delivered shortly after the announcement of the present consultation process.[14] According to the officials, the definition of OCSPs under the proposal would include social media platforms such as Facebook, Youtube, TikTok, Instagram, Twitter, as well as the website PornHub. Private communications and telecommunications service providers that would be exempt include Shaw, Telus, Bell, WhatsApp, and Facebook Messenger. The slide deck also describes how the definition of OCSPs would not capture the fitness streaming app Peloton, an app for tracking diet and exercise called MyFitnessPal, the rideshare app Uber, and travel review site TripAdvisor.

The views stated at the briefing may reflect the government's intent, but this is not reflected in the definition of the terms OCS and OCSP in the technical paper.[15] Take TripAdvisor as an example — a site which features user-generated reviews of hotels and restaurants. According to PCH officials, the proposed legislation would not apply to TripAdvisor because it is not an OCSP. Yet TripAdvisor's core functionality involves hosting user-generated reviews of travel businesses that everyone on the internet can read, and registered users can upvote and flag. This core functionality is similar in many ways to YouTube, except YouTube hosts videos, while TripAdvisor hosts travel reviews. If YouTube meets the definition of a service available in Canada that has the "primary purpose" of allowing users of the service to "communicate with other users of the service, over the internet," then so too does TripAdvisor.

Correspondingly, the definitions of OCSs and OCSPs need to be refined to reflect what the government means for them to say.

There is a further problem with the proposed definitions of OCSs and OCSPs, which is that they are not up to the task of dealing with the serious problem of non-consensual distribution of intimate images (NCDII) over the internet. While the proposed legislation would clearly apply to a site like PornHub, the legislation does nothing to address the problem of NCDII on the vast array of websites and online services that have been created

---

[14] "Technical Discussion Paper: Online Harms Legislation", (August 2021) *Minister of Canadian Heritage, Minister of Public Safety and Emergency Preparedness, and Minister of Justice and the Attorney General*.

[15] Indeed, it is inconsistent with rule of law principles for the public to have to rely on a slide deck distributed prior to an invite-only presentation to clarify the meaning of these terms.

to host such content, yet do not meet the statutory definition of an OCSP.[16] These difficulties point to the limitations of a "one size fits all" approach to addressing different kinds of online harms.[17]

Recommendations

- The statutory language needs to precisely define which service providers this law applies to, and which it does not.
- Canada should follow international best practices and scope the legislation either in a broad and technologically neutral fashion, or narrowly so that it applies to a small range of specified services. Exceptions such as services that facilitate private communication should be equally as clear.[18]

THE 24-HOUR BLOCKING REQUIREMENTS MUST BE SCRAPPED

The proposal's requirement that OCSPs block unlawful content within 24 hours of being notified that such content is available on their services should be scrapped, in view of the serious free expression concerns it raises. The proposed requirement is more heavy-handed even than Germany's controversial NetzDG law, given that the latter's 24-hour blocking requirement applies only to "manifestly" unlawful content.[19] NetzDG has served as a prototype for online censorship by authoritarian regimes around the globe,[20] and Canada

---

[16] See e.g., "'Revenge porn' site owner faces lengthy jail term" (6 April 2015), *BBC News*, online: https://www.bbc.com/news/technology-32194196; Adam May, "Meet the suburban mom who runs a revenge porn site" (12 December 2013), *Aljazeera America*, online: http://america.aljazeera.com/watch/shows/america-tonight/america-tonight-blog/2013/12/12/meet-the-suburbanmomwhorunsarevengepornsite.html.

[17] Cynthia Khoo, "Deplatforming Misogyny" (2021) Women's *Legal Action Fund*, online: https://www.leaf.ca/publication/deplatforming-misogyny/; Michael Geist, "'They Just Seemed Not to Listen to Any of Us' – Cynthia Khoo on the Canadian Government's Online Harms Consultation" (23 August 2021), *Law Bytes Podcast*, online: https://www.michaelgeist.ca/podcast/episode-99-they-just-seemed-not-to-listen-to-any-of-us-cynthia-khoo-on-the-canadian-governments-online-harms-consultation/.

