Submission: Consultation on an Exposure Draft *Online Safety Bill 2020*

International Justice Mission welcomes the opportunity to provide comments on the *Online Safety Bill* exposure draft. We applaud the leadership taken by the Australian government on this vital issue and look forward to continuing discussion to ensure appropriate and considered legislation that both provides protection from online exploitation for all Australians and prevents Australians from committing online harms.

About International Justice Mission

International Justice Mission (IJM) is a global organisation that protects people in poverty from violence. IJM partners with local authorities in 21 program offices in 14 countries to combat slavery, violence against women and children, and police abuse of power against people who are poor. IJM works to rescue and restore victims, hold perpetrators accountable, and help strengthen public justice systems.

Since 2011, IJM has partnered with the Philippines Government, international law enforcement and NGOs to combat online sexual exploitation of children, in particular the trafficking of children by adults to create new child sexual exploitation materials, including via livestream video, for paying sex offenders. As of October 2020, IJM has supported dedicated law enforcement partners in the Philippines in 210 operations, leading to the rescue of 687 victims or at-risk individuals, the arrest of 263 suspected traffickers and the conviction of 94 perpetrators.

In 2020, IJM expanded our programming by launching IJM's Center to End Online Sexual Exploitation of Children. The Center partners with governments, industries, NGOs, and other stakeholders to expose, neutralize, and deter online sexual exploitation of children around the world. Leveraging practices proven effective in IJM's ongoing program against online sexual exploitation of children in the Philippines, the Center helps (1) improve technology and financial sector detection and reporting of livestreaming child sexual exploitation, (2) strengthen international collaboration in law enforcement and prosecution, and (3) support effective justice system (law enforcement, prosecution, and aftercare) responses in source and demand-side countries, resulting in sustainable protection for children and accountability for perpetrators.

The Center to End Online Sexual Exploitation of Children has contributed to the recommendations and comments below is and is available to provide further consultation to the Australian Government about the online sexual exploitation of children and recommendations to combat it.

Executive Summary

IJM agrees that despite the myriad of benefits the proliferation of internet connectivity has brought around the world, the internet also poses a dark and very real threat to children in the form of online exploitation. This appalling reality that exists on the internet takes shape in a multitude of ways, whether it is grooming, the sharing of child sexual exploitation material

(CSEM), or cyber-bullying, but none is nearly as destructive, dark and challenging to combat as the **trafficking of children** for the purpose of **livestreamed** sexual abuse at the direction of a remote sex offender.

IJM commends the Australian government's efforts over the years to combat online sexual exploitation of children. We welcome the new offences that specifically address this crime and the stronger penalties introduced by the *Crimes Legislation Amendment (Sexual Crimes Against Children and Community Protection Measures) Act 2020* as important steps in addressing demand for online sexual exploitation of children in Australia.[1] Along with the existing punitive measures to deter and hold perpetrators accountable for such crimes, greater effort is needed for *proactive detection of online abuses as they are happening* in order to protect children from continued and future online sexual exploitation. The Online Safety Bill, in regulating the digital industry's responsibility vis-à-vis the use of their platforms for online harms, should also address and define the instrumental role technology companies must play in preventing the trafficking of children through online sexual exploitation.

Our comments on the Online Safety Bill will primarily address this aspect of online harms.

Recommendation 1: Create a statutory "duty of care" for platforms and include specific provisions for the eSafety Commissioner to require providers to take *proactive* steps to detect and report in real-time to appropriate authorities the online sexual exploitation of children, especially in livestreaming and CSEM production.

Recommendation 2a: Include in the Online Safety Bill a requirement for annual transparency reports by technology companies (*i.e.* ESPs, social media services and messaging apps) on the tools they are using to detect OSEC and relevant data on livestreaming child sexual exploitation and new CSEM detected on their platform.

Recommendation 2b: Civil penalties should apply to enforce compliance with the transparency reporting requirement.

Recommendation 3: Require industry codes and industry standards to incorporate procedures and practices that implement the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*.[2]

Recommendation 4: Require technology companies to provide transparent reporting on livestreaming and production of new CSEM according to geographic locations of abuse.

Strengths of the Online Safety Bill

The establishment of the eSafety Commissioner in 2015 has shown to be an effective framework in streamlining the Australian government's response and action on various forms of online abuses, including the online sexual exploitation of children. The clarity that comes with having a designated Commissioner for these matters allows for a stronger, unified approach from the government of Australia.

