To the Standing Committee on Justice and Human Rights,

We are pleased that Bill C-63 has moved to pre-study in Committee, *An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts.*

We agree with and uphold MP Virani's decision to split the Bill, prioritizing Section 1 and 4 to address online child sexual exploitation and abuse. Bill C-63 is a critical and long-awaited piece of legislation that will help ensure children, both in Canada and abroad, are protected offline and online, and that penalties for in-person and online offenders of child sexual abuse and exploitation are aligned.

Children in Canada and around the world are being abused and exploited online by Canadians. We need to ensure that actions taken by the federal government to protect Canadian children online extend to protecting children in other countries from Canadian perpetrators. Our perspective, as an international non-government organization, is informed by our work in the Philippines supporting local and international law enforcement to address cases of livestreamed child sexual abuse and exploitation perpetrated by people from around the world, including Canada.

In the past, we focused on protecting the physical spaces where children learn, grow and play. Today, we must prioritize online spaces and improve the mechanism to prevent, detect and report crimes of online child sexual abuse and exploitation.

International Justice Mission Canada (IJM) and IJM's Center to End the Online Sexual Exploitation of Children submit five recommendations for the Committee to consider as they study this important piece of legislation.

1. Ensure livestreaming child sexual abuse is specifically included in the legislation.
2. Take a preventive and safety by design approach.
3. Take into account victim and survivor voice when developing regulations.
4. Include offender deterrence in addition to protecting Canadian children.
5. Include private messaging and video-chat platforms and features.

International Justice Mission requests to present as a witness to expand on these recommendations and answer any questions the Committee may have.

We desire to see this legislation passed, believing it will have a global impact for the safety and protection of children.

Sincerely,

Anu George Canjanathoppil

Chief Executive Office, IJM Canada

INTERNATIONAL JUSTICE MISSION CANADA

IJM.ca PO Box 88031 RPO Levi Creek Mississauga, ON L5N 8M1 1.877.579.5030

International Justice Mission Submission On:

Bill C-63: Online Harms Act

International Justice Mission (IJM) welcomes this opportunity to provide a formal written consultation on Bill C-63, *An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts*. This submission is jointly prepared by IJM Canada and IJM's Center to End Online Sexual Exploitation of Children.

IJM commends the Honourable Arif Virani, Minister of Justice, for the years of detailed policy work and public consultation to create this bill. The *Online Harms Act* has the potential to strengthen the responsibility of technology companies to prevent child sexual abuse (CSA) and exploitation from happening on their platforms and to prevent the spread of child sexual exploitation material (CSEM) online.[1] If passed, Bill C-63 will position Canada as one of the leading countries in preventing online sexual exploitation of children, alongside its Five Eyes peers, Australia and the United Kingdom.

About IJM's Program to End Online Sexual Exploitation of Children

Since 2011, IJM has worked closely with all levels of the Philippine Government, international law enforcement, community service organisations, victims, survivor leaders, tech and financial sector companies, and other relevant stakeholders to combat online sexual exploitation of children (OSEC). In particular, IJM has supported combating the trafficking of children to produce and sell first-generation or new child sexual exploitation material, especially via livestreaming or live video in popular messaging and video chat apps. Live video child sexual abuse online is a live crime scene happening on tech platforms and apps. In 2022, IJM and the University of Nottingham Rights Lab conducted its Scale of Harm study which found that, in 2022 alone, nearly half a million Filipino children – 1 in 100 - were sexually abused to produce and sell new child sexual exploitation material.[2]

To date, IJM has supported 448 law enforcement operations, safeguarding 1,422 victims or at-risk individuals, leading to the arrest of 431 suspects and conviction of 255 offenders. Leveraging IJM Philippines' promising practices in combatting livestreamed child sexual

---

[1] The definitions for child sexual exploitation material (CSEM) and child sexual abuse material (CSAM) used in this paper come from the Terminology Guidelines for the Protection of Children from child sexual abuse and child sexual exploitation, pg. 39-40:

- The term "child sexual exploitation material" encompasses material that sexualises and is exploitative to the child although it is not explicitly depicting the sexual abuse of a child. It is a broader category that encompasses both material depicting child sexual abuse and other sexualised content depicting children.
- "Child sexual abuse material" describes a subset of "child sexual exploitation material" where there is actual abuse or a concentration on the anal or genital region of the child. Both terms refer to material that depicts and/or that documents acts that are sexually abusive and/or exploitative to a child.

