Testimony of John Tanagho, International Justice Mission Before the Senate Judiciary Committee Subcommittee on Crime and Counterterrorism

"Ending the Scourge: The Need for the STOP CSAM Act"
March 11, 2025

Chairman Hawley, Ranking Member Durbin, members of the subcommittee – thank you for inviting me to testify at this important hearing.

My name is John Tanagho, and I serve as Executive Director for International Justice Mission (IJM)'s Center to End Online Sexual Exploitation of Children. IJM is a global nongovernment organization (NGO) that protects people in poverty from violence. IJM partners with governments in 19 countries to combat modern slavery, violence against women and children, and other forms of abuse. For 27 years, IJM has strengthened public justice systems to hold traffickers, online sex offenders, and other violent criminals accountable, help survivors on their journey to safety and healing, and reduce the prevalence of crimes by up to 86%.[1]

At an alarming scale, offenders from around the world conspire with traffickers online in countries like the Philippines, paying to livestream the sexual abuse of children as directed by the offenders in real time.

I spent seven years living in the Philippines, leading IJM teams to protect children from this brutally pernicious form of trafficking, where young victims are trafficked to produce child sexual abuse material, or CSAM[2], especially in live videos. Since 2011, IJM has worked closely with all levels of the Philippine Government, international law enforcement, community service organisations, survivor leaders, and other relevant stakeholders to combat this form of child sex trafficking. And we're seeing big results. Through IJM-supported cases, Philippine law enforcement has brought to safety over 1,470 victims (and at-risk individuals), arrested over 430 traffickers, and convicted over 265 perpetrators. **Thanks in part to U.S. foreign assistance through the U.S.-Philippines Child Protection Compact from 2017-2021[3], the government of the Philippines has developed innovative child-protective, trauma-informed social services and prosecution policies to ensure survivors receive the justice they deserve.**

In IJM's casework experience from 2011 to 2024, demand-side offenders, often from the U.S., use popular internet platforms and mobile apps with live video and chat functions to issue graphic abuse instructions. This sexual abuse is transmitted live for the offender's sexual consumption and documented in photos and videos that create new CSAM. While the U.S.

[1] https://www.ijm.org/

[2] Child Sexual Exploitation Material (CSEM) is any visual or audio (and/or any combination thereof) representation of children (under the age of 18) engaged in sexual activity or of minors engaging in lewd or erotic behavior recorded, produced and/or published to arouse the viewer's sexual interest. Child sexual abuse material (CSAM), which depicts the contact sexual abuse of a child, is a subset of CSEM. See ECPAT Luxembourg, Interagency Working Group (2016), "Luxembourg Guidelines," https://www.ilo.org/ipec/Informationresources/WCMS_490167/lang--en/index.htm.

[3] https://www.ijm.org.ph/articles/us-and-philippines-conclude-child-protection-compact-partnership

Department of Justice calls this "virtual child sex trafficking,"[4] the abuse is shockingly real and traumatizing.

This is pay-per-view CSAM, live on-demand.

Based on IJM's experience, live video child sexual abuse usually involves rape, children forced to engage in sex acts with other children, or sexually abused by an adult, and other degrading harms, such as bestiality.[5] According to the Internet Watch Foundation (IWF)'s research on livestreamed child sexual abuse, 98% of victims are 13 or under, and forty percent of the livestream "captures" or recordings were classified as containing serious sexual abuse, with 18% involving the rape and sexual torture of children.[6]

The severity of harm to children in extreme child sexual abuse material globally is rapidly growing. In 2022, the IWF found that "extreme child sexual abuse" online doubled in just two years (with such abuse defined as images/videos involving penetrative sexual activity, sexual activity with an animal, or sadism).[7]

In the Philippines, victims are abused for two years on average, in part because the abuse goes undetected and unreported. According to a 2020 study published by IJM, the median age of victims is only 11 years old, while children as young as infants were also abused. Research by the Australian Institute of Criminology found that sex offenders pay as little as $33 dollars to direct and watch a child be abused in a livestream.[8] This is consistent with IJM's casework, with payment amounts typically increasing based on the number of children abused, the severity of abuse, and the younger age of victims.

And while the victims may be overseas, make no mistake: This is an American problem.

- One IJM study found 34% of cases involved U.S. offenders.
- Another study found that, in an 18th-month period, individuals in the United States sent over $7.3 million dollars to the Philippines in payments flagged by financial institutions as suspicious transactions.

In his December 2024 piece, investigative journalist Michael Keller reported finding 100 U.S. federal criminal cases of men paying to watch the livestreaming of child sexual abuse.[9] In preparing for this hearing, a cursory web search identified cases of Americans sexually abusing

---

[4] U.S. Department of Justice, National Strategy for Child Exploitation Prevention and Interdiction, *Livestreaming and Virtual Child Sex Trafficking*, at 2 (2023), https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction.

[5] See exemplary cases involving U.S. demand-side offenders, https://www.justice.gov/usao-mdfl/pr/florida-man-who-financed-and-patronized-child-sex-trafficking-ring-philippines-pleads; https://www.scmp.com/news/world/united-states-canada/article/3164587/us-man-who-live-streamed-sex-abuse-filipino

[6] *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

[7] Internet Watch Foundation, "'*Extreme' Category A child sexual abuse found online doubles in two years*." 25 April 2023, https://www.iwf.org.uk/news-media/news/extreme-category-a-child-sexual-abuse-found-online-doubles-in-two-years/.

[8] https://www.aic.gov.au/sites/default/files/2021-10/ti639_live_streaming_of_child_sexual_abuse.pdf

[9] "*On These Apps, the Dark Promise of Mothers Sexually Abusing Children,*" Michael Keller, New York Times, Dec. 7, 2024, https://www.nytimes.com/2024/12/07/us/child-abuse-apple-google-apps.html?unlocked_article_code=1.fk4.RJ2i.dRBch4XE-_0O

children online from all 10 states currently represented on the Senate Judiciary Subcommittee on Crime and Counterterrorism. For eight of those 10 states, we found cases where U.S.-based offenders abused children in the Philippines in-person or online from the safety of their homes in Missouri, Illinois, Texas, Tennessee, Alabama, Minnesota, and New Jersey. (See Annex I.) Just last week, a Kentucky man was sentenced for sexually exploiting children in the Philippines, including livestreamed "custom-created CSAM."[10]

Another important element of this crime must be understood: The products and services of global tech companies domiciled in the United States are among those misused to abuse and traffic children. It would be one thing if offenders used sophisticated technology to hide their abuses, resorted to the dark web, or untraceable payment platforms. But according to Keller, offenders are using apps easily available on Apple and Google app stores, including so-called adult webcam apps used for cybersex.