[18] When it comes to private communications specifically, any definition provided must be crafted in a way that does not compromise or undermine encryption technology, which is used to ensure the security and privacy of communication and serves numerous other purposes in society. See Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide" (14 May 2018) *Citizen Lab at the Munk School of Global Affairs & Public Policy*, online: https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/.

[19] See e.g., Keller, *supra* note 5; "Germany: Flawed Social Media Law" (14 February 2018), *Human Rights Watch*, online: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law; "EU action needed: German NetzDG draft threatens freedom of expression" (23 May 2017), *EDRi*, online: https://edri.org/our-work/eu-action-needed-german-netzdg-draft-threatens-freedomofexpression.

[20] Jacob Mchangama and Joelle Fiss, "The Digital Berlin Wall: How Germany (Accidentally) Created a Proto-type for Global Online Censorship" (16 November 2019), Global Freedom of Expression, Columbia University, online: https://globalfreedomofexpression.columbia.edu/publications/the-digital-berlin-wall-how-germany-accidentally-created-a-prototype-for-global-online-censorship/.

places its long history of leadership in advocating for human rights at risk by following such an approach.

The proposal's draconian requirements are in sharp contrast to the immunity provided to service providers in the US for user-generated content,[21] and the requirement for "expeditious" removal of unlawful content in the UK[22] and the EU.[23] They may also be inconsistent with Canada's international obligations under Article 19.17 of the Canada-US-Mexico Agreement (CUSMA).[24]

Content moderation decisions are extremely difficult.[25] An enormous amount of content is uploaded daily to social media platforms, and the volume keeps growing as social media use increases.[26] Given the risk of massive fines of up to 5 percent of gross global revenues or $25 million, online service providers are likely to remove vast quantities of lawful content to avoid the risk of liability under the proposed legislation.[27]

Simply put, Canada's proposed 24-hour blocking requirement will lead to over-removal and censorship of legitimate expression.[28] This in turn will have deleterious effects on the rights of marginalized communities to speak online — as evidence shows that such content is erroneously removed by online platforms much more frequently than content from mainstream groups.[29] Automated decision-making systems used to detect hate speech and harmful content are also particularly known to be biased against the posts of marginalized communities, such as Black and other racialized people.[30]

---

[21] "Section 230 of the Communications Decency Act", *Electronic Frontier Foundation*, online: https://www.eff.org/issues/cda230.

[22] Draft Online Safety Bill, *supra* note 10 at. s. 9(3)(d).

[23] Directive on E-Commerce, *supra* note 8, at arts. 13 and 14; Digital Services Act, *supra* note 8, at arts. 4 and 5.

[24] Vivek Krishnamurthy and Jessica Fjeld, "CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States" (July 2020), *Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) and the Harvard Law School's Cyberlaw Clinic*, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3645462.

[25] Consider the takedown of the photo featuring the 'Napalm girl', which indicates that a balance must be found in moderation decisions between rights such as privacy and free expression. See Carmichael and Emily Laidlaw, "The Federal Government's Proposal to Address Online Harms: Explanation and Critique" (13 September 2021), *ABlawg.ca*.

[26] "Social Media Fact Sheet" (7 April 2021), *Pew Research Center*, online: https://www.pewresearch.org/internet/fact-sheet/social-media/; Sam Andrey et al, "Private Messages, Public Harms Disinformation and Online Harms on Private Messaging Platforms in Canada" (11 May 2021), *Cybersecure Policy Exchange*, online: https://www.cybersecurepolicy.ca/private-messages-public-harms.

[27] Technical paper, *supra* note 12 at para 119.

[28] Daphne Keller, *supra* note 5.

[29] See e.g., Kendra Albert et al, "FOSTA in a Legal Context" (2021) 52:3 *Columbia Human Rights LR* 1084, online: http://hrlr.law.columbia.edu/hrlr/fosta-in-legal-context/; Ángel Díaz and Laura Hecht-Felella, "Double Standards in Social Media Content Moderation" (4 August 2021), *The Brennan Center*, online: https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation.