The definition for child sexual abuse (CSA) comes from Action Canada for Sexual Health & Rights, while builds on the World Health Organization's definition:

- Child sexual abuse is the involvement of a child in sexual activity that s/he does not fully comprehend, give informed consent to, or for which s/he is not developmentally prepared and cannot give consent or that violates the laws or social taboos of society. It is evidenced by an activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, the activity being intended to gratify or satisfy the needs of the other person. It may include, but is not limited to, the inducement or coercion of a child to engage in any unlawful sexual activity, the exploitative use of a child in prostitution or other lawful sexual practices or the exploitative use of pornographic performances and materials.

Action Canada (n.d.) *Policy on Protection from Sexual Exploitation and Abuse, and Child Protection*. https://www.actioncanadashr.org/about/policy-protection-sexual-exploitation-and-abuse-and-child-protection.
World Health Organization and International Society for Prevention of Child Abuse and Neglect (2006) *Preventing child maltreatment: A guide to taking action and generating evidence*. Geneva, Switzerland. http://www.who.int/violence_injury_prevention/publications/violence/child_maltreatment.

[2] International Justice Mission and University of Nottingham Rights Lab (2022) *Scale of Harm*. *https://assets.ijm.app/IJM_Scale_of_Harm_2023_Full_Report_5f29259309.pdf*.

abuse, IJM's Center to End Online Sexual Exploitation of Children strengthens the global response to this crime. IJM partners with the Philippine Internet Crimes Against Children Center, a cooperation between Philippine and foreign law enforcement, including the Royal Canadian Mounted Police (RCMP).[3]

In November 2024, IJM was invited as a speaker to the Annual Provincial ICE Strategy conference hosted by the Ontario Provincial Police. IJM presented the Scale of Harm findings and data from the Philippines Anti-Money Laundering Council indicating that Canada has the fourth-highest volume of financial transactions to the Philippines suspicious for OSEC activity.[4] IJM made recommendations for an enhanced Canadian response to this crime type, resulting in conversations with law enforcement and prosecutorial personnel on addressing Canadian involvement in live video abuse.

Livestreamed Child Sexual Abuse in the Philippines

Livestreamed child sexual abuse is a particularly egregious form of online harm and online child sexual exploitation. Offenders around the world pay traffickers or "facilitators" to commit hands-on sexual abuse of often pre-pubescent children while the offenders direct and watch this abuse live online. The offenders, including Canadians, are not passive observers—they actively direct the assaults and rapes of specific children by typing directives in the chat or audibly on the video call. The offenders and traffickers work together to produce new child sexual abuse material (CSAM) that—because it is produced and transmitted in live video—often leaves very little digital trace for investigation. IJM cannot overstate this that these are "live crime scenes" committed daily on common, popular messaging and video-chat applications.[5] And moreover, technology exists to detect, disrupt, prevent and even report this type of abuse.[6]

While the Philippines is a hotspot, this crime type is not limited to the Philippines but is truly global. Cases have been reported with victims identified in the United States, Colombia, Brazil, Romania, Thailand, the United Kingdom, and elsewhere.[7]

---

[3] International Justice Mission (2022) *Philippine Internet Crimes Against Children Center (PICACC) marks its third year with more than 500 rescued.* https://www.ijm.org.ph/articles/philippine-internet-crimes-against-children-center-picacc-marks-its-third-year-with-more-than-500-rescued.

