**IJM Submission On:**

***Parliamentary Inquiry into Law Enforcement Capabilities in Relation to Child Exploitation***

July 7, 2023

Thank you for the opportunity to provide a submission to the Parliamentary Joint Committee on Law Enforcement inquiry into Law Enforcement Capabilities in relation to Child Exploitation.

International Justice Mission[1] (IJM) is a global organisation that protects people in poverty from violence. We partner with local authorities in 29 program offices in 17 countries to combat slavery, violence against women and children, and other forms of abuse against people living in poverty. IJM works with local authorities and governments to safeguard and restore survivors, hold perpetrators accountable, and help strengthen public justice systems so they can better protect people from violence.

Since 2011, IJM has worked with the Philippine Government, international law enforcement, and relevant stakeholders to combat online sexual exploitation of children (OSEC), in particular, the trafficking of children to produce new child sexual exploitation material (CSEM) especially via livestreaming video. To date, IJM has supported 338 law enforcement-led operations, leading to the safeguarding of 1,123 victims or at-risk individuals, the arrest of 355 suspected traffickers, and the conviction of 195 perpetrators. Leveraging IJM Philippines' promising practices in combatting livestreaming of child sexual abuse and exploitation, IJM's Center to End Online Sexual Exploitation of Children[2] works to strengthen the global response against this crime, including via improved industry detection and reporting. The Center is available for consultation to industry, government, and NGOs.

Our submission addresses the following points in the Terms of Reference (TOR) of the inquiry, as they pertain to particular forms of online child exploitation: the production of new child sexual exploitation material, especially via real-time live video ("livestreamed child sexual abuse"):

a. Trends and changes in relation to the crime of online child exploitation;

c. Streamlining legislative constraints to enable faster investigations that can better respond to rapidly evolving trends in offending;

e. Considering the role technology providers have in assisting law enforcement agencies combat child exploitation, including but not limited to the policies of social media providers and the classification of material on streaming services; and

f. Considering the link between accessing online child abuse material and contact offending, and the current state of research into and understanding of that link.

[1] https://www.ijm.org/
[2] https://www.linkedin.com/company/ijmendosec/

## (a) Trends and changes in relation to the crime of online child exploitation

### *Livestreamed child sexual abuse is an egregious form of online child exploitation*

Online child sexual exploitation has many different forms, including creating, possessing or distributing previously produced Child Sexual Exploitation Material (CSEM), enticing children to "self-produce" new CSEM, grooming children for later contact abuse, and more. One severe trend in relation to online child exploitation is *livestreaming* of child sexual abuse and exploitation whereby adults produce new child sexual exploitation material for paying sex offenders around the world. This crime involves the real-time sexual abuse of a child by a third party, directed by the remote offender, who often specifies the type of abuse they wish to see. It is perpetrated through common, popular messaging and video-chat applications used for video calls.

Livestreamed child sexual abuse is a pervasive crime, with untold numbers of children across the globe facing this form of exploitation. While no country is immune to this crime, the Philippines is believed to be the epicentre of this form of online sexual exploitation.[3] In the Philippines, IJM[4] partners with the Philippine Government and other stakeholders to protect children from traffickers who create child sexual exploitation materials (CSEM)—livestreamed, videos, and photos—to satisfy online demand of paying sex offenders who often direct the abuse from their homes. 84% of the time, traffickers are relatives of the children being exploited, the very people who are supposed to protect them (IJM 2020)[5].

### *Livestreamed child sexual abuse is a growing global crime*

Livestreaming child sexual abuse cases have also recently been identified across dozens of countries, including Romania,[6] Ghana,[7] and Thailand.[8] Australian children are also victims of child sexual abuse production and distribution via livestreaming. According to the Australian Center to Counter Child Exploitation (ACCCE), "Australian children as young as eight are being coerced into performing live-streamed sexual acts by online predators, who often record and share the videos on the dark net and sexually extort victims into producing even more graphic content."[9]

Offenders who pay for the livestreamed abuse of children often come from Western countries, such as US, UK, EU, Australia, Germany and Canada. *IJM's 2020 study*[10] found that Australia is in the top 3 countries of livestreamed CSEM customers, with 18% of livestreamed child sexual exploitation cases in the Philippines being initiated by Australia-based offenders. A study by the Australian Institute of Criminology (AIC) found that 256 Australians spent

[3] https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines; https://www.austrac.gov.au/sites/default/files/2022-12/2022%20AUSTRAC%20Child%20Sexual%20Exploitation%20Financial%20Crime%20Guide.pdf