[30] See e.g., Merlyna Lim and Ghadah Alrasheed, "Beyond a technical bug: Biased algorithms and moderation are censoring activists on social media" (16 May 2021), *The Conversation*, online: https://theconversation.com/beyond-a-technical-bug-biased-algorithms-and-moderation-are-censoring-activists-on-social-media-160669; Shirin Ghaffary, "The algorithms that detect hate speech online are biased

Whether private corporations should be responsible for striking the delicate balance between safety, privacy, and freedom of expression is worth scrutinizing.[31] To the extent that a government is privatizing this function by requiring platforms to determine whether content on their sites is illegal, the government should provide platforms with incentives to do so in a transparent and fair-minded fashion.[32] Unfortunately, the government's proposal fails in these regards.

Safeguards are needed that protect freedom of expression for all content removal decisions, including the ability to contest the removal of material. If the government wishes to require OCSPs to remove illegal content, a better alternative is to require them to do so expeditiously rather than setting a precise 24-hour limit.

Recommendations

- The 24-hour blocking requirement should be scrapped.
- If service providers are required to assess and block illegal content, a better approach is to provide for a general requirement to do so expeditiously.

PROACTIVE CONTENT MONITORING AND FILTERING IS UNDEMOCRATIC

CIPPIC views the proposed legislation's proactive monitoring and filtering requirements as fundamentally flawed. By requiring OCSPs to proactively monitor and filter content online, the Canadian government risks conscripting the private sector to engage in a form of dragnet surveillance that would have a chilling effect on people's communications and behaviour online, and pose risks to their privacy. Such a requirement has no place in Canadian legislation, especially in tandem with mandatory reporting to law enforcement.

The proposal requires OCSPs to take all reasonable measures, including through use of automated systems, to identify harmful content and make it inaccessible to people in Canada.[33] OCSPs could also be ordered by the proposed Digital Safety Commissioner to do

---

against black people" (15 August 2019), *Vox*, online: https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter.

[31] Jillian C. York, *Silicon Values: The Future of Free Speech Under Surveillance Capitalism*, (Brooklyn, NY: Verso Books, 2021); Kirsten Gollatz, Martin J. Riedl, and Jens Pohlmann, "Removals of online hate speech in numbers" (9 August 2018), *Alexander von Humboldt Institute for Internet and Society (HIIG)*, online: https://www.hiig.de/en/removals-of-online-hate-speech-numbers/.

[32] The Canadian government's proposal also falls short of the public reporting requirements set out in the NetzDG for platforms that receive more than 100 complaints per year, which was one of the few parts of the law that received the most universal support. Heidi Tworek and Paddy Leerssen, "An Analysis of Germany's NetzDG Law" (15 April 2019), *Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*, online: https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/NetzDG_TWG_Tworek_April_2019.pdf.

[33] Technical paper, *supra* note 12 at para 10.

"any act or thing necessary" to ensure compliance under the proposed law, including proactive monitoring.[34]

Requirements to proactively monitor and filter online content are tantamount to pre-publication censorship.[35] From a legal standpoint, obligating OCSPs to take all reasonable measures to identify content falling within the proposals' harm categories can effectively amount to a general monitoring obligation. While the technical paper indicates that nothing in the proposal would require or authorize an OCSP to seek out content falling outside the Act's five harm categories, in practice proactively discovering *any* harmful content requires monitoring *all* content.[36] General monitoring obligations are inherently intrusive and deeply disproportionate.

The legal requirement to proactively discover harmful content also violates Canada's trade obligations. Article 19.17 of the Canada-United States-Mexico Agreement (CUSMA) prohibits Canada from imposing liability on a platform as if it was the originator of illegal content.[37] Under the government's proposal, however, platforms will face steep penalties if they fail to proactively remove harmful content, in accordance with regulatory orders issued to secure compliance with the proposed Act's content identification and proactive removal obligations.[38] By making platforms directly responsible for assessing the legality of all user-generated content, the proposal treats platforms identically to content creators in violation of CUSMA.[39]

---

[34] *Ibid* at para 80.