[4] Philippines Anti-Money Laundering Council, 2023
ONLINE SEXUAL ABUSE AND EXPLOITATION OF CHILDREN IN THE PHILIPPINES: An Evaluation Using STR Data
http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf.

[5] Suojellaan Lapsia, Protect Children (2024) Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://bd9606b6-40f8-4128-b03a-9282bdcfffof.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf.

[6] John Tanagho, "Child protection at our fingertips: What governments, corporations can do," FastCompany, https://www.fastcompany.com/91223353/child-protection-at-our-fingertips-what-governments-corporations-can-do.

[7] *See, e.g.*, Davis, Barney, "*Brit Jailed after Paying for Sexual Abuse of Children from All over the World*." The Independent. 26 January 2024, https://www.independent.co.uk/news/uk/crime/matthew-bower-fbi-nca-paedophile-kent-b2485430.html; INTERPOL, *"Columbia: Two arrested for live streaming child sex abuse."* 27 February 2023, https://www.interpol.int/en/News-and-Events/News/2023/Colombia-Two-arrested-for-live-streaming-child-sexual-abuse (reporting that police safeguarded three children aged 19 months, seven years, and nine years, and arrested their mother and aunt, who were accused of selling livestreamed child sexual abuse); INTERPOL. *"Brazil: Two Arrested in Global Hunt to Catch Child Predators."* 14 April 2021, https://www.interpol.int/en/News-and-Events/News/2021/Brazil-Two-arrested-in-global-hunt-to-catch-child-predators#:~:text=The%20coordinated%20police%20actions%20follow; Kessler, Ryan, "Sask. *Appeal Court Increases Sentence for Child Pornographer Philip Chicoine."* Global News. Updated 17 October 2019, https://globalnews.ca/news/6042218/appeal-court-increases-sentence-for-child-pornographer-philip-chicoine/; Clark, Tamara, *"Man Pleads Guilty to Seeking Violent Sex Abuse Images from Source in Thailand*." ABC News. 24 July 2023, https://www.abc.net.au/news/2023-07-24/arslan-safdar-guilty-in-sex-transmission-case/102641592; Elvin, Sian, *"Sex offender, 36, jailed for life for encouraging women to abuse children."* Metro. 15 August 2020, https://metro.co.uk/2020/08/15/sex-offender-36-jailed-life-encouraging-women-abuse-children-13132864/. According to Canada's National Financial Intelligence Unit, FINTRAC, the top 10 jurisdictions receiving money transfers from Canadians linked to online child sexual exploitation are: Philippines, Thailand, Colombia, the United States, Ghana, Ukraine, Dominican Republic, Romania, Jamaica, and Russia. *See* WeProtect Global Alliance. "Project Shadow." Last accessed 11 November 2024, https://www.weprotect.org/case-study/project-shadow/.

EUROPOL's latest Organized Crime Threat Assessment states that:

> "Live-distant child abuse (LDCA) is a persistent threat, where offenders watch child sexual abuse on demand with the support of one or more facilitators who perpetrate the abuse on the victim(s) in exchange* for payment. *It stands out as the main form of commercial sexual exploitation of children and as a major source of unknown** CSAM* using capping, which entails covertly recording the victim (i.e. in a video call/live-streaming session)."[8] (emphasis added)

CSEM can also be produced by perpetrators directly without the aid of a facilitator/trafficker. In these situations, an offender might groom children directly enticing them into "self-generated" CSEM of themselves.

The crime of livestreamed child sexual abuse requires urgent attention by tech platforms and the Canadian government. One study by the Philippine Anti-Money Laundering Council found that Canadians are the fourth top remitter of payments flagged by financial institutions in suspicious transactions reports for online sexual exploitation and abuse, in an 18-month reporting period from 2020 to 2022.[9] Notably, Canada has continually ranked fourth in this study since 2015.

