International Justice Mission Submission On:

Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

Since 2011, International Justice Mission (IJM) has worked closely with the Philippine Government, international law enforcement, community service organisations, survivor leaders, and other stakeholders to combat online sexual exploitation of children (OSEC), including the trafficking of children to produce new child sexual exploitation material (CSEM) via live video streams. This form of child sexual abuse online is a live crime scene happening on tech platforms and facilitated via payments on international money service businesses and other financial institutions.

As of May 2024, IJM has supported 400 law enforcement operations, safeguarding over 1,300 victims or at-risk individuals, leading to the arrest of 400 suspects and conviction of 231 offenders in the Philippines. IJM is part of the Philippine Internet Crimes Against Children Center, a cooperation between Philippine and foreign law enforcement. Leveraging IJM Philippines' promising practices in combatting these crimes, IJM's Center to End Online Sexual Exploitation of Children strengthens the global response.

Livestreamed Child Sexual Abuse For-profit is a Global Crime. Offenders Weaponize Live Video Streams (i.e. Video Chats) to Produce and Consume New Child Sexual Abuse Material.

Much has been written about the global pandemic of child sexual abuse material and various forms of online sexual exploitation of children (i.e., sextortion, grooming, self-generated and AI generated CSAM, etc). One form of OSEC and CSAM that, despite its depravity and some media exposure,[1] has hidden under the radar with governments, CSOs, tech and financial sector companies needing to do much more to prevent and address this crime.

Livestreamed child sexual abuse is a form of human trafficking, namely, the trafficking of children to produce new CSEM.[2] In this exploitation, a child is sexually abused by an adult while a foreign offender, typically a man from a Western, English-speaking country such as the United States, United Kingdom, Australia, Canada, or EU watches the abuse happen in real time via a video call. These demand-side offenders pay adults for the opportunity to *direct* specific acts of sexual abuse against specific children in real-time by typing in the chat and/or dictating the abuse audibly on the video call.

[1] See for example "The rise of live-streamed child abuse – and Britain's role in it," The Telegraph, 11 March 2024, https://www.telegraph.co.uk/global-health/terror-and-security/live-streamed-child-abuse-philippines-surges-britain-demand/; "Inside the Global Taskforce Fighting Child Sex Abuse in the Philippines," Foreign Correspondent, 2 March 2023, https://www.youtube.com/watch?v=sYXgHV_SNeY&list=PLT6CmQ1R9UBlofg7v2b6fIMlfS3U03i79.

[2] International Justice Mission and University of Nottingham Rights Lab. (2023). Scale of Harm Research Method, Findings, and Recommendations: Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines. International Justice Mission, page 19.

Based on IJM's experience, the abuse usually includes rape, or children being forced to engage in sex acts with other children and sometimes harmed in other degrading ways, such as in bestiality. In a recent case, financial data and chat logs showed that a 58-yr old British man paid a woman in the Philippines to livestream the abuse of a 9-year-old girl.[3] The man caused and incited the abuse, directing that the girl be penetrated. Demand-side offenders proliferate a global criminal industry by directing, paying for, and producing new child abuse material from the comfort of their homes. Hiding behind their screens, they abuse the most vulnerable children around the world.

Because offenders pay between $20 and $100 to incite and watch child abuse, that makes this crime very lucrative when one payment constitutes days of Filipino wages. Offenders exploit the dollar's power in markets like the Philippines. **Make no mistake, the supply is created because of the demand.**

Speaking about a demand-side offender who paid for and directed livestreamed abuse, the now-retired 4-decade veteran of Internet Crimes Against Children, Detective Inspector Jon Rouse of the Australian Federal Police Taskforce Argos, said this, *"[The offender] may as well have been in the room with the kids. The fact he was seeing it in the virtual world is irrelevant…what happened to those kids happened because of him."*[4] Indeed, in IJM's over 13-years' experience combating online sexual exploitation of children, we have seen demand-side sex offenders proliferate a global criminal industry by directing, paying for, and producing new child abuse material from the comfort of their homes.