[4] http://ijm.org.ph

[5] https://ijmstoragelive.blob.core.windows.net/ijmna/documents/Final-Public-Full-Report-5_20_2020.pdf

[6] https://www.independent.co.uk/news/uk/crime/paedophiles-philippines-romania-national-crime-agency-b2112832.html

[7] https://www.nationalcrimeagency.gov.uk/news/registered-sex-offender-paid-to-watch-live-streamed-child-abuse

[8] DISRUPTING HARM IN THAILAND: Evidence on online child sexual exploitation and abuse, available at https://www.end-violence.org/sites/default/files/2022-02/DH_Thailand_ONLINE_final.pdf, p. 58 ("The victimisation of children via video calls is a common form of OCSEA, according to [the Thailand Internet Crimes Against Children task force] TICAC, and live-streaming of CSEA has appeared in the caseload of DSI. In addition, one foreign law enforcement agency notes that Thailand accounts for 5% of its total reports to date on live-streamed CSEA.")

[9] AFP warn about fast growing online child abuse trend, Sept. 2021, https://www.afp.gov.au/news-media/media-releases/afp-warn-about-fast-growing-online-child-abuse-trend

[10] https://ijmstoragelive.blob.core.windows.net/ijmna/documents/Final-Public-Full-Report-5_20_2020.pdf

AUD$1.3 million to view live streaming child sexual abuse from the Philippines over a 13-year period. This amount was spent over 2,714 separate payments.[11] According to the AFP, 29.3% of rescues and 35.5% of arrests made in the Philippines between February 2019 and July 2022 have been a direct result of an AFP referral, pointing to a significant proportion of Australian offenders.[12]

This crime is a global phenomenon and requires a global response from every nation. This response must be against both demand-side offenders (typically from wealthier countries, including Australia, who commission, pay for, and direct CSEM production) and financially motivated traffickers (often in low- to middle-income countries, who sexually abuse children for profit). Europol warns that 'livestreaming of child sexual abuse increased and became even more popular during the COVID-19 pandemic,' (Europol 2021[13]). This rise in threat, in part due to global increase in internet usage and access, indicates that all countries need to widen and strengthen their child protection laws. Similarly, INTERPOL[14] notes that "Live-streaming of child sexual exploitation for payment has seen an increase in recent years," as demand surged during the pandemic as an alternative to 'in-person' abuse.

### *Nature and extent of abuse*

Not only is livestreamed CSAM growing, but it contains some of the worst child sexual abuse acts. Internet Watch Foundation (IWF) research on child sex abuse livestreaming reveals 98% of victims are 13 or under.[15] Forty percent of the livestream captures or recordings were classified by IWF as containing 'serious' sexual abuse, *with 18 percent involving the rape and sexual torture of children*. This is consistent with IJM's on-the-ground casework experience in the Philippines. In the over 330 cases IJM has worked on, the livestreamed abuse suffered by children at the behest of Australian and other offenders who watch on video calls is rarely limited to erotic displays: it usually includes forcible sexual penetration constituting rape in most jurisdictions. Children are forced to engage in sex acts with other children, sexually abused by an adult, and sometimes harmed in other degrading ways, such as in bestiality. IJM social workers and lawyers have journeyed with hundreds of survivors as they pursued healing and justice from these traumatic harms perpetrated both in person and online.

Survivors have spoken out about the devastating impact of the abuse perpetuated against them with the following words:

> "A lot of young people have been abused and many of them commit suicide because of what happened to them. It's not just mental health, it affects the child's background. It also affected their family life. We don't want children to experience this – especially our future children. Its effects are grave and our recovery was not easy."[16]

[11] Brown R. Napier S & Smith R 2020. "Australians who view live streaming of child sexual abuse: an analysis of financial transactions." *Trends & issues in crime and criminal justice* no. 589. Canberra: Australian Institute of Criminology https://www.aic.gov.au/sites/default/files/2020-05/ti589_australians_who_view_live_streaming_of_child_sexual_abuse.pdf

[12] https://www.afp.gov.au/news-media/media-releases/adelaide-man-jailed-and-15-young-victims-rescued-after-international-child

[13] https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[14] https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-Secretary-General-Online-child-sexual-abuse-at-record-levels

[15] *See* https://www.iwf.org.uk/news-media/news/iwf-research-on-child-sex-abuse-live-streaming-reveals-98-of-victims-are-13-or-under/; Internet Watch Foundation 2018. Trends in child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse. Cambridge, UK: Internet Watch Foundation. https:// www.iwf.org.uk/resources/research

[16] https://www.ijmuk.org/stories/survivor-letter-to-uk-government-online-safety-bill

### *Challenges in responding to livestreamed child sexual abuse*

While the creation, possession, and distribution of these materials are criminal offences, there is currently very little detection or disruption of these livestreaming offences. Because the livestream does not, by nature, result in a stored image or video file – the most commonly detected indicators of online child sexual exploitation offences – detection methods in common use do not typically recognise livestreamed sexual exploitation of children. This results in the majority of instances remaining unreported. The report of the eSafety Commissioner's first non-periodic reporting notices issued to 7 online service providers revealed that none of the major tech companies questioned were taking any action to detect abuse in live video streams or calls.[17] To quote the report, "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."