"The most powerful companies in the world are enabling the sexual abuse of a child to be livestreamed on the internet," according to Sarah Gardner, who leads the Heat Initiative.[11]

The stark reality is that any video-chat application or platform can be used to abuse children this way. According to research by the University of Nottingham Rights Lab, documented cases also include offenders misusing Microsoft Skype, Facebook Messenger, and WhatsApp (see also Annexes I-II for a list of cases), as some concrete examples.[12]

Yet, American tech companies have still not publicly announced any actions to address livestreamed child sexual abuse. In fact, just two weeks ago Australia's online safety regulator had this to say on national radio:

> *When a child is being raped and abused you would think there would be some sense of urgency in tackling those reports … In terms of the livestreaming of live child sexual abuse material … [a]ny kind of video platform, that could be Facetime, that could be Viber, and the questions we were asking [in transparency notices] is what are you doing to detect? There are a range of markers or signals they can look at. Plus, they all have technologies that they can use to identify whether child sexual abuse is happening in real time. Most companies have said they're doing nothing because it's too expensive. These are trillion-dollar companies that have a responsibility to make sure that their platforms are not being misused for the most [grievous] kinds of harm. This has been happening for decades, but until regulators focused on online safety, companies were letting this happen under the radar. Willful blindness as I would call it."*[13]

This is consistent with the a 2022 report from that Australian regulator summarizing tech company transparency reporting, revealing "that the providers are neither taking action to

---

[10] https://www.justice.gov/opa/pr/kentucky-man-sentenced-sexually-exploiting-minors-philippines

[11] "*On These Apps, the Dark Promise of Mothers Sexually Abusing Children,*" Michael Keller, New York Times, Dec. 7, 2024, https://www.nytimes.com/2024/12/07/us/child-abuse-apple-google-apps.html?unlocked_article_code=1.fk4.RJ2i.dRBch4XE-_0O

[12] "Legal and institutional responses to the online sexual exploitation of children," University of Nottingham Rights Lab, September 2023, https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/legal-and-institutional-responses-to-the-online-sexual-exploitation-of-children-the-united-kingdom-country-case-study.pdf, page 10.

[13] Interview on February 24, 2025, https://www.abc.net.au/listen/programs/radionational-breakfast/esafety-commissioner-julie-inman-grant-senate-estimates/104975774

detect [child sexual exploitation and abuse] 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."[14]

Pause for a moment to let that sink in. We are talking about children repeatedly sexually abused *live* via platforms, apps, and devices by their users for their users to watch in real time, in what Europol calls "a persistent threat" that "stands out as the main form of commercial sexual exploitation of children and as a major source" of new CSAM.[15] In the Philippines, this impacts nearly half a million children[16], in addition to victims in Colombia[17], the U.S.[18], U.K.[19], Romania[20], and elsewhere.

Globally, Europol's 2024 Internet Organized Crime Threat Assessment[21] reveals 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)."*[22]

Congressional action is needed now. Behind every livestream is a real child, suffering serious emotional and physical trauma. Even after being brought to safety by law enforcement, the exploitation continues, as offenders repeatedly share and trade images and videos of child abuse via encrypted messaging apps and online platforms.

I have heard survivors of this abuse recount its devastating impact. Ruby*[23], who was sexually abused in livestreams as a 16-year-old and today advocates globally against this crime, recalls how the abuse eroded her will to live:

---

[14] eSafety Commissioner, "*Basic Online Safety Expectations: Summary of industry responses to the First mandatory transparency notices*." December 2022, https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf.

[15] https://www.europol.europa.eu/cms/sites/default/files/documents/Internet Organised Crime Threat Assessment IOCTA 2024.pdf

[16] https://assets.ijm.app/IJM_Scale_of_Harm_2023_Full_Report_5f292593a9.pdf

[17] https://www.semana.com/nacion/articulo/horror-en-medellin-madre-obligaba-a-sus-tres-hijos-de-19-meses-7-y-9-anos-a-grabar-pornografia-infantil/202311/

[18] https://www.independent.co.uk/news/uk/crime/matthew-bower-fbi-nca-paedophile-kent-b2485430.html

[19] https://metro.co.uk/2020/08/15/sex-offender-36-jailed-life-encouraging-women-abuse-children-13132864/

[20] https://globalnews.ca/news/6042218/appeal-court-increases-sentence-for-child-pornographer-philip-chicoine/

[21] https://www.europol.europa.eu/cms/sites/default/files/documents/Internet Organised Crime Threat Assessment IOCTA 2024.pdf

[22] https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf, p. 24.

[23] All names with an * indicate a pseudonym.

> *"While doing every disgusting show [in front of the computer camera with the customer], I lost every bit of my self-esteem to the point where I felt disgusted with myself as well. It's like being trapped in a dark room without any rays of light at all. There's no point in living at all."*[24]

Joy*, who was abused for seven years and now is also a global survivor leader shares her ongoing battle for her privacy, dignity, and peace of mind:

> *"Survivors are still being retraumatized. Today, I am free. I am safe. I am not being livestreamed anymore, but my pictures and videos are still out there. Every time those videos and photos are viewed, I am traumatized again. Even as we speak, how am I supposed to move on with my life, because every day my privacy can still be violated. Survivors should have the right to have our pictures and videos deleted. I am free, but my pictures can be accessed by anybody. I have always wanted to travel, but I live in fear, about safely protecting my identity. Can you imagine, carrying the weight of constantly protecting your identity? I'm afraid someone will approach me, recognize me. When I apply for jobs, when I meet new people. When I travel. I am so afraid of my identity being revealed."*

Some lobby against online safety bills under the banner of free speech or privacy. But those arguments are red herrings. **Child sexual abuse material and child sex trafficking are not protected by the First Amendment.** *See New York v. Ferber, 458 11 U.S. 747 (1982); Paroline v. United States, 572 U.S. 22 434 (2014).*

Moreover, can you imagine a greater privacy violation than a child raped while offenders watch live on their phones and tablets, with the images and videos shared over and over again for years to come? We simply cannot accept this perverse status quo.

As the land of the free, the United States of America must defend the freedom of victims and survivors to not have their abuse and exploitation paint the internet for every man, woman, and child to see.