Another example: In one of Germany's first prosecutions[5] for livestreamed child sexual abuse, a 48 year old man from Bavaria, Germany, gave specific instructions via webcam to a Filipino trafficker to create and transmit child sexual abuse material live. At the beginning of the abuse, the three Filipino victims were a 4-year-old girl, a 7-year-old boy, and an 8-year-old girl. The abuse lasted over 2 years. It ended, when Philippine law enforcement in partnership with IJM safeguarded the 3 victims and arrested the trafficker. IJM professional social workers provided trauma crisis intervention and supported the children through police interviews, while beginning the process of assessing their rehabilitation needs.

Evidence against the offender included **120 pages of chatlogs**, as well as photos and videos of the children being sexually abused. He transferred over **10,000 euros** between 2014 and 2016, of which **3,000 euros were** directly in return for child sexual abuse – not known CSAM that is identified with PhotoDNA, but new sexual abuse images, recorded and live videos of these 3 children. In 2018, the German offender was sentenced to 5.5 years in prison, while the seller received a 20-yr prison sentence in the Philippines, a sentence nearly 4x that of the demand-side offender, despite the gravity of his crimes. Offender sentences must be commensurate to the gravity of their crimes, ensuring that overseas survivors also receive financial remuneration or restitution.

---

[3] "Windsor man jailed for paying to live-stream child sex abuse in the Philippines," Maidenhead Advertiser, 15 January 2021, https://www.maidenhead-advertiser.co.uk/news/windsor/165097/windsor-man-jailed-for-paying-to-live-stream-child-sex-abuse-in-the-philippines.html .

[4] https://www.smh.com.au/world/children-as-young-as-two-rescued-from-philippine-cybersex-abuse-dens-20170603-gwjmg5.html

[5] https://www.dw.com/en/german-man-sentenced-to-five-and-a-half-years-for-livestreaming-sex-abuse/a-43330106

IJM's Groundbreaking Prevalence Study Measured Trafficking to Produce CSEM For the First time.

In 2023, IJM and the University of Nottingham Rights Lab released our Scale of Harm study which found that, in 2022 alone, nearly half a million Filipino children were sexually abused to produce new child sexual exploitation material for sale to offenders globally. The study also found that approximately nearly a quarter of a million adult Filipinos, or roughly 3 in every 1,000, were involved in financially motivated CSEM production. The Scale of Harm study advanced understanding of online sexual exploitation of children by specifically examining, using robust methodology, a subset of this crime: the *trafficking of children to produce new CSEM*. The study builds upon the 2020 IJM-led study and employed a rigorous and comprehensive methodology developed over the course of a year in collaboration with the world-leading University of Nottingham Rights Lab and a 24-member External Advisory Council. The study also incorporated input from Filipino survivors who helped design the household survey and led focus group discussions.

The Scale of Harm findings highlight the need for accelerated action to combat the production of CSEM, including via live video streams, for sale to offenders globally. Key recommendations include strengthening community-based reporting; intensifying criminal justice system responses; enforcing tech and financial sector safety by design safeguards; speeding up tech and financial detection and reporting; and urging demand-side governments to pass and implement online safety legislation and regulation with survivor consultation.

Survivor Leader Ruby* noted in her WeProtect Global Alliance op-ed:

> "As someone who experienced the harm of online sexual abuse, I would say that no one can validate study results like Scale of Harm the way survivors can. My advocacy work is equally important as my other jobs. I was there, experienced and witnessed the horrors of online sexual abuse. Because of that, I am fully committed to protecting children from this crime. I cannot imagine other children going through similar, and maybe even worse, trauma."[6]

And this does not just happen in the Philippines but many other countries. For instance, in a Colombia February 2023 case, police safeguarded three children aged 19 months, seven and nine years, and arrested their mother and aunt accused of livestreaming child sexual abuse for profit.[7]

---

[6] "More than 'Just Survivors'," WeProtect Global Alliance, October 11, 2023. https://www.weprotect.org/blog/more-than-just-survivors/

[7] "Horror en Medellín: madre obligaba a sus tres hijos de 19 meses, 7 y 9 años a grabar pornografía infantile." 27 February 2023, https://www.semana.com/nacion/articulo/horror-enmedellin-madre-obligaba-a-sus-tres-hijos-de-19-meses-7y-9-anos-a-grabar-pornografia-infantil/202311/. In Romania as well, see Sask, "Appeal Court Increases Sentence for Child Pornographer Philip Chicoine," *Global News*, accessed 9 May 2024, https://globalnews.ca/news/6042218/appeal-court-increases-sentence-for-child-pornographer-philip-chicoine/.