This creates considerable challenges for law enforcement investigations and prosecutions to hold offenders accountable for their crimes. With the majority of instances going undetected, law enforcement is hampered in their ability to enforce the law, allowing offenders in demand side countries - often from Western countries like Australia, the US, UK, EU, and Canada – to enjoy impunity for creating, possessing, or distributing child sexual exploitation material.

IJM, through its collaborative efforts with local authorities to combat commercial sexual exploitation of children in the Philippines, demonstrated the deterrent impact of holding offenders accountable for their crimes. In 2016, IJM conducted studies[18] to measure the prevalence of the children sold for sex in bars and brothels in select cities in the Philippines. These externally validated studies found 72% reduction of child sex trafficking in Metro Cebu, 75% reduction in Manila, and 86% in Pampanga. It affirms that when laws are consistently enforced, children are protected.

## (c) Streamlining legislative constraints to enable faster investigations that can better respond to rapidly evolving trends in offending

A common constraint identified by law enforcement for timely investigations of online child abuse offences is the response times to obtain information from electronic service providers and foreign agencies. As outlined by the Victoria Police Force in their submission[19], Page 6, TOR C:

> "The following inefficiencies and time delays are experienced by Victoria Police investigators. Addressing these issues would enable faster investigations, resulting in better community safety outcomes including limiting harm to children and identifying victims and offenders sooner:
>
> • The response times from ISPs to requests from Victoria Police investigators currently range from weeks to months. A timelier response from ISPs would greatly assist Victoria Police to conduct investigations more quickly. Likewise, the timeliness of responses from overseas technology providers such as Facebook, to law enforcement agency requests can vary, which can delay the identification/location of offenders and/or victims. However, Victoria Police acknowledges that these response

[17] https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf
[18] https://www.ijmuk.org/documents/studies/philippines-csec-program-evaluation.pdf
[19] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/ChildExploitation/Submissions, Victoria Police Force, Page 6, TOR C

> times should be reduced from late 2022 with the implementation of the CLOUD Act (USA)."

NSW Police Force shared in their submission[20], Page 7, 2.24 :

> "24. Previously, the NSWPF CEIU was able to access IP addresses via Homeland Security Investigation (HSI) services, however this process has been replaced by the Mutual Legal Assistance Treaty (MLAT). The MLAT is utilised to acquire IP information from overseas countries. Requests can take months or, in some instances, years before a response is received. This can lead to prosecutions being abandoned. Another issue on the MLAT process is that in order for International Service Providers to provide an IP address, they need to be assured that the risk is within their "home" country."

Current legislation pertaining to the provision of information by electronic service providers to law enforcement is not helpful in ensuring a timely response. Provisions under the *Telecommunications Act*[21] and the *Telecommunications (Interception and Access) Act*[22] provide guidance on when service providers can, or are required, to disclose information to law enforcement authorities, but there is no obligation to comply with any particular disclosure authorisation within a certain period of time. Section 474.25[23] of the Criminal Code Act, 1995 (Cth) sets out the obligations of internet service providers and internet content hosts to refer details of any suspected child abuse material to the AFP "within a reasonable time after becoming aware of the existence of" the CSAM; but with no guidance as to what constitutes a "reasonable time."

Existing legislation should be reviewed to determine whether the obligation on electronic service providers to promptly respond to law enforcement requests for information should be strengthened. The establishment of *minimum standards* – either through legislation, subsidiary legislation or other means - that streamline reporting and responses by electronic service providers can provide the much-needed support to law enforcement to conduct investigations in a timely manner. Such minimum standards for electronic service providers can include response times to law enforcement and information sharing requirements, both of which can support investigative speeds. In establishing appropriate response times, guidance can be taken from time frames set out for the digital industry to comply with similar obligations – such as the 24-hour time for digital service providers to comply with notices issued by the eSafety Commissioner for removal of CSAM, link deletion or app removal under the *Online Safety Act*.[24]

Removing investigative delays can safeguard victims and remove them from situations of ongoing abuse and harm. IJM's study found that in cases of livestreamed child abuse in the