That is why I recommend that Congress enact public policies that:

- Maximize the actionability of CyberTipline reports to help law enforcement better identify victims and offenders.
- Require major tech companies to submit an annual transparency report disclosing their efforts and progress made to address CSAM.
- Empower federal courts to authorize trustees who can facilitate restitution safely for minor and foreign survivors.
- Codify a notice and takedown regime that allows survivors to directly require companies to take down their CSAM and take effective steps to prevent its recirculation or uploading.
- Incentivize companies to disrupt and deter the *production* and distribution of CSAM.
- Increase the use of U.S. foreign assistance, like the Child Protection Compacts, to keep kids safe online and hold American perpetrators accountable.

[24] Ruby recounts her story from start to finish in a 6-part podcast series, *The Fight of My Life: Finding Ruby*, https://fightofmy.life/

With this background, the remainder of my written testimony will cover:

I. The prevalence of this global crime in the Philippines.
II. The importance of holding demand-side offenders in the U.S. accountable, including the risk they pose to abuse children in the U.S.
III. How U.S. policy and targeted foreign assistance can help stop CSAM.
IV. How privacy and free speech debates need survivor voices.
V. Conclusion and Recommendations: Deploy Multi-Sector Interventions at Scale.

I. IJM's *Scale of Harm* Study Measured the Prevalence of this Crime.

In 2021, IJM, together with the University of Nottingham Rights Lab, a world-leading human trafficking research institution, launched the *Scale of Harm* project, which developed and implemented a research method estimating the prevalence of child trafficking to produce new child sexual exploitation material (CSEM), including via livestreaming, in the Philippines.[25]

A prevalence estimate is critical to determine the protective impact of government and multi-stakeholder efforts over time. In other words, prevalence estimates are crucial to ascertain if multi-stakeholder efforts are working to accomplish the most important goal, namely, protecting more children from child sexual abuse and exploitation in the first place (i.e., prevention). After all, successful child protection interventions should lead to fewer children being harmed in the first place.

Previous IJM prevalence studies[26] on various forms of violence have proven that increased perpetrator accountability – through detection, arrest, and prosecution – can have a disproportionate impact on reducing crime when done in a trauma-informed, holistic justice system. For example, externally validated prevalence studies showed between 72% to 86% reductions of in-person child sex trafficking in commercial establishments and red-light districts in Philippine regions.[27]

IJM's *Scale of Harm* study revealed a significant national prevalence[28] with nearly half a million Filipino children sexually abused to create new CSEM for sale to offenders around the world. The study also found that approximately nearly a quarter of a million adult Filipinos, or roughly 3 in every 1,000, were involved in this financially motivated CSEM production. *Scale of Harm* provides recommendations co-developed with survivor leaders.

---

[25] "Scale of Harm: prevalence measurement, multi-sector partnerships and survivor engagement," https://www.weprotect.org/resources/case-study/scale-of-harm-prevalence-measurement-multi-sector-partnerships-and-survivor-engagement/

[26] See International Justice Mission's prevalence studies: https://www.ijm.org/studies.

[27] Haarr, R. (2017). Evaluation of the Program to Combat Sex Trafficking of Children in the Philippines: 2003-2015. https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/philippines-csec-program-evaluation_2021-02-05-063357.pdf.

[28] International Justice Mission. Scale of Harm: Research Method, Findings, and Recommendations – Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines, Summary Report. https://assets.ijm.app/IJM_Scale_of_Harm_Summary_Report_Sept_2023_f733d4e011.pdf

Relevant to this hearing, Recommendation #6 specifies that "Demand-side governments should urgently pass online safety legislation with survivor consultation" because "[o]nline safety legislation can facilitate the protection of children from sexual abuse and exploitation online, including abuse streamed in video calls and other CSEM production."[29]

In response to the Scale of Harm study, the Philippine government is doubling down on efforts to combat CSAM. President Ferdinand Marcos Jr. reaffirmed this commitment at a national summit co-organized by IJM in September 2024, stating: "I have said it before, and I will say it again: This Administration will do everything—we will spare no effort—to combat these heinous crimes against our children."[30] Executive Order No. 67 issued by the President created the Presidential Office for Child Protection (POCP) to monitor and harmonize government policies and programs to address the crime.

Thanks to strategic U.S. foreign assistance from 2017-2021, justice system strengthening to address these crimes in the Philippines is stronger than before and continues to grow through NGO and international partnerships. Philippine law enforcement, prosecutors, and social services have prioritized trauma-informed, child protection efforts. Within its first five years of operation, the Philippines Internet Crimes Against Children Center (PICACC) made possible the safeguarding of 672 individuals from online sexual exploitation and the arrest of 141 suspects.

II. The U.S. Must Hold Demand-Side Offenders Accountable, Thus Protecting Children in the US and Abroad.

Governments must holistically address demand-side offenders within their jurisdictions. This includes incentivizing tech sector detection, disruption, and reporting, applying effective justice system responses, and engaging in robust international law enforcement collaboration.

According to available data, the United States is the number one demand-side country of offenders paying for and directing the sexual abuse of Filipino children. According to a 2020 IJM study, 34% of Philippine cases involved U.S.-based offenders.[31] Moreover, according to an April 2023 report by the Philippine Anti-Money Laundering Council, since 2015, individuals in the U.S. have sent the highest number of payments for suspected child exploitation online flagged by financial institutions in suspicious transaction reports. Over 67,000 of these suspicious transaction reports occurred in the 18-month period from mid-2020 to 2022, accounting for 52.25% of all reports.[32] This 18-month period saw nearly $7.3 million in

[29] Scale of Harm, at p. 54.

[30] Speech by President Ferdinand R. Marcos Jr. at the OSAEC Summit 2024, September 16, 2024, https://pco.gov.ph/presidential-speech/speech-by-president-ferdinand-r-marcos-jr-at-the-osaec-summit-2024/?__cf_chl_tk=M3kqlijcIKpjchSU1TeYSZ8OOGxkTo9hecOv_ml4lMw-1741392066-1.0.1.1-OxdG00U_dBxiC6L5fdN6DMoldAeG6kMfDDGkaa93xkM

[31] International Justice Mission, "*Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society*." 2020, https://www.ijm.org.ph/assets/resource/IJM-OSEC-in-the-Phils-Analysis-and-Recommendations-for-Governments-Industry-and-Civil-Society-Full-2020.pdf.