Europol warns that 'livestreaming of child sexual abuse increased and became even more popular during the COVID-19 pandemic.'[8] 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 reports 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.[9] According to a Protect Children Darkweb CSAM survey, "45% of respondents say that they watch livestreamed CSAM."[10]

Moreover, all countries need be concerned because research indicate livestreaming offenders not only pose risks to children abroad but also at home. Australian Institute of Criminology in their report, The overlap between child sexual abuse live streaming, contact abuse and other forms of child exploitation:

> "[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."

University of Edinburgh's Childlight research confirms this:

> "Men in Australia, UK and USA who report online sexual offending behaviours against children also report being 2-3 times more likely to seek sexual contact with children between the ages of 10-12 years old if they were certain no one would find out."

Promising Online Safety Legislation and Regulation Exists in the UK and Australia.

The Governments of Australia and the UK have both passed online safety laws requiring tech companies to step up their efforts to address online sexual exploitation of children through Australia's eSafety Commissioner and the UK's Ofcom regulator. As it relates to livestreaming, Ofcom's initial Illegal Harms Draft Codes of Practice outline the issues of child sexual abuse via livestream from the Philippines to the UK. In developing a register of risks, livestreaming is one of the functionalities that can deem a platform to be higher risk of facilitating child sexual abuse material creation, production, and distribution.

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 the in

---

[8] Europol (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. [online] Europol. Available at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

[9] Interpol (2020). *INTERPOL report highlights impact of COVID-19 on child sexual abuse*. [online] www.interpol.int. Available at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse.

[10] "ReDirection Launch: 'Protecting Children Through Prevention'," Protect Children, September 2021. https://www.suojellaanlapsia.fi/en/post/redirection-launch-protecting-children-through-prevention ("Another key finding reveals that CSAM is increasingly livestreamed").

their regulatory guidance on the Basic Online Safety Expectations.[11] Not only this, but eSafety has also included questions on livestreaming in their non-periodic transparency notices to tech companies operating in Australia.

In the US, the bipartisan Revising Existing Procedures on Reporting via Technology (REPORT) Act became law in May 2024. The REPORT Act is an essential step toward increased online safety, with critical updates to CyberTipline reports as it will:

- Require electronic service providers to report sex trafficking of children and enticement crimes.
- Increase penalties for failure to report such exploitation.
- Increase the preservation period for information submitted to the CyberTipline, which gives law enforcement more time to investigate and prosecute.[12]

Robust regulation and enforcement are needed to deliver the child protection promises of the REPORT Act, UK and Australia's Online Safety Acts to every child in need, and that should be followed by further online safety laws in the U.S., Canada, and elsewhere. Importantly, those efforts should address newly produced CSAM and live video CSAM.

Technical Solutions to detect, prevent, and disrupt new CSAM and livestreamed child sexual abuse exist.

SafeToNet | HarmBlock
This is a real-time video & 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, etc.

Thorn | Safer
Safer scales CSAM detection, increases content moderation efficiency, and optimizes detection using advanced AI technology. 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 | DragonflAI
This prevention, detection, and disruption tool screens imagery, including livestreams, on-device using a combination of nudity detection and age estimation technology before they are streamed

[11] Basic Online Safety Expectations Regulatory Guidance, eSafety Commissioner, September 2023. https://www.esafety.gov.au/sites/default/files/2023-09/Basic-Online-Safety-Expectations-Regulatory-Guidance-updated-September-2023_0.pdf.
[12] https://www.ijm.org/news/ijm-applauds-senate-passage-report-act; https://www.ijm.org/news/biden-signs-report-act-protect-kids-online. "Americans are some of the top offenders paying for and consuming child sexual abuse material and committing child sex trafficking online, including via livestreaming. Additionally, most of the technology platforms and apps weaponized to exploit and abuse children, including in the Philippines, are based in the U.S. and governed by our laws. … The signing of this bill into law is an important step in strengthening federal policy to better protect children online in the U.S. and around the globe," said Nate King, Director of Congressional Affairs for IJM.

to platform. This prevention, detection, and disruption tool screens imagery, including livestreams, on-device using a combination of nudity detection and age estimation technology. The primary implementation of this tool would redirect flagged content to human moderators for review and further action as appropriate before it could be transmitted or broadcast any further.