[35] Carmichael and Laidlaw, *supra* note 25. The duty of care model may indeed be interpreted as enabling a proactive monitoring requirement in those countries.

[36] *Ibid* at para 9.

[37] Canada-United States-Mexico Agreement, 30 November 2018, online: https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/toc-tdm.aspx, at art. 19.17; Krishnamurthy and Fjeld, *supra* note 25.

[38] Technical paper, *supra* note 12 at paras 10, 80 and 94(a).

[39] CUSMA, *supra* note 25. We note that paragraph 4(c)(i) of Article 19.17 exempts measures taken to enforce criminal law. However, the online harm categories adopted in the proposal explicitly extend beyond criminally prohibited content (Technical Paper, *supra* note 12 at para 8).

For example, in outlining the parameters of child exploitation material, the proposal indicates that: "The concept … should capture … material … that may not constitute a criminal offence…". Similarly, the proposal does not rely on the Criminal Code definition of hate speech, but rather the broader regulatory definition which the Government intends to introduce in parallel amendments to the *Canadian Human Rights Act*. This definition modelled on the Supreme Court of Canada's guidance regarding the appropriate scope of regulation for hate speech in.a regulatory context, which is explicitly broader than the Criminal Code definition (see e.g., *Saskatchewan (Human Rights Commission) v Whatcott*, 2013 SCC 11, at para 105.

Beyond this explicit extension in the hate speech context, none of the content definitions adopted in the proposal include a mens rea requirement in their definition. For example, the proposed definition for non-consensually distributed intimate images encompasses content where "it is not possible to assess if a consent to the distribution was given by the person depicted in the image or video." While this definition is defensible in a regulatory context (see e.g., Emily Laidlaw et al, "Nonconsensual Disclosure of Intimate Images (NCDII) Tort" (August 2019), *Uniform Law Conference of Canada*), online: https://ulcc-chlc.ca/ULCC/media/EN-Uniform-Acts/Uniform-Non-consensual-Disclosure-of-Intimate-Images-Report-(2019).pdf), consent is central to the mens rea component of s. 162.1 of the *Criminal Code,* RSC 1985, c C-46. Correspondingly, this cannot fall within the exception in paragraph 4(c)(i) of Article 19.17. The proposal would additionally empower the government to define specific harmful content 'terms' through an Order-in-Council (Technical Paper, para 9).

The proactive monitoring requirement must also be considered in light of the proposed provisions requiring mandatory reporting of unlawful content to law enforcement. These monitoring and filtering requirements will have discriminatory impacts on marginalized and racialized communities, who already face barriers to engaging in the public sphere online.[40] The combination of these requirements is draconian and will further exacerbate the over-policing and surveillance of racialized communities online.

The government's proposal would make Canada an outlier in comparison to its global peers. There is no general obligation to monitor online content in Germany, the EU, and the US,[41] while Australia and the UK use a duty of care model.[42] Actual knowledge is required for any monitoring (and reporting) of child sexual exploitation material in the US[43] and for intermediary liability to attach in the EU.[44]

Recommendations

- There should be no general requirement to proactively monitor content, including across all types of regulated content.
- While the law need not prohibit voluntary proactive monitoring initiatives already in place, it must be explicit that it does not impose or authorize any legally binding proactive monitoring obligations at all.

MANDATORY REPORTING TO LAW ENFORCEMENT MUST BE NARROWED

CIPPIC has serious concerns about the government's proposed requirement that OCSPs report certain kinds of content to the RCMP and CSIS. Such mandatory reporting requirements, when combined with the proactive monitoring requirements detailed above, pose an unacceptable risk to the privacy rights of Canadians. Such measures should have no place in the laws of a free and democratic society. In any case, there needs to be actual

---

There is no obligation that the resulting definitions will respect baseline mens rea knowledge requirements inherent in the government's criminal law power.