[32] Anti-Money Laundering Council. (2023). Online Sexual Abuse and Exploitation of Children in the Philippines: An Evaluation Using STR Data (July 2020 – December 2022), http://www.amlc.gov.ph/16-news-and-announcements/454-online-sexual-abuse-and-exploitation-of-children-in-the-philippines-an-evaluation-using-str-data.

suspected child exploitation-related transactions enter the Philippines from U.S. senders, according to the Anti-Money Laundering Council report.

Legislators, prosecutors, and judges in demand-side countries, such as the U.S., need to be extremely clear about who is driving livestreamed abuse: Online sex offenders initiate live sexual abuse by paying and instructing in-person traffickers to abuse young children in specific ways. Plainly put, demand-side sex offenders are the directors and funders of the most horrific child abuse imaginable.

With offenders thousands of miles away, you may be tempted to view these offenses as image-based or virtual; yet real, physical sexual abuse is the result. Detective Inspector Jon Rouse APM, the now-retired 39-year veteran of Internet Crimes Against Children unit of the Queensland Police Service and Australian Federal Police (Task Force Argos), said this about a demand-side offender who paid for and directed livestreamed abuse:

> *"[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."*[33]

In IJM's 13-plus years of combating this crime, 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.

And the risk to American children is also real. Offenders who use the internet to abuse children overseas or consume CSAM also pose a threat to harm American children. Offenders who consume CSAM are more likely to sexually abuse children in person. To make America safer, we should invest in holding livestreaming offenders accountable.

Recent research from the Australian Institute for Criminology suggests that individuals who view livestreamed CSAM have already crossed the "psychological threshold" to contact offenses, by directing and watching the live sexual abuse of a child online – which is on par with abusing the children themselves.[34] This may partly explain why, according to IJM research, 9% of known demand-side offenders in our 2020 study also traveled to the Philippines to abuse children in person.[35]

Nearly half of respondents to a survey[36] in the Stanford Internet Observatory's Journal of Online Trust and Safety said they had sought direct contact with children through online platforms

---

[33] The Sydney Morning Herald, 3 June 2017. *Children as young as two rescued from Philippine cybersex abuse dens*. https://www.smh.com.au/world/children-as-young-as-two-rescued-from-philippine-cybersex-abuse-dens-20170603-gwjmg5.html

[34] https://www.aic.gov.au/sites/default/files/2023-05/ti671_overlap_between_csa_live_streaming_contact_abuse_and_other_child_exploitation.pdf

[35] https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020_2021-02-05-055439.pdf

[36] https://www.theguardian.com/global-development/2022/mar/01/online-sexual-abuse-viewers-contacting-children-directly-study

after viewing CSAM, and 58% reported feeling afraid that viewing CSAM might lead to them committing abuse in person.[37]

Similarly, men in Australia, the U.K. and the U.S. who report online sexual offending behaviors against children also report being 2 to 3 times more likely to seek sexual contact with children between the ages of 10 and 12 years old if they were certain no one would find out.[38]

And a 2015 U.S. DOJ study found that 85% of "offenders disclosed hands-on sexual abuse," concluding that the findings "suggest that crossover to hands-on offending may be more prevalent among internet offenders."[39]

Our law enforcement partners at the U.K.'s National Crime Agency (NCA) report a similar crossover: "The NCA is seeing a direct link between online offending and contact abuse. In the UK we estimate that there are between 550,000 and 850,000 UK-based individuals posing various degrees of sexual risk to children – a figure which has grown in line with increased online activity."[40]

Even those offenders view, possess, and share CSAM – without initiating the production – fuel the demand for new abuse of children. In their Exploiting Isolation report released in June 2020, Europol states:

> *"The demand for such [CSAM] perpetuates the ongoing abuse of children by [offenders] and others. It is likely that the increase in the circulation of online CSAM in recent weeks will continue to feed the cycle of physical sexual abuse of children and their victimisation in real life and online. This is particularly so because offender forums often require the production of "never before seen" CSEM, motivating new victimisation of children."*[41]

With such a significant demand-side offender problem, the U.S. should lead the way by ensuring that local, state and federal law enforcement agencies are sufficiently resourced to investigate U.S.-based offenders who pay for, direct and remotely produce child sexual abuse material.

When impunity reigns – as it does today – no one is safe. Protecting children from these crimes requires coordinated global efforts from governments, the tech and financial sectors, civil society, and survivor leaders. Offender impunity must end on both the source and demand side,

---

[37] ReDirection Project, Final Report, p. 10, https://www.suojellaanlapsia.fi/en/post/redirection-final-report-3, reported in "Risk Factors for Child Sexual Abuse Material Users Contacting Children Online: Results of an Anonymous Multilingual Survey on the Dark Web," p. 1, https://tsjournal.org/index.php/jots/article/download/29/17/118

[38] https://childlight.org/nature-online-offending-against-children-population-based-data-australia-uk-and-usa

[39] https://smart.ojp.gov/somapi/chapter-3-sex-offender-typologies (Chapter 3: Sex Offender Typologies, Dominique A. Simons).

[40] "Online child abuse survey finds third of viewers attempt contact with children," The Guardian, Sept. 27, 2021, https://www.theguardian.com/global-development/2021/sep/27/online-child-abuse-survey-finds-third-of-viewers-attempt-contact-with-children

[41] Europol, 'Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic', (Report, 19 June 2020) 4. https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-duringcovid-19-pandemic.

and with more offenders in the U.S. driving child sexual abuse online globally, the U.S. should ensure it is doing its part.

III. A Strong U.S. Policy Response Can Stop CSAM In its Tracks.

As child sexual abuse rages online, governments can help reduce the production of "first -generation" CSAM, including livestreamed abuse. **Legislation should incentivize tech companies to make their platforms and products safe by design.**

Unfortunately, global tech platforms, including those headquartered in the U.S., remain fertile ground for child sexual abuse and exploitation online, according to Australia's eSafety Commissioner in its December 2022 Basic Online Safety Expectations report, which indicates that companies are not taking action to detect child sexual exploitation and abuse in livestreams or videos calls.[42]

Without strengthened laws and effective law enforcement, child exploitation online will continue to be a global crisis spiraling out of control. Since the U.S. is the host of major multi-national tech companies whose platforms are weaponized to abuse children, Congress should pass legislation that shifts the fundamental business incentives for U.S.-based tech companies and motivates them to prevent child sexual exploitation on their platforms. The U.S. State Department should also continue to deploy targeted foreign assistance to strengthen the capacity of partner governments to address online sexual exploitation of children and improve coordination between U.S. and foreign law enforcement partners in countries of concern.