CSEM livestreamed in video calls allow Canadian offenders to produce child sexual abuse material of children anywhere in real-time, with less digital evidence than image- or video-based CSEM distribution. Detection, reporting, and technological prevention of this type of online abuse is critical because the victims are being repeatedly abused "live." IJM's 2020 study of livestreamed child sexual abuse in the Philippines found that victims were abused on average for two years prior to intervention, in part because technology and financial sector companies failed to detect, disrupt, or report the crimes happening on and through their platforms.[10]

IJM RECOMMENDATIONS:

IJM Consultation on C-63: An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts

IJM commends the Canadian government for proposing C-63, a critical piece of legislation to improving child protection and deterring Canadians from abusing children online in Canada and around the world, especially in high-risk countries like the Philippines. The inclusion of livestreaming social media services, proposal for the development of a regulatory framework, and requirement to quickly remove CSEM from platforms are all needed elements to protect children across the globe.

---

[8] Europol (2024) *Internet Organised Thread Assessment (IOCTA) 2024,* page 24, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.

[9] Anti-Money Laundering Council (2023) *OSAEC in the Philippines: an evaluation using STR data*. http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf.

[10] International Justice Mission (2020) *Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society*. *https://www.ijm.ca/studies/summary-report-online-sexual-exploitation-of-children-in-the-philippines-analysis-and-recommendations-for-governments-industry-and-civil-society*.

Through IJM's casework experience and consultation with victims and survivors, IJM proposes several recommendations to further strengthen this legislation:

1. **Ensure livestreaming is specifically included in the legislation.**

In IJM's 13 years of combatting online sexual exploitation of children in the Philippines in partnership with the Philippine government, IJM has identified livestreamed child sexual exploitation to be a common form in which the abuse takes place. Traffickers abuse the children via livestream video at the direction of the western offender paying for the abuse. Unfortunately, Australia's eSafety Commissioner, pursuant to powers under their *Online Safety Act 2021,* has learned that very little is being done on platforms to detect, disrupt, or report child sexual exploitation via livestream video:

> "eSafety's understanding from their responses to the notice questions is that the providers are neither taking action to detect CSEA in livestreams (insofar as any of these could be regarded as livestreaming services) or taking action to detect CSEA in video calls or conferences." [11]

> "Live streaming is live video that can be created and watched on a service by end-users in real time."[12]

There should be no distinction made between live video child sexual abuse that is streamed publicly to broad audiences (i.e., Facebook live) or live video child sexual abuse that requires a unique link to a video conference platform (i.e., Microsoft Teams, Zoom) or a live video call (i.e., Microsoft Skype, WhatsApp). In every instance, CSAM is being produced and transmitted, and a child is being sexually abused and exploited using digital services and platforms in real-time. Companies should be required to address that.

Because perpetrators can abuse children with little fear of detection via livestream, IJM recommends the specific inclusion of livestreamed abuse in all definitions of C-63 – not only under "Interpretation and Application, for greater certainty – social media service". By naming livestreamed abuse throughout the Bill, future regulation will include livestreamed child sexual abuse in its framework and enable a nuanced approach to addressing this type of harm when making regulations and issuing guidelines and codes of conduct.

Specifically highlighting livestreamed child sexual abuse is critical, as research indicates that livestreaming offenders not only pose risks to abuse children online but also to abuse children in person both abroad and at home in Canada. A 2023 study by the Australian Institute of Criminology found that:

> "[V]iewing CSA live streaming is different to viewing CSAM. Wortley and Smallbone (2012) suggest that individuals who sexually offend against a child must first cross a psychological threshold. Arguably, CSA live streaming offenders have already done this, by directing and watching the live sexual abuse of a child online—which is on par with abusing the children themselves. This may partly explain why some CSA live

[11] Australian Government eSafety Commissioner (2023) *Basic Online Safety Expectations: Summary of industry responses to mandatory transparency notices. https://www.esafety.gov.au/sites/default/files/2022-12/BOSE transparency report Dec 2022.pdf*, at 15.

[12] Australian Government eSafety Commissioner (2024) Phase 1 Standards (Class 1A and 1B Material) https://www.esafety.gov.au/sites/default/files/2024-11/Phase1-Standards-Class1A-and-1B-Regulatory-Guidance-Nov2024.pdf?v=1732572256140, at 25.