Finally, we note that paragraph 4(c)(ii) of Article 19.17 of CUSMA also exempts "specific, lawful order(s) of a law enforcement authority" from the scope of its intermediary liability protections. However, compliance orders realizing a platform's general obligation to discover and remove all content falling within the proposal's harm categories are not 'specific' and, moreover, are inconsistent with Article 19.17 more broadly (see footnote 8 to that Article).

[40] Carmichael and Laidlaw, supra note 25; Khoo, supra note 17 at 200.

[41] NetzDG, *supra* note 7; E-Commerce Directive, *supra* note 8, at art. 15; Section 230, *supra* note 9.

[42] Online Safety Act, *supra* note 11; Draft Online Safety Bill, *supra* note 10. See also Carmichael and Laidlaw, *supra* note 25, who note that the duty of care model may indeed be interpreted as enabling a proactive monitoring requirement in those countries.

[43] 18 U.S. Code § 2258A – Reporting requirements of providers.

[44] E-Commerce Directive, *supra* note 8, at arts. 12-15.

knowledge of wrongdoing before service providers are required to notify law enforcement of illegal conduct.

The technical paper proposes significant changes to the current mandatory reporting regime for online service providers, which applies only to child sexual abuse material that a service provider discovers in the course of its operations. Part E of the government's proposal would require OCSPs to do one of the following:

- **Approach A**: Notify the RCMP when it has reasonable grounds to suspect that content falling within the 5 categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property;[45]
- **Approach B**: Report "prescribed information" in respect of "prescribed criminal offences" within the 5 categories of regulated harmful content to "prescribed" law enforcement officers or agencies.[46]

For Approach B, OCSPs would be required to report information to CSIS about terrorist content and content that incites violence — both of which are subject to the proposal's 24-hour removal requirement.[47] This approach would also require OCSPs to report to CSIS in secret if the disclosure "could be injurious to national security."[48] Under both approaches, the government will have the option of obligating OCSPs to include identification information — including the names and account identifiers of anyone implicated in the report.[49] Module 2 of the proposal would impose a similar customer identification obligation on ISPs such as Bell and TELUS with respect to child exploitation material.

The government's proposals are unprecedented among democratic nations. The only approach to mandatory reporting that resembles what is being proposed here are amendments to Germany's NetzDG in 2020, which requires service providers to report certain types of criminal content to federal law enforcement even before suspicion has been established.[50] The reporting requirements under the German law have been characterized as allowing "user data to be passed to law enforcement before it is clear any crime has been committed," and their constitutionality is being challenged in the German courts.[51] Yet Canada's proposal is even more extreme than the German proposal, in that the government will be empowered to force provision of identification information such as customer names and addresses.

---

[45] Technical paper, *supra* note 12 at para 20.

[46] Ibid.

[47] Ibid at para 22.

[48] Ibid at para 27.

[49] Technical paper, *supra* note 12 at para 32. While the government must take into account "the privacy interests engaged" by any information it mandates for disclosure, other elements of the Technical paper confirm that the government currently considers subscriber identification information to be fair game (see e.g., Module 2 of the Technical paper at para 8).

[50] Phillip Grüll, "German online hate speech reform criticised for allowing 'backdoor' data collection" (19 June 2020), *Euractiv*, online: https://www.euractiv.com/section/data-protection/news/german-online-hate-speech-reform-criticised-for-allowing-backdoor-data-collection/.

[51] "Google takes legal action over Germany's expanded hate-speech law" (27 July 2021), *Reuters*, online: https://www.reuters.com/technology/google-takes-legal-action-over-germanys-expanded-hate-speech-law-2021-07-27/.