A. Maximizing the Actionability of CyberTipline Reports Helps Identify Victims and Offenders.

Online child sexual exploitation is a global crime, requiring a coordinated global response by government, civil society and the private sector. For instance, of the 36 million reports that the National Center for Missing and Exploited Children (NCMEC)'s CyberTipline received in 2023, over 91% were referred to law enforcement outside of the U.S.[43] The sheer amount of CyberTipline reports consistently outpace law enforcement's capacity to respond in almost every jurisdiction, especially in under-resourced countries.

[42] eSafety Commissioner, "Basic Online Safety Expectations: Summary of industry responses to the First mandatory transparency notices." December 2022, https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf.

[43] https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf

IJM has firsthand experience working alongside under-resourced law enforcement partners in responding to this challenge. Together with NCMEC, Meta and other industry partners, law enforcement and NGO partners, IJM provides specialized training that builds capacity for investigators as they learn to access, review and act on CyberTipline reports through NCMEC's Case Management Tool. IJM has provided such trainings in Kenya, Nigeria, Ghana, Malaysia, Sri Lanka, Cote d'Ivoire, and the Philippines.[44]

From IJM's experience in training international law enforcement partners on CyberTipline investigations, it is clear that the existing reporting framework needs updating. IJM supports enhanced reporting requirements that will improve consistency, quality and timeliness in reports of suspected child sexual exploitation submitted by electronic service providers (ESPs) to the CyberTipline.

Enhancements to the CyberTipline reporting requirements will help ensure that ESPs promptly disclose relevant information that may help police identify and locate victims and suspects. We know that timely, high quality, actionable reports in the hands of trained, resourced law enforcement are more likely to lead to victim safeguarding and offender accountability than reports lacking essential information.

In particular, based on IJM's years of experience supporting the assessment of CyberTipline reports in numerous countries with diverse legal and structural frameworks, IJM has seen a need for data points to be contextualized by ESPs in their reports. Complete and contextualized data points are more valuable to law enforcement, enabling them to assess reports and potential criminal activities more effectively. For example, including an Internet Protocol ("IP") log that shows whether IP addresses were linked to a password change, file upload, login/logout event, or account creation provides context that helps investigators determine which IP addresses are most relevant to their investigation.

Similarly, providing full copies of chat logs (rather than just the parts containing violations) provides greater context for the investigator, since this often includes additional insight into the relationship between the communicating parties and may include suspect/victim location or identity information. Since these reports are shared with law enforcement agencies worldwide, the more comprehensive the information, the more helpful it may be to an investigator in another country who is unable to use legal process or subpoena powers to obtain ESP information in the way U.S. law enforcement can. Other critical information to maximize the actionability of ESP CyberTipline reports include:

- Contact information of all users and accounts involved in the report
- Current status of user account (active, shut down)
- Whether the user was notified of account shutdown or notified of the current report
- Billing and payment information
- Device information, including make, Operating System, and device ID
- Relevant linked accounts for multi-service platforms.

[44] "International Justice Mission Partners with NCMEC, Law Enforcement and Tech to Protect Children Online through Training in Côte d'Ivoire," May 13, 2024, https://www.ijm.org/news/international-justice-mission-partners-ncmec-law-enforcement-tech-protect-children-online-training; see also https://www.missingkids.org/blog/2022/online-child-abuse-has-no-borders-ncmec-training-out-of-africa

- Indicate whether live video or livestreamed abuse and exploitation

B. Tech Transparency is Essential for Meaningful Change.

IJM recommends Congress enact a statutory requirement for large U.S.-based tech companies to submit annual reports describing their efforts to address child sexual exploitation on their products, services, and platforms. As proposed in the previous version of the STOP CSAM Act, key information required in the tech company annual report could include:

- "A description of the policies of the provider with respect to the commission of child sexual exploitation and abuse using the provider's product or on the provider's service, including how child sexual exploitation and abuse is defined."
- "The measures and technologies that the provider deploys to protect children from sexual exploitation and abuse using the provider's product or service. The measures and technologies that the provider deploys to prevent the use of the provider's product or service by individuals seeking to commit child sexual exploitation and abuse," along with "an assessment of the efficacy of the measures and technologies described …"

We urgently need this type of transparency from tech companies to hold them accountable for their actions and/or inactions to combat child sexual abuse. This type of reporting can influence benchmarking to show progress in the fight against child sexual abuse, impact policy decisions, and determine resource allocation needs for governments, NGOs, and tech companies alike. Moreover, a report from the Organisation for Economic Co-operation and Development (OECD) examined the top 50 online platforms' transparency reporting and their policies and procedures in relation to child sexual exploitation and abuse. It found that **80% of platforms provided no detailed policy on online sexual exploitation of children and 60% of platforms did not issue a transparency report on such abuse.**[45]

A provision requiring companies to report on the measures and technologies deployed to "prevent the use of their product or service by individuals seeking to commit child sexual exploitation and abuse" is especially important. It is also consistent with global expertise. For example, in the World Economic Forum Global Coalition for Digital Safety's paper, "Making a Difference: How to Measure Digital Safety Effectively to Reduce Risks Online,"[46] experts from the tech sector, government, online safety regulators and NGOs target the need for digital safety to include preventing harm to nonusers:

> "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."[47]
>
> "Additionally, showcasing strong safety measures promotes trust among users, customers and partners, demonstrating a commitment to protecting online users while

[45] https://www.oecd.org/publications/transparency-reporting-on-child-sexual-exploitation-and-abuse-online-554ad91f-en.htm

[46] https://www.weforum.org/publications/making-a-difference-how-to-measure-digital-safety-effectively-to-reduce-risks-online/

[47] Id. at p. 14.

> also minimizing the risk of harm to nonusers or the public caused by misuse of platforms."[48]

In the case of livestreamed abuse, the victims are often not the users of platforms. As such, it is critical to know what companies are doing to prevent the use of their service by criminals to commit CSAM offenses.