[1] Summary.Crimes-Legislation-Amendment-Bill.24jun2020.pdf (ijm.org.au)

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/870623/11_Voluntary_principles_-_formal_letter__1_.pdf

Schemes to Address Harmful Online Material

The enhanced powers of the eSafety Commissioner across the schemes for cyberbullying, adult cyberabuse, intimate image-abuse, harmful online content schemes, and blocking measures for terrorist and extreme violent material online are vitally important to ensure the removal of harmful and illegal content online. IJM welcomes these measures, particularly around the reduced times for the removal of material to 24 hours, the ability for the eSafety Commissioner to issue take-down notices under the online content scheme irrespective of whether the content is hosted in or outside Australia, and the system of infringement notices, enforceable undertakings, and injunctions, and civil penalty provisions to enforce compliance with take-down or blocking notices.

We also welcome the Government's recognition of the myriad of ways in which search aggregator, distribution and broadcasting services help the spread of harmful online material. The powers of the Commissioner to issue link deletion notices and app removal notices to ancillary service providers, such as search engines and app stores, and the enforceable penalties for non-compliance will enhance the ability to disrupt access to services that provide a means to host harmful online material.

Basic Online Safety Expectations (BOSE)

The framework for establishing an enhanced and cohesive set of Basic Online Safety Expectations and new powers to require service providers to report on their compliance with upholding these expectations represent a strong step in defining shared responsibilities for protecting children from sexual abuse online. A common issue for Electronic Service Providers (ESPs) is not having clear guidance from governments on minimum standards for detecting and reporting online sexual exploitation of children, particularly with ESPs who have a global reach. Establishing and enhancing the BOSE parameters allow for a clear framework of reporting standards and expectations to be communicated.

Opportunities to Further Strengthen the Bill

Protecting Children from Livestreamed Sexual Abuse

The robust scheme for addressing pre-existing harmful and illegal content online needs to be complemented by measures to address online harms which happen in real time, in particular the trafficking of children to create new CSEM. The Online Safety Bill can be strengthened by defining the responsibility of electronic service providers to help *detect* and *disrupt* the global crime of the trafficking of children to create new CSEM, specifically in the form of livestreamed child sexual abuse in developing countries such as the Philippines at the direction of demand-side offenders in Australia.

The livestreaming of child sexual exploitation and abuse is complex because it allows offenders to engage in child sexual abuse production in real-time while leaving limited evidence. Remote adult offenders take an active role in creating the visual display of child sexual abuse and exploitation by directing the actions of the trafficker and exploited children, whilst the acts are streamed live. In some cases, a livestream is captured and distributed. The trafficking of children online and the proliferation of livestreamed child sexual exploitation are subsets of online sexual exploitation of children generally.

Detecting this form of online abuse is critical because the victims are young children in situations of human trafficking and slavery, being repeatedly abused "live" to create new CSEM, satisfying the financial greed of traffickers and the deviant sexual interests of demand-side offenders. Major ESPs with livestreaming functionality typically do not monitor such data streams for possible CSEM. Because the livestream does not, by nature, result in a stored image or video file – the most commonly detected indicators of internet crimes against children – detection methods in common use do not typically recognise livestreaming sexual exploitation of children. This results in the majority of instances remaining unreported. The evidence that does exist is often spread across different platforms including social media apps, MTAs, and computers/mobile devices, making it difficult for ESPs, law enforcement, and others to identify when this crime occurs.

IJM's study of livestreamed online sexual exploitation of children in the Philippines (OSEC Study), released in May 2020, found that **victims were abused on average for two years prior to intervention**,[3] in large part because technology and financial sector companies failed to detect in real-time the crimes happening on and through their platforms. The digital industry can and should play a vital role in *preventing* online services and platforms from being used to facilitate online child exploitation. Increasing detection and reporting requirements on ESPs, internet service providers, social media companies, and financial institutions allows for law enforcement to rescue children from exploitation more quickly and prevent more children from ever being exploited through early detection of online offenders.

Restraining Australians that Pose an Online Threat to Vulnerable Children

While it is imperative for the government of Australia to take action to *protect* vulnerable Australian children online, it is also vital that the government takes action to *identify and restrain* Australians that pose an online threat to vulnerable children around the world.

The evidence that many Australians pose an online threat to children is undeniable.