---

[20] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/ChildExploitation/Submissions, NSW Police Force, Page 7, 2.24

[21] *Telecommunications Act 1997* (Cth), sections 280, 313, 317E http://classic.austlii.edu.au/au/legis/cth/consol_act/ta1997214/

[22] *Telecommunications (Interception and Access) Act 1979* (Cth), section 178 https://www.legislation.gov.au/Details/C2023C00005

[23] Criminal Code Act 1995 (Cth) https://www.legislation.gov.au/Details/C2022C00324

**474.25 Obligations of internet service providers and internet content hosts**

A person commits an offence if the person:

(a) is an internet service provider or an internet content host; and

(b) is aware that the service provided by the person can be used to access particular material that the person has reasonable grounds to believe is child abuse material; and

(c) does not refer details of the material to the Australian Federal Police within a reasonable time after becoming aware of the existence of the material.

Penalty: 800 penalty units.

[24] See *Online Safety Act 2021*, sections 110, 124 and 128. https://www.legislation.gov.au/Details/C2022C00052

Philippines, victims were often abused for an average of two years[25] before they are safeguarded.

**We recommend that a legislative review be undertaken of existing obligations on electronic service providers to respond to law enforcement requests for information in a timely manner and that minimum standard timelines be established setting out the time frames within which internet service providers and electronic service providers would be required to respond to law enforcement requests.**

## (e) Role of technology providers in assisting law enforcement agencies to combat child exploitation

IJM's experience working on livestreamed child sexual abuse, as well as other research[26] indicates that livestreaming of child sexual abuse occurs via open web popular video chat platforms that Australians use every day and are operated by the largest multinational tech companies. Those companies that provide the platforms where online child abuse is carried out have a responsibility to prevent and disrupt offending and remove and report abusive material.

Currently, law enforcement globally is overwhelmed with the volume of reports received regarding child sexual abuse and exploitation. In 2022, the US-based National Center for Missing & Exploited Children received more than 32 million reports globally, over 99.5% of which are regarded as incidents of suspected CSAM (NCMEC 2023[27]). For example, the volume of CyberTipline reports in each country consistently outpace law enforcement capacity to review and investigate each individual report.

More responsibility should be placed on the digital industry to address this problem. Technology providers collectively possess both the financial and technological capabilities to prevent and deter this crime by making their platforms safer by design.

### *1) Technology companies must proactively prevent and disrupt CSEM:*

Electronic service providers can implement preventative technology that halts child sexual abuse material (whether photo, video or livestreamed child abuse) from ever being uploaded to a platform's server. Through preventative technology implementation, law enforcement capacity would increase simply by decreasing the volume of reports.

The following are some examples of currently available preventative technological tools:

- The UK-based NGO, Internet Watch Foundation (IWF[28]) partnered with digital forensics company Cyacomb to create an innovative tool that can **block** known images and videos of CSAM from being uploaded within end-to-end encrypted (E2EE) platforms, while still respecting user privacy. Another such preventative technology already in existence is SafeToNet's product, SafeToWatch[29]. This is a real-time video &

[25] https://ijmstoragelive.blob.core.windows.net/ijmna/documents/Final_OSEC-Public-Summary_05_20_2020.pdf
[26] Napier S., Teunissen C., & Boxall H. 2021 "Live streaming of child sexual abuse: An analysis of offender chat logs", *Trends & issues in crime and criminal justice* no. 639. Canberra: Australian Institute of Criminology https://www.aic.gov.au/sites/default/files/2021-10/ti639_live_streaming_of_child_sexual_abuse.pdf
[27] https://www.missingkids.org/cybertiplinedata
[28] https://annualreport2022.iwf.org.uk/tech-rd/our-role-in-the-safety-tech-challenge/
[29] https://safetonet.com/safetowatch/

image threat detection technology, capable of determining whether visual data represents undesirable and illegal content such as pornography, sexually suggestive imagery, cartoon pornography, and/or CSAM. The machine-learning algorithm can trigger several possible actions, such as obscuring harmful images, disabling image capture/recording/transmission, displaying a warning messages, etc.

Because solutions like SafeToWatch detect, disrupt, and prevent the creation and distribution of CSAM at the device level, blocked content would never reach a platform's servers, where discovery would trigger mandatory reporting obligations. Therefore, this strategy serves to reduce reporting to law enforcement through prevention. Law enforcement globally, including in Australia, is overwhelmed by the number of reports received, and the majority of countries cannot review each report. A preventative tool such as SafeToWatch can lead to increased prevention of image creation and distribution, reducing the number of reports received by law enforcement agencies.