C. Statutory Framework for Trustee Appointment is Needed to Safely Facilitate Restitution to Foreign Victims.

IJM's work with thousands of survivors reveals that access to restitution is a critical piece to their recovery and a vital form of justice. It is tangible recognition of the harm done to them. Oftentimes the parents or guardians of child survivors are complicit in their abuse, and survivors may lack their own bank account to accept and manage restitution funds. While federal prosecutors can arrange for a trustee to collect and disburse restitution in those situations, the lack of a statutory framework hinders the process. **IJM recommends that Congress amend existing law to explicitly authorize courts to appoint a trustee to manage restitution payments for certain vulnerable victims and offenses, especially CSAM victims outside the U.S.** Court-appointed trustees can help ensure survivors receive the compensation they deserve no matter their age or where they live, while alleviating any burden on U.S. law enforcement or prosecutor offices.

An excerpt from a 2023 speech by Philippine Survivor Network survivor leader, Joy*, highlights the importance of restitution for overseas survivors of child sexual abuse online:

> *"Survivors are still trapped financially. I lost a lot of time when we were trapped. The world just expects us to move on. But it is hard – because survivors are often left with nothing. We need medical treatment, we need counselling, we need to heal from our trauma. We need education, but shelters are under-resourced, and cannot fully prioritize college education, just elementary or high school for survivors. I wanted to be a social worker, but there is no public school in my community that has social work, so I had to enroll in private school, which cost me a lot. I couldn't have my family come visit me regularly in the shelter, because they couldn't afford travel costs. My brother is also a victim, and he refuses to live in the same community we did, because the family of the perpetrators live nearby. We need to move and find a new community. All of that requires money. I tell you MY STORY because we need to consider how justice must be holistic. Survivors need to be seen as whole individuals, in need of trauma informed care and safe communities.*
>
> *"[Governments] can consider ways to ensure justice is not just served by the court system but also through reparations for international victims, like me, living abroad. Countries should prioritize having all survivors receive reparations from perpetrators, by holding them financially accountable. After all, they have profited from our pain, and are able to pay fines, hire lawyers, delay the judicial system, while even after we are rescued, we need to continue our long journey of healing and we need your*

[48] Id. at p. 5.

support. International perpetrators … increase this demand, and therefore should contribute to our reparations. So my recommendation is: These international reparations can help provide access to social services for victims and survivors of online sexual exploitation, through financial compensation that can help them achieve healing and restoration."

IJM highlights the reality that demand-side offenders of livestreamed sexual abuse are usually in Western countries. IJM has helped survivors of this abuse in the Philippines receive in aggregate over $190,000 in restitution in dozens of U.S. cases, including federal cases against defendants Carl Sara, Anthony Shultz, Max Makati, and Robert Martin Hall, among others. For example, in the case of United States vs. Christopher Streeter, according to court documents a Florida District Court sentenced the defendant to life in prison for sex trafficking after he sent $130,000 over a decade to criminals in the Philippines to produce CSAM of children as young as 12 years old.[49] The Court ordered him to pay $70,000 in restitution. Two years later, thanks to the work of IJM and a pro bono law firm, two survivors finally received their restitution. But most survivors lack the benefit of an international NGO and law firms to access what they are owed.

When it comes to providing restitution payments, **U.S. law enforcement or prosecutor offices are often tasked with determining how to deliver funds to overseas victims. This is a constant problem. Courts order restitution but there is no mechanism to get the money to survivors without working through their parents or guardians**. Yet oftentimes the parents or guardians of child survivors are complicit in their abuse, and survivors may lack their own bank account to accept and manage restitution funds.

Court-appointed trustees can help ensure survivors receive the compensation they deserve no matter their age or where they live. They will have the time and resources to coordinate with NGOs, relevant government social services agencies, and others to ascertain the best way to ensure survivors receive the restitution they are owed in a safe and effective manner. Some countries like the Philippines have promulgated victim compensation guidelines to facilitate this process, but most countries lack any formal mechanisms.

Congress should also consider the appropriation of funds for such training and educational programs, as trustees and guardian-ad-litem would benefit from guidance on these dynamics and how to overcome them.

D. Codify a Notice and Takedown Regime in Federal Law.

The previous version of the STOP CSAM Act included a "notice and takedown" provision that is valuable and essential. Survivors should always have recourse to ask companies to remove their CSAM from their platforms and services. At the same time, such a provision could be strengthened by requiring companies to take effective measures to prevent the republication or uploading of that same CSAM. Once the companies are on notice that any image or video is known CSAM, they have the legal right and should have the obligation to not simply let it happen again. The dignity, safety, and privacy of the survivors depicted in the abuse deserves protecting.

[49] https://annualreport2022.iwf.org.uk/tech-rd/our-role-in-the-safety-tech-challenge/

"There must be an easier process developed for us victim-survivors. We shouldn't have to spend 2+ hours every single day looking for our own abuse just so that companies will take it down. This shouldn't be our job, yet it's become clear that it is," stated one survivor of CSAM.[50] "There are zero excuses for allowing known child sexual abuse to be uploaded to a platform – the tools to prevent this from happening exist and have for years," said Lianna McDonald, C3P's Executive Director. Ian Stevenson, Chair of the Online Safety Tech Industry Association and CEO of tech company Cyacomb, similarly explains:

> *"Technologies to detect child sexual abuse material have advanced rapidly, and many platforms remain largely or completely unprotected which enables their use by abusers. This is often positioned as a choice between privacy and safety, but the latest technologies block abuse content without compromising on user privacy. We believe platforms can, and should, be doing more."*[51]

One such technology is Cyacomb Safety, which "allows social networks and platforms to check uploaded user content instantly against contraband material (a blocklist) with practically no overhead. And thanks to its 'privacy by design' approach, it is even compatible with end-to-end encrypted messaging platforms."[52]
Congress need not legislate any specific technological response; it merely needs to create a statutory duty on companies to take effective steps or measures to prevent the recirculation or uploading of known child sexual abuse images and videos. It is then up to each company to determine how best to comply, depending on its terms of services, platform features, and other unique circumstances.

E. U.S. Foreign Assistance Can Keep Kids Safe from Online Exploitation and Hold American Offenders Accountable.

IJM's own experience in the Philippines shows the impact of targeted U.S. foreign assistance to address online child sexual exploitation.

On April 11, 2017, the U.S. and the Philippines signed the U.S.-Philippines Child Protection Compact (CPC) Partnership, a four-year jointly developed and implemented plan between the two governments to strengthen the capacity of the Philippine government and civil society to address online sexual exploitation of children and child labor trafficking in the Philippines, specifically improving their ability to prosecute and convict child traffickers, provide comprehensive, trauma-informed care for victims and prevent these crimes from occurring in the first place.[53] The partnership facilitated a U.S. State Department investment of $4.9 million in foreign assistance. The Philippine Department of Justice Inter-Agency Council Against Trafficking in Persons (IACAT) also pledged approximately $921,760 to meet CPC Partnership objectives. The partnership formally ended on April 11, 2021.