- IJM's OSEC Study found that Australians accounted for nearly 1 in 5 of offenders who directed and paid for livestreamed exploitation of children in the Philippines.[4]
- The Australian Federal Police and the Australian Center to Counter Child Exploitation (ACCCE) have observed the emergence of child abuse forums established as a result of COVID-19 stay-at-home measures[5]. Moreover, they learned about child sexual abuse sites crashing during the pandemic due to the increased volume of traffic.[6]
- In April, May and June 2020, reports to the ACCCE increased by 122% compared to the same period last year.[7]
- In 2016, Queensland Police Taskforce Argos arrested Australian national, I. Turner. Their investigation of Turner found that he was purchasing CSEM, including live-stream videos, originating from the Philippines. After referring the case to the Philippines' authorities and subsequent arrest of the local Filipina trafficker, evidence was discovered that another Australian, M. Baden was also funding the trafficking of these children online through purchasing livestreams and CSEM from the Filipina

[3] https://www.ijm.org/documents/studies/Final_OSEC-Public-Summary_05_20_2020.pdf, p. 11
[4] https://www.ijm.org/documents/studies/Final_OSEC-Public-Summary_05_20_2020.pdf, p. 13.
[5] https://www.afp.gov.au/news-media/media-releases/predators-exploiting-kids-online-during-virus-second-wave; see also IJM's COVID-19 OSEC Brief, https://osec.ijm.org/news/wp-content/uploads/2020/09/2020-10-IJM-COVID-19-Brief-on-Online-Sexual-Exploitation-of-Children.pdf
[6] https://www.abc.net.au/news/2020-05-20/afp-concerned-by-child-exploitation-spike-amid-coronavirus/12265544
[7] https://www.afp.gov.au/news-media/media-releases/predators-exploiting-kids-online-during-virus-second-wave

trafficker. Both Turner and Baden were sentenced to prison for these crimes—but due to slow detection, they abused Filipino children online for years.[8]

- A study by the Australian Institute of Criminology found that 256 Australians spent more than **$1.3 million** over 13 years to commission and watch livestreamed child sexual abuse of Filipino children.[9] This does not include the live streamed sexual abuse of children from any other country, including within Australia; nor is this a comprehensive total from the Philippines but rather a snapshot of 256 *identified* offenders.

Furthermore, these online predators often do not only exploit children online. **Demand-side offenders of online sexual exploitation of children often pose an active threat to children in their physical proximity, not limiting their abuse to online interactions**.[10] For instance, IJM's OSEC Study found that 9% of the online sex offenders identified in law enforcement case files were known to have traveled to the Philippines to abuse children in-person.[11] A Swedish report showed that 48% of persons convicted of possession of child sexual abuse material had also been convicted of other types of child sexual abuse.[12] Further, an Australian study found possible escalation—when the offenders were involved in networking—from passive participation, to the production of CSEM, and to contact sexual offending against children.[13] Thus, increasing detection of livestreamed sexual exploitation protects children from being abused in source countries like the Philippines, but also acts to protect Australian children from the risk of being abused by these same offenders in-person.

Recommendations

1. Statutory Duty of Care and Proactive Detection and Reporting Requirement

Recommendation 1: Create a statutory "duty of care" for platforms and include specific provisions for the eSafety Commissioner to require providers to take *proactive* steps to detect and report in real-time to appropriate authorities the online sexual exploitation of children, especially in livestreaming and CSEM production.

Early detection will allow law enforcement to identify and disrupt offenders much sooner before they abuse children online for years. Offenders should not operate with impunity for years on social media and livestreaming platforms before being discovered and investigated.

---

[8] International Justice Mission, 'Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society', (Report, 5 May 2020), https://www.ijm.org/documents/Final-Public-Full-Report-5_20_2020.pdf

[9] Rick Brown, et al., '*Australians who view live streaming of child sexual abuse: An analysis of financial transactions*', (Research paper, No. 589 in *Trends and issues in crime and criminal justice*, Australian Institute of Criminology, 19 February 2020); see also, Matthew Doran, *'256 Australians spend more than $1.3million watching child sexual abuse online'*, ABC Live Blog (online), 19 February 2020. <https://www.abc.net.au/news/2020-02-19/australians-paying-to-watch-child-sex-abuse-online/11979844>.

[10] https://www.ijmuk.org/documents/IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children-Composite-Case-Review-Analysis-and-Recommendations-for-the.pdf, p. 35.

[11] https://www.ijm.org/documents/Final-Public-Full-Report-5_20_2020.pdf, p. 12.