> streaming offenders in the current study attempted to travel to offend against children in person."[13]

Conversely, failing to include "live video" in the Act sends a message to offenders that they can abuse children to produce and disseminate CSAM in live video with impunity and without fear of detection. Therefore, IJM recommends that under s. 2(1) in each instance under the definition for "content that sexually victimizes a child or revictimizes a survivor" where the definition includes "visual representation, written material or audio recording" to also include '*or live video*'. This is consistent with the Online Harms Act focus and the specific intent of s. 2(1) as live video is one form of a "visual representation" of a child engaged or depicted in explicit sexual activity.

IJM RECOMMENDATIONS

Current Section 2(1) text	Proposed Section 2(1) text
Content that sexually victimizes a child or revictimizes a survivor means (a) a visual representation that shows a child, or a person depicted as being a child, who is engaged in or depicted as being engaged in explicit sexual activity; (b) a visual representation that depicts the sexual organs or anal region of a child, if it is reasonable to suspect that the representation is created or communicated for a sexual purpose; (c) written material or an audio recording whose 10 dominant characteristic is the description, presentation or representation of explicit sexual activity with a child, if it is reasonable to suspect that the material or recording is created or communicated for a sexual purpose; (d) a visual representation, written material or an audio recording that shows, describes, presents or represents any of the following, if it is reasonable to suspect that the representation, material or recording is created or communicated for a sexual purpose:	Content that sexually victimizes a child or revictimizes a survivor means (a) a visual representation, including live video, that shows a child, or a person depicted as being a child, who is engaged in or depicted as being engaged in explicit sexual activity; (b) a visual representation, including live video, that depicts the sexual organs or anal region of a child, if it is reasonable to suspect that the representation is created or communicated for a sexual purpose; (c) written material or an audio recording whose 10 dominant characteristic is the description, presentation or representation of explicit sexual activity with a child, if it is reasonable to suspect that the material or recording is created or communicated for a sexual purpose; (d) a visual representation, written material, live video or an audio recording that shows, describes, presents or represents any of the following, if it is reasonable to suspect that the representation, material or recording is created or communicated for a sexual purpose:

[13] Coen Teunissien and Sarah Napier (2023) *The overlap between child sexual abuse live streaming, contact abuse and other forms of child exploitation*. No. 671. Australian Institute of Criminology. www.aic.gov.au/sites/default/files/2023-05/ti671_overlap_between_csa_live_streaming_contact_abuse_and_other_child_exploitation.pdf.

2. Take a preventative and safety by design approach

In an increasingly digital world, the safety of online spaces, especially for vulnerable populations like children, is critical. Canadian legislation aimed at enhancing the safety of tech platforms should adopt a preventative approach. Focusing on creating platforms that are safe by design, rather than merely reacting to incidents after they occur, can position Canada as a global leader in online safety. Online sexual exploitation of children is a growing crisis, with Justice & Care calling it an 'epidemic.'[14] By implementing stringent measures that require tech platforms to prioritize safety features from the outset, Canada can send a powerful message: the exploitation of children will not be tolerated, regardless of where it occurs.

Potential safety by design measures can include preventing the digital rendering of child sexual abuse material, including AI generated material, as well as prevent the upload or distribution of both new and previously identified CSEM.

Consider including provisions requiring companies to invest in developing and eventually deploying preventative technologies so child sexual abuse material can never be streamed, uploaded or distributed online. Both Australia's eSafety Commissioner and the United Kingdom's Ofcom are working closely with safety tech companies to understand what is possible in terms of safety technology deployment. While there are a number of prevention technologies in existence, the following are a few examples:

- The social livestreaming platform, Yubo, proactively screens live video to keep children safe online, implementing automated prompts to users to change behaviour and disabling violative livestreams.[15]
- Safety technology company, SafeToNet, has created a real-time video and image threat detection technology, HarmBlock, capable of determining whether visual data represents undesirable and illegal content such as pornography, sexually suggestive imagery, cartoon pornography, and/or CSEM. [16] The machine-learning algorithm will hash images with harmful content and render the content harmless. SafeToNet can provide more information to the Canadian government upon request.
- Safer, built by Thorn, scales CSAM detection, increases content moderation efficiency, and optimizes detection using advanced AI technology. [17] It identifies known and first-generation CSAM, leveraging cryptographic, perpetual hashing and machine learning algorithms to detect CSAM at scale and disrupt its viral spread.
- DragonflAI is a prevention and disruption tool that moderates livestreams completely on-device before they are streamed to platform. [18] It detects indecent content such as CSEM and prevents content from being uploaded.

The 2023 WeProtect Global Alliance *Global Threat Assessment* further articulates this point by noting:

---

[14] Justice & Care, Dublin City University, De La Salle University (2024) *Facilitation of Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines*. https://justiceandcare.org/policies-and-reports/facilitation-of-online-sexual-abuse-and-exploitation-of-children-osaec-in-the-philippines/.

[15] Yubo (n.d.) https://www.yubo.live/safety/safety-tools ("We **monitor all livestreams**, through first-of-its-kind video and audio moderation to detect inappropriate behaviour, and intervene in real-time when we see our Community Guidelines being broken").

[16] SafeToNet (n.d.) https://safetonet.com/harmblock.

[17] Safer (n.d.) https://safer.io/.

[18] DragonflAI (n.d.) https://www.dragonflai.co/.

> "It is technically possible to detect child sexual exploitation and abuse in end-to-end encrypted environments in a privacy- and security-preserving way. Proposed solutions include:
>
> - Client-side scanning, which involves scanning messages on devices for matches or similarities to a database of illegal child sexual abuse material before the message is encrypted and sent).
> - Homomorphic encryption. This is the use of a different type of encryption which allows operations to be performed without data decryption at any point).
> - Intermediate secure enclaves, which decrypt the message at server level by a third party and use tools to detect child sexual abuse materials."[19]

We can deploy safety technology to detect, disrupt, and prevent child sexual abuse in a sustainable and privacy preserving fashion. We urge you to consider this as Canadian Parliament determines paths forward to prevent online sexual exploitation. Consider this statement from an individual with lived experience and member of the survivor advocacy group, the Philippine Survivor Network:

"I envision a community where we can speak freely and draw safety from each other.

Safety is not just about being safe in our physical environment but also in our daily interactions online. How are we ensuring the safety of our children and survivors in an online environment? Online sexual exploitation of children is a global problem that needs global solutions. The solution involves not just the country where the victim lives but also in places where online predators live and drive demand.

What we really lack now is the support from the community and government. It is impossible to end child sexual abuse online without whole society solutions. The community needs to be engaged and demonstrate what accountability means by stopping the crime of exploiting children."

More than "Just Survivors" by Ruby*[20]

Consider amending Part 1, 7 (1):

Current text	Proposed text
'Nothing shall require an operator to proactively search content on a regulated service that it operates in order to identify harmful content.'	'Nothing shall require an operator to proactively search content on a regulated service that it operates in order to identify harmful content, unless that content sexually victimizes a child or revictimizes a survivor.'

[19] WeProtect Global Alliance (2023) *Global Threat Assessment*. https://www.weprotect.org/global-threat-assessment-23/#full-report.
[20] Ruby (2023) *More than Just Survivors*. https://www.weprotect.org/blog/more-than-just-survivors/.
*a pseudonym has been used to protect Ruby's identity. Her legal name is on file with IJM.

3. Take into account victim and survivor voice when developing regulations

Canada has the opportunity to be a world leader in hearing victim and survivor voices when building its regulatory framework. Survivor leader Ruby*--who experienced livestreamed child sexual abuse firsthand—says that:

> "Survivor's voices only become meaningful when their ideas and voices impact material things, like legislation, policies and products. Survivor inclusion adds so much credibility when their experiences are heard."[21]

Victims and survivors bring lived-experience, expertise and credibility that regulators, legislators, civil society, government, and NGOs need to build a safer internet.