### *2) Technology companies must invest in new technological tools*

Electronic service providers should be required to make ongoing investments in technological tools that prevent, detect and disrupt CSAM – in particular new material and livestreamed child abuse. These measures are critical in order to keep abreast of continually evolving technologies and the scale of online harm and the sophistication of offenders when perpetuating such harm. Such a requirement for ongoing investment in technological tools forms part of the *Social Media Services Online Safety Code,*[30] recently registered by the eSafety Commissioner, as well as a requirement to implement systems, processes and/or technologies that aim to detect and remove CSAM from the service.

For further discussion of current and emerging technological tools to prevent, detect and deter CSAM, see IJM's Submission on the draft Online Safety Industry Codes and Submission on the Revised draft Online Safety Industry Codes.[31]

### *3) Improve quality of reports to law enforcement*

Electronic service providers can support law enforcement by improving the quality of the content of their reporting. Currently, most tech companies provide insufficient information in their reports for law enforcement to conduct an investigation, leaving children vulnerable to further victimisation and offenders free from accountability. For example, technology companies fail to provide port information along with IP addresses in CyperTipline reports. If port information was provided with IP addresses, this would greatly help law enforcement determine which device is the actual suspect device.

Digital service providers should be required to provide sufficiently detailed reports to law enforcement to allow them to make effective use of the information, including any associated information that might help identify offenders and victims in a timely manner.

---

[30] Social Media Services Online Safety Code (Class 1A and Class 1B Material). https://www.esafety.gov.au/sites/default/files/2023-06/Schedule-1%E2%80%93Social-Media-Services-Online-Safety-Code-%28Class-1A-and-Class-1B-Material%29.pdf

We anticipate that similar provisions would be included in the Industry Standards being developed by eSafety for the two industry sections Designated Internet Services (eg. file storage platforms) and the Relevant Electronic Services (eg. messaging apps, including encrypted platforms) whose draft codes were refused registration

[31] https://onlinesafety.org.au/wp-content/uploads/wpforms/31-9e10405917e4c106ebe4ec5e69a7bc86/IJM-Online-Industry-Codes-Submission-Sept2022-fbb2fc2b31ab7278c4d829640acb7bf2.pdf ; https://onlinesafety.org.au/wp-content/uploads/wpforms/31-9e10405917e4c106ebe4ec5e69a7bc86/IJM-Industry-Codes-v2.0-Submission.23032023-60ec5b1af7a7be5e693d02efd6054577.pdf

**We recommend the establishment of minimum standards of response quality that require tech companies to promptly respond to law enforcement requests for information of detection, including relevant usernames, IP addresses, account profile URLs, and relevant chat or image content.**

## (f) Link between accessing online child abuse material and contact offending

Recent research by the Australian Institute of Criminology[32] reveals important connections between online sexual exploitation of children and contact offending.

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

Additional research by Finnish NGO, Protect Children[33] has been conducted by anonymously surveying offenders of online sexual exploitation.

> "CSAM use endangers not only the children depicted in the abuse material: many CSAM users try to contact a child online. Establishing contact with a child may result in further offences: CSAM users can try to lure the child to an in-person meeting or manipulate them into live-streaming or producing sexual images or videos."
>
> "52% of users have felt afraid that viewing CSAM might lead to sexual acts against a child
>
> 44% of users have thought about seeking direct contact with a child online after watching CSAM
>
> 37% of users have sought direct contact with a child online after watching CSAM"

This research, along with that of other organisations indicates that there is a direct link between online offending and contact offending. Beyond perpetrators attempting to contact offend, children are often still facing in-person abuse by a trafficker, even if the online abuse is directed on the other side of the world. In addition, there is continued victimisation of the depicted children when the CSAM continues to be shared online, even after the trafficker has been arrested and the child has been rescued. CSAM offenders regularly share files with one another for years or even decades after the creation of the CSAM. A person who causes the creation of one CSAM image is contributing to the unstoppable flow of CSAM worldwide.

IJM is available for further consultation and would be pleased to provide more information or respond to any questions relating to online child exploitation to assist the Committee.

[32] https://www.aic.gov.au/sites/default/files/2023-05/ti671_overlap_between_csa_live_streaming_contact_abuse_and_other_child_exploitation.pdf
[33] https://www.suojellaanlapsia.fi/en/post/redirection-blog04-not-just-viewers

## Contact:

**John Tanagho**
*Executive Director*
**IJM's Center to End Online Sexual Exploitation of Children**
LinkedIn| ijm.org.ph/Center

**Hiroko Sawai**
*Analyst, Advocacy Research*
**IJM Australia**
hsawai@ijm.org.au | IJM.org.au