---

[50] https://protectchildren.ca/en/press-and-media/news-releases/2024/new-report-csam-removal-survivor-experiences

[51] Email on file with author.

[52] https://www.cyacomb.com/products/cyacomb-safety/ (it "prevents the sharing of known online child sexual abuse content on end-to-end encrypted messaging platforms without compromising user privacy").

[53] https://2021-2025.state.gov/child-protection-compact-partnership-between-the-government-of-the-united-states-of-america-and-the-government-of-the-republic-of-the-philippines/

Over these four years, IJM worked with the Government of the Philippines to improve its capacity to prevent and respond to this crime through increased prosecutions of offenders, enhanced protection for survivors, and strengthened prevention and local-level response for vulnerable children in the Philippines.

Key accomplishments from this partnership included:

- 82 operations, resulting in 312 child victims brought to safety and the arrest of 97 suspected perpetrators.
- 237 law enforcement officers and 95 public prosecutors provided with training to prosecute and adjudicate online child sexual exploitation cases in a victim-centered approach.
- 54 aftercare service providers trained in identifying and providing comprehensive services for victims.
- Establishment of the Philippine Internet Crimes Against Children Center (PICACC) in February 2019, which forged greater collaboration and cooperation between Philippine units and foreign law enforcement agencies, including U.S. law enforcement.

The U.S.-Philippines CPC Partnership is also an example of strategic U.S. foreign assistance successfully driving partner government investments and reducing reliance on continued foreign aid. In addition to the initial financial commitment by the Philippines Department of Justice noted above, IJM worked with Philippine legislators to advocate for increased resources for the Philippine National Police - Women and Children Protection Center (PNP-WCPC), resulting in a 2018 budget increase for the PNP-WCPC from 10 million pesos to 45 million pesos – a 350% increase.

IJM recommends the State Department continue and increase the use of targeted foreign assistance mechanisms like the Child Protection Compact Partnerships[54] to increase partner government capacity and will to protect children from sexual exploitation online and hold perpetrators of such crimes accountable. IJM also recommends Congress appropriate continued and increased funding for the State Department's Office to Monitor and Combat Trafficking in Persons, which negotiates and manages CPC Partnerships.

These partnerships also help *make America safer*, because effective global collaboration against child sexual exploitation crimes requires stronger, more effective justice systems in the Global South. For instance, the United States Attorney's Office was able to prosecute a Bangladeshi national for "offenses related to his alleged abuse and exploitation of hundreds of minor victims in the District of Alaska and elsewhere in the United States and abroad in one of the most malicious, digitally facilitated sextortion and child pornography production schemes investigated to date by the FBI" *only after* this offender was arrested by the D11 Unit of the Royal Malaysian Police in Kuala Lumpur.[55] This is the exact Unit that IJM trained as part of a State Department-funded grant.

[54] https://2021-2025.state.gov/child-protection-compact-partnerships/

[55] https://www.justice.gov/media/1250591/dl?inline

IV. Privacy and Free Speech Debates Lack Survivor Voices and Balance.

While tools exist to detect known and new child abuse in images, recorded and live video -- implementation of online safety rules, tools, and systems is uneven across the sector, with no established standards. Online safety legislation is desperately needed to create industrywide incentives and standards for child protection and online consumer safety.

Some who lobby against online safety bills do so under the so-called banner of free speech or privacy. Yet while privacy and free speech are essential, tech solutions exist and can be further developed to provide a win-win—to combat CSAM while preserving privacy and freedom of speech, as explained below.

Debates about online safety bills have lacked survivor voices and balance. They have been marked by hyperbole and exaggerated claims. Case-in-point is the debate pitting privacy vs. protection: In 2021, Apple announced child safety measures that were met with a cacophony of responses, both critical and supportive, from a variety of sources.[56] IJM applauded Apple for its proposed child safety initiatives related to iCloud Photos and Messages specifically. Two years later, Apple faced criticism[57] from child safety advocates and investors calling on Apple to do more to protect children from sexual abuse online, after having pulled their proposals. IJM was a proud signatory to the HEAT Initiative-led open letter calling on Apple to do more, as they initially promised.[58]

Common objections to Apple's announcement – and to online safety actions more broadly describe a slippery slope toward government abuses and mass surveillance.

Critics fear a hypothetical future risk while apparently dismissing a very real, current, and widespread harm: Untold numbers of vulnerable children have been and are being abused, exploited, and otherwise victimized by the continued production, possession, and distribution of such illegal images. In fact, due to uneven detection and reporting across tech companies, the world does not actually know how many children globally are sexually abused to produce CSAM, or how many such live videos, recorded videos, or images of child sexual abuse and exploitation are produced and shared online.

Yet, we know that tech companies have both the moral obligation and the combined resources necessary to create and implement advanced safety technologies to safeguard children. There is no doubt that the wealthiest companies in the world can use technology—signals, AI and other tools—to disrupt and report abuse on their apps, platforms, and devices.

The current conversations against proposed online safety legislation elevate the hypothetical corruption of solutions over the known and rampant misuse of existing technology to harm children. IJM deeply respects and values what survivors of child sexual abuse tell us: **Children are entitled to have every image memorializing the most painful and dehumanizing moments of their lives detected, reported, and removed from illegal circulation.**

---

[56] http://apple.com/child-safety/

[57] https://www.nytimes.com/2023/09/01/technology/child-sex-abuse-imagery-apple-safety-privacy.html

[58] https://www.documentcloud.org/documents/23935189-apple-letter-to-heat-initiative

In contrast, offenders have no legal or privacy right to create, possess, or share child sexual exploitation material. In fact, these acts undeniably violate the privacy of victimized children.

In the face of privacy arguments against child safety measures, a group of child sexual exploitation survivors and advocates, the Phoenix 11, have rightly asked:

> **What about *our* right to privacy? … It is our privacy that is violated each time an image of our child sexual abuse is accessed, possessed or shared.**[59]

While others have provided more technical reviews of Apple's plans, the voices of survivors have been muted. Accordingly, it is essential that governments consider the perspectives and recommendations of survivor leaders, such as from the Philippines Survivor Network[60], who have unique credibility to advise on building safe internet and digital ecosystems.