[12] Research project which targets potential perpetrators - World Childhood Foundation

[13] Virtual Global Taskforce, 'Online Child Sexual Exploitation: Environmental Scan Unclassified Version 2019' 2019-Virtual-Global-Taskforce-Environmental-Scan_Unclassi.pdf, p. 17

2. Transparency Reporting

Recommendation 2a: Include in the Online Safety Bill a requirement for annual transparency reports by technology companies (i.e. ESPs, social media services and messaging apps) on the tools they are using to detect online sexual exploitation of children and relevant data on livestreaming child sexual exploitation and new CSEM detected on their platform.

This requirement would be analogous to the provision requiring annual reporting from companies on slavery in their supply chains under the *Modern Slavery Act 2018*, and should require the technology sector to report on how their platforms are being abused to sexually exploit children and what steps, if any, they take to detect and report it. Australian consumers and the public deserve to know what platforms children are trafficked on to create new CSEM/via livestreaming the most so they can exercise their voice and influence as consumers.

Recommendation 2b: Civil penalties should apply to enforce compliance with the transparency reporting requirement.

3. Industry Codes and Industry Standards

Recommendation 3: Require industry codes and industry standards to incorporate procedures and practices that implement the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*.[14]

The *Voluntary Principles to Counter Online Child Sexual Exploitation and* Abuse, developed by the governments of Australia, UK, US, Canada and New Zealand in close consultation with leading technology companies and civil society, establishes a base-line framework for companies that provide digital services to protect children online. In particular, Principle 5 addresses livestreaming child exploitation:

> Principle 5: Companies seek to identify and combat the use of livestreaming services for the purpose of child sexual exploitation and abuse, take appropriate action under their terms of service and report to appropriate authorities.

Examples of procedures and practices that could form part of an industry code or standard for relevant sections of the online industry include:[15]

- Use safety by design measures to make predatory offender-child interactions less likely and to deter offenders from these interactions.
- Proactively identify, through language or behaviours, individuals engaging in criminal predatory behaviour such as sexual communication with a child.
- Ensure search results do not surface child sexual exploitation and abuse and seek to prevent automatic suggestions for such activity and material.
- Develop in-house or integrate third-party tools that are able to identify - based on previously seen characteristics - the language, behaviour (such as suspicious financial activity) or imagery indicative of child sexual exploitation and abuse in livestreamed content or the user interactions around it.
- Stop a livestream as soon as CSEM activity or a vulnerable child is identified. Capture any information necessary to help identify the child.

---

[14] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/870623/11_Voluntary_principles_-_formal_letter__1_.pdf

[15] Examples from UK Home Office, *Interim Code of Practice on Online Child Sexual Exploitation and Abuse*, p.15 Interim code of practice on child sexual exploitation and abuse (publishing.service.gov.uk)

- Take steps to disrupt the use of livestreaming services by adults to broadcast contact abuse to other offenders, including in return for money.
- Close accounts involved in child sexual exploitation and abuse and take steps to prevent individuals re-registering under different details.

4. Support Prevalence Measurements

There is a dearth of data on the prevalence or scale of the trafficking of children to create new CSEM or via livestreaming. As a result, many developing countries may fail to allocate proper resources to their justice system response to protect children. To support the gathering of relevant country data, companies should be required to report on hotspot geographic locations of abuse, whether in Australia or internationally. For instance, a popular social media platform detects the production and sharing of new CSEM from countries X and Y at a much higher rate than other countries and reports the number of such instances. Such transparency reporting would be immensely helpful to NGOs and source-side governments seeking to protect children from abuse, while also helping the Australian Government make international development decisions to strengthen justice systems in hotspot source countries for livestreaming online sexual exploitation of children.

Recommendation 4: Require technology companies to provide transparent reporting on livestreaming and production of new CSEM according to geographic locations of abuse.

Conclusion

In order to effectively combat the growing crime of online sexual exploitation of children, restrain Australian demand-side offenders, and protect vulnerable children in Australia and around the world, ESPs, social media companies, and financial institutions **must detect the crimes happening on their platforms in real-time.** The framework within the Online Safety Act, with the increased power of the eSafety Commissioner to enforce BOSE, industry codes and industry standards on these entities should be utilised to articulate the responsibility of technology companies to proactively detect and prevent online services and platforms from being used to facilitate the online sexual exploitation and abuse of children.