Consider amending General Provisions, section 27:

Current text	Proposed text
When making regulations and issuing guidelines, codes of conduct and other documents, the Commission must take into account (a) freedom of expression; (b) equality rights; (c) privacy rights; (d) the needs and perspectives of the Indigenous peoples of Canada; and (e) any other factor that the Commission considers relevant.	When making regulations and issuing guidelines, codes of conduct and other documents, the Commission must take into account (a) freedom of expression; (b) equality rights; (c) privacy rights; (d) the needs and perspectives of the Indigenous peoples of Canada; (e) the experiences and needs identified by victims and survivors of online harms; and (f) any other factor that the Commission considers relevant.

IJM advises the government to intentionally seek insights and recommendations from Canadian victims and survivors of online child sexual abuse as well as victims and survivors from other countries who have been abused online by a Canadian or individual from another G7 country. IJM Canada is able to facilitate an introduction to members of the Philippine Survivor Network who have made recommendations on similar legislation in the United Kingdom, Germany, United States and Australia.

4. Include offender deterrence in addition to protecting Canadian children

Canadians are not only victims of online harms; they are also perpetrators of the crime. Alongside photos and recorded videos, CSEM is increasingly being produced and distributed live by Canadians. In the Philippines, Canada is among the top four countries with remittances flagged as suspicious transactions for online sexual exploitation and abuse of children.[22] Children globally are being targeted, groomed and exploited online by Canadians and other offenders online.

Creating standards and requirements for online service providers to not only protect users but also to ensure the safe use of their platforms to protect vulnerable non-user groups—

[21] Ibid.
[22] Anti-Money Laundering Council (2023) *OSAEC in the Philippines: an evaluation using STR data*. http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf.

such as children—is consistent with globally accepted expertise and recommendations by multi-stakeholder experts. For instance, the World Economic Forum Global Coalition for Digital Safety, comprised of experts from leading tech companies, non-government organizations, and governments recommends that:

> "Online platforms can also be evaluated based on their processes, tools and rules designed to promote the "safe use" of their services in a manner that mitigates harm to vulnerable non-user groups."[23]

The provisions setting out the purposes of the Act and mandate of the Commission in sections 9(a), 9(e), and 11 can be strengthened by adding prevention and deterrence language around Canadian offenders.

Current text	Proposed text
9(a) Promote the online safety of persons in Canada	9(a) Promote the online safety of persons in Canada. 9(b) Disrupt and prevent Canadians from abusing children in Canada and globally
9(e) Reduce harms caused to persons in Canada	9(e) Reduce harms caused to and by persons in Canada
11 The Commission's mandate is to promote online safety in Canada and contribute to the reduction of harms caused to persons in Canada as a result of harmful content online by, among other things…	11 The Commission's mandate is to promote online safety in Canada and contribute to the reduction of harms caused to and by persons in Canada as a result of harmful content online by, among other things…

5. Include private messaging platforms and features.

Most grooming and new CSEM, including livestreams, occur on private messaging and video chat platforms. Bill C-63 specifically excludes private messaging platforms or private messaging features within public platforms. For the Canadian government to most effectively address the exponential increase of child sexual abuse and exploitation online, including CSEM, private messaging and video chat platforms should be within scope of Bill C-63.

Victims, survivors, NGOs and government agencies agree that CSEM must be prevented, reported and removed from both public and private platforms. In Australia, the government has included 'one-to-one live aural communications' in their Online Safety Act and specifically called out Australia as a major consumer of child sexual abuse in their regulatory guidance on the Basic Online Safety Expectations.[24] The eSafety Commissioner has also included questions on livestreaming to video-chat and messaging platforms in their non-periodic transparency notices to tech companies operating in Australia.