The government's sweeping proposal far exceeds what is being considered in Australia and the United Kingdom. Proposals in those countries would obligate online harms regulators to report and disclose certain user activity to law enforcement if discovered during the course of their regulatory oversight activities.[52] Neither appears to contemplate an open-ended obligation to monitor all user content and report any user suspected of violating one of the proposal's harm categories to law enforcement or national security bodies. Similarly, reporting obligations currently imposed on service providers in the United States and on Canadian ISPs are limited to child exploitation material and, more importantly, do not include any open-ended content discoverability mandate.[53] An EU proposal is similarly limited, in that it would only require service providers to report instances where the platform discovers a serious crime that poses a threat to life but imposes no proactive monitoring requirement.[54]

While each of these proposals poses its own challenges and problems, the combination of proactive discovery and reporting obligations in the proposal effectively transforms Canada's service providers into an investigative tool for law enforcement and CSIS. This is especially so given that the identification and classification — and even reporting — processes are likely to be automated given the volume of content at issue.

Online service providers in Canada must not be turned into "suspicion databases."[55] As Carmichael and Laidlaw observe, some major service providers already engage in the first of the proposal's approaches on a voluntary basis.[56] The second approach laid out in the consultation paper is particularly worrying because it may capture a wide range of content and activity that is legal. By requiring platforms to feed data on their users to the RCMP and CSIS, the epidemic of surveillance and over-policing faced by marginalized and equality-seeking groups in Canada in the offline sphere will be extended online as well.[57]

Recommendations

- Reporting obligations should remain limited to child exploitation material.
- Reporting requirements must remain limited to content that service providers discover through the general course of providing their services. A reporting obligation cannot be combined with a proactive content discovery obligation.

---

[52] Online Safety Act, *supra* note 11 at s. 224; "Online Safety Bill Impact Assessment" (26 April 2021), *UK Department for Digital, Culture, Media and Sport*, online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985283/Draft_Online_Safety_Bill_-_Impact_Assessment_Web_Accessible.pdf at paras 205-206.

[53] United States, Sexual Exploitation and Other Abuse of Children, 18 USC 2258A; Canada, *Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service Act*, SC 2011, c 4, at s 2.

[54] Digital Services Act, *supra* note 8 at recital 48.

[55] Grüll, *supra* note 50.

[56] Carmichael and Laidlaw, *supra* note 25.

[57] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada" (1 September 2020) *Citizen Lab at the Munk School of Global Affairs & Public Policy*, online: https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/ at 3.

CONCLUSION

CIPPIC believes that the proposed legislation is fundamentally flawed. As Parliament reconvenes after the recent election, we call upon the new government to reconsider Canada's approach to online regulation. Rather than focusing just on online harms, the government should tackle platform regulation holistically — as is happening in the European Union with the introduction of the Digital Services Act and the Digital Markets Act in tandem.[58]

Online harms also cannot be legislated in isolation. There is a growing consensus that platform amplification of harmful material is a symptom of business models premised on surveillance capitalism[59] and the concentration of market power by technology companies.[60]

Canada needs to reconsider its approach to platform regulation from the ground up. We urge the Government of Canada to engage in significant study and consultation with experts and stakeholders in Canada and beyond. A comprehensive regulatory strategy is needed that aligns with efforts in like-minded countries, and that respects the global nature of the internet.[61]

A new approach that prioritizes the respect of human rights and internet freedom is needed. And the first step of that approach must be to set aside this proposal. Anything less will jeopardize Canada's claim to being a leader in advancing free expression, a free and open internet, and the human rights upon which our democratic society has been built.

---

[58] Digital Services act, *supra* note 8; "The Digital Markets Act: ensuring fair and open digital markets" (2019), *European Commission*, online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

[59] See e.g., Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* (New York, NY: PublicAffairs, 2019); Jillian C. York, *supra* note 29.

[60] Vas Bednar and Robin Shaban, "The State of Competition Policy in Canada: Towards an Agenda for Reform in a Digital Era" (21 April 2021), *Centre for Media, Technology and Democracy*, online: https://www.mediatechdemocracy.com/work/the-state-of-competition-policy-in-canada.

[61] See e.g., Ron Deibert, *Reset: Reclaiming the Internet for Civil Society,* (Toronto: House of Anansi, 202) at pp. 15-16.