It is not simply safety tech companies developing safety technology using image or video classifiers. Even Apple and Instagram appear to deploy somewhat similar safety technology apparently using image or content classifiers:

> "Communication Safety uses on-device machine learning to analyze photo and video attachments and determine if a photo or video appears to contain nudity. **Because the photos and videos are analyzed on your child's device, Apple doesn't receive an indication that nudity was detected and doesn't get access to the photos or videos as a result**."[13]

Instead of providing a warning and initially blurring the harmful or illegal content, companies should prevent the production, sharing and consumption of CSAM, including via on-device solutions. The Protech Project is an innovative pilot study on just that.[14]

Survivors Recommend that Companies Deploy Technology to Prevent Livestreamed Child Sexual Abuse.

> **Joy*:** "I think there should be a technology that will detect CSAM. Because in my experience, I was abused when I was still young but I was only rescued after several years after the abuse. It is better that children will be rescued earlier by early detection. With early detection, there will be less children that will be further abuse if perpetrators are detected or arrested early on. Foreigner pedophiles must also be detected and stopped early on because they create the demand for CSAM both on the production and livestreaming."[15]

> **Ruby*:** "It is really important to be vigilant and people who have power, to invest to create a system that will ensure safer community online for children. Most specially on present times that children are using online gadgets. There's a child that I personally knew whom I caught using a phone. What's worst was there a foreigner stranger that was waving on her and trying to communicate with her. It frightened me how these 'stranger's can easily access children online. This ignite my desire to advocate for safety of children online. To create a technology that will detect CSAM online and protect children from harm specially in livestreaming."[16]

> **Liberty*:** "I agree that there shall be a technology that will detect CSAM. To prevent these CSAM from being shared most specially in livestreaming. There's a platform I know that detects if there are 'harmful' material online, if other online platform is able to do it, I believe it can really be reported."[17]

---

[13] https://support.apple.com/en-us/HT212850
[14] https://www.protechproject.eu/about
[15] IJM Submission on Draft Industry Codes of Practice for the Online Industry, page 8. https://www.aph.gov.au/DocumentStore.ashx?id=9d5fdd7d-30e8-41e6-9c90-1ddc7a48c199&subId=745049.
[16] Ibid.
[17] Ibid.

**Pseudonyms (real names and case files on file with IJM)*

Finally, the Financial Sector Should Step Up Efforts to Detect and Disrupt Livestreamed and Other Child Sexual Abuse Payments.

IJM recommends the following:

1) Financial regulators and financial intelligence units should provide prescriptive regulations and explicit guidance to institutions on how to detect, interdict, and report transactions suspicious for child sexual exploitation online.
2) Financial sector should implement specific methodologies to proactively monitor transactions to detect payments suspicious for child sexual exploitation.
3) Financial institutions should treat child exploitation payments like terrorist financing or fraud by striving to detect, interdict and report as soon as possible once the suspicious payment behavior is identified.[18]
4) Governments should allow information sharing among financial institutions and facilitate public-private partnerships.
5) Financial intelligence units should proactively provide actionable financial intelligence disclosures to law enforcement agencies.

May 15, 2024

About IJM

International Justice Mission is a global organization that protects people in poverty from violence. IJM partners with local authorities in 31 communities in 16 countries to rescue and restore survivors, hold perpetrators accountable, and help strengthen public justice systems so they can better protect people from violence.

[18] Recommendations to banks and credit unions when responding to suspicious financial transactions involving human trafficking similarly call for a 'rapid response': "Ensure that policies and procedures allow for a timely review of case characteristics to identify and permit a rapid response in cases of urgency." Peter A. Allard School of Law, "Follow the Money: The Role of Financial Institutions in Canada's Fight Against Human Trafficking," *International Justice and Human Rights Clinic* (July 2020): 7, https://allard.ubc.ca/sites/default/files/2021-03/Follow%20the%20Money%20Report%20-%20with%20cover%20-%20FINAL_1.pdf.