Data and the lived experience of victims and survivors prove the scale of harm inflicted on private platforms. Survey data released by *Protect Children* in February 2024 revealed that 37% of CSEM viewers first established contact with a child via a messaging app, mostly via

[23] World Economic Forum. (2024). *Making a Difference: How to Measure Digital Safety Effectively to Reduce Risks Online*, p. 20. https://www.weforum.org/publications/making-a-difference-how-to-measure-digital-safety-effectively-to-reduce-risks-online/

[24] Australian Government eSafety Commissioner (2023) *Basic Online Safety Expectations Regulatory Guidance*. https://www.esafety.gov.au/sites/default/files/2023-09/Basic-Online-Safety-Expectations-RegulatoryGuidance-updated-September-2023_0.pdf.

end-to-end encrypted messaging apps like Telegram (45%) and WhatsApp (41%). The next most mentioned apps include Signal (28%), WickrMe (25%), Session (21%), Viber (16%), and Wire (12%). Other platforms mentioned by respondents include Discord, Omegle, Snapchat, and Likee.[25]

Including private messaging platforms and features in the scope of Bill C-63 ensures the $37M estimated for fiscal years 2024-2026 of the Digital Safety Commission will address all CSEM.[26] CSEM creation, production, and dissemination on platforms with private communication channels must also be addressed. This expansion in scope has also been recommended by the Canadian Centre for Child Protection.[27] Introducing a Bill that only regulates public platforms will increase the amount of exploitation taking place on private platforms, continuing to leave millions of children in Canada and globally vulnerable to ongoing and future sexual abuse and exploitation.

IJM is available to provide subsequent consultation and act as a witness before Parliament to share its expertise in addressing child sexual abuse and exploitation online, including the production and dissemination of new CSEM in livestreaming.

Lorianne Dueck Rebello, Advocacy and Public Engagement
Ldueck@ijm.ca +1 343-262-9040
International Justice Mission Canada

About IJM Canada

International Justice Mission Canada (IJM) is part of a global organisation that protects people in poverty from violence. As the largest anti-slavery organisation in the world, IJM partners with local authorities in 29 program offices in 17 countries to combat modern slavery, violence against women and children, and other forms of abuse against people who are poor. IJM program offices work with local authorities and governments to rescue and restore survivors, hold perpetrators accountable, and help strengthen public justice systems so they can better protect people from violence. IJM Canada supports this mandate through advocacy, fundraising and community engagement.

Learn more about IJM Canada at ijm.ca and on LinkedIn. For more information, email Lorianne Dueck Rebello, Advocacy and Public Engagement Ldueck@ijm.ca.

About IJM's Center to End Online Sexual Exploitation of Children

IJM's Center to End Online Sexual Exploitation of Children protects children in the Philippines and scales the fight against this crime globally. The Center leverages and shares effective practices and models from IJM's Philippines program to enhance justice system and private sector responses to online sexual exploitation, resulting in sustainable child protection and offender accountability. *Learn more about the Center's work at ijm.org.ph/center and on LinkedIn. For more information, email endosec@ijm.org.*

---

[25] Suojellaan Lapsia, Protect Children (2024) *Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry*. https://bd9606b6-40f8-4128-b03a-9282bdcfffof.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf.

[26] Zachary Vrhovsek (2024) *The Online Harms Act: Establishment of a Digital Safety Commission, Ombudsperson and Office*. Office of the Parliamentary Budget Officer. https://www.pbo-dpb.ca/en/publications/LEG-2425-008-M--online-harms-act-establishment-digital-safety-commission-ombudsperson-office--loi-prejudices-ligne-etablissement-commission-ombudsman-bureau-securite-numerique#:~:text=The%20PBO%20estimates%20that%20from,the%20Commission%2C%20Ombudsperson%20and%20Office.

[27] Canadian Centre for Child Protection (2024) *Exclusion of private messaging features from proposed Online Harms Act leaves substantial threat to children unaddressed*. https://protectchildren.ca/en/press-and-media/blog/2024/online-harms-bill-messaging.