IJM has seen firsthand the harm and trauma children experience when sexual abuse and exploitation go undetected and unreported. We've also seen the very good reality of protection and hope when that abuse is uncovered and those victims are identified and brought to safety, with their offenders held to account.

Among those protected are individuals like Ruby*, Joy*, and Marj*,[61] Filipino survivors of what the U.S. Department of Justice calls "virtual child sex trafficking,"[62] who demand that governments require tech companies to make their platforms safe by design and "prevent, detect, report and remove child sexual abuse produced or shared on their sites…"

Joy* advocates for improved detection and reporting, informed by her own story of abuse:

> *"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 abused 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."*

Ruby*, now an adult survivor leader, describes the trauma she endured as a 16-year-old:

> *"I felt disgusted by every action I was forced to do to satisfy customers online. I lost my self-esteem, and I felt very weak. I became so desperate to escape, to the point that I would shout whenever I heard a police siren go by, hoping somebody would hear me."*

Marj* was first exploited at the age of 13 by her friend's older sister and explains:

> *"I was confused because I was just a child. I was shaking. Then, I felt different. I felt ashamed. But I also had nowhere else to go."*

---

[59] https://protectchildren.ca/en/press-and-media/news-releases/2021/phoenix-11-apple-statement

[60] https://osec.ijm.org/news-and-insights/news-updates/philippine-survivor-network-launched/

[61] https://www.ijm.org/news/survivors-need-us-to-address-online-sexual-exploitation-keep-children-safe

[62] https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction

The act of forcing her to take explicit pictures was painful enough, but as Marj shared with IJM: "… that abuse, I did not expect that it would spread. That it would be sent to other people."

Take it from these brave survivors and others[63]: Survivors are harmed first by the abuse they suffer and then repeatedly harmed again by offenders who share images and videos depicting their sexual exploitation. As explained further in the next section, on-device (or "client-side") and other innovative safety features – such as those proposed in 2021 by Apple – are a step toward protecting the privacy of survivors while reasonably respecting the privacy of users.

Despite references to Apple, this is not about any single company. Improving the entire tech industry's detection, disruption, and reporting of child sexual abuse is critical to protecting victims and survivors from ongoing harm. Innovations like on-device solutions hold significant promise precisely because of the potential to balance user privacy with child protection.

What *can* we expect from industry?

According to Sharon Pursey, co-founder of safety tech firm SafeToNet, "Technology exists that can detect and block child sexual abuse from being digitally created or consumed via images, video or livestream. Artificial intelligence, machine learning tools can detect new abusive content and be dropped onto applications, networks or operating systems of smart devices, preventing devices from rendering illegal sexual images of children."

And we need look no further than child safety policies and statements from big tech companies themselves to realize that child protection is at our fingertips. Namely, tech sector actions to address financial sextortion and even malware give governments clues on how to strike a balance between child protection and user privacy because, after all, companies are acutely aware of the need to strike this balance for commercial purposes.

For instance, Apple touts its Communication Safety tool as user-privacy-preserving, explaining that:

> *"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."*[64]

Meta-owned Instagram likewise reports that:

> *"[N]udity protection uses **on-device** machine learning to analyze whether an image sent in a DM on Instagram contains nudity. Because the images are analyzed on the device itself, nudity protection will work in end-to-end encrypted chats, where Meta won't have access to these images."*[65]

---

[63] The Canadian Centre for Child Protection, Survivors' Survey: Executive Summary (2017) https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf

[64] "About Communication Safety on your child's Apple device," February 28, 2025, https://support.apple.com/en-us/105069

[65] "New Tools to Help Protect Against Sextortion and Intimate Image Abuse," April 11, 2024, https://about.instagram.com/blog/announcements/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse

Google's safety blog in October 2024 explains how the company uses nudity filters to blur content. You will see a pattern:

> *"All of this happens **on-device** to protect your privacy and keep end-to-end encrypted message content private to only sender and recipient. Sensitive Content Warnings doesn't allow Google access to the contents of your images, nor does Google know that nudity may have been detected."*[66]

Finally, "*WhatsApp automatically performs checks* to determine if a link is suspicious. To protect your privacy, these checks take place entirely **on your device**. Remember, because of end-to-end encryption, WhatsApp can't see the content of your messages." [67]

Clearly, companies can address child exploitation while preserving user privacy—the principles and tools just need to be applied across the board to disrupt and deter abuse in the first place.

V. Conclusion and Recommendations: Deploy Multi-Sector Interventions at Scale.

In conclusion, most experts agree, there is no single approach to protect children from sexual abuse and exploitation. Rather, like other crime prevention efforts, effective prevention is multi-sectoral and multi-faceted.

Congress should enact public policies that:

- Maximize the actionability of CyberTipline reports to help law enforcement better identify victims and offenders.
- Require major tech companies to submit an annual transparency report disclosing their efforts and progress made to address CSAM.
- Empower federal courts to authorize trustees who can facilitate restitution safely for minor and foreign victims.
- Codify a notice and takedown regime that allows survivors to directly require companies to take down CSAM and prevent its recirculation.
- Incentivize companies to disrupt and deter the production and distribution of CSAM
- Increase the use of U.S. foreign assistance, like the Child Protection Compacts, to keep kids safe online and hold American perpetrators accountable.

Companies should prioritize the safety and privacy of victims, by expediting detection, reporting and removal of CSAM. Early detection and reporting allow law enforcement to do their job of bringing offenders to justice and victims to safety. Based on IJM prevalence studies across crime types, replacing offender impunity with accountability can also serve to prevent future harm by deterring offenders.

---

[66] "5 new protections on Google Messages to help keep you safe," October 22, 2024, https://security.googleblog.com/2024/10/5-new-protections-on-google-messages.html?m=1

[67] https://faq.whatsapp.com/393169153028916/?cms_platform=web

The sheer scale of CSAM necessitates technological prevention in video-chat and messaging apps. With U.S. law enforcement reporting having only "infiltrated .0001 percent of the actual abuse that's occurring,"[68] more must be done upstream. Critical safeguards should be deployed to disrupt the production of new CSAM. Safety technology that can detect and disrupt child sexual abuse in real-time already exists.[69] Use of this type of technology could help disrupt livestreamed sexual abuse, whether in trafficking, grooming or sextortion contexts to protect children, including in the U.S.

A safety-by-design approach can play a central role in making it harder for criminals to abuse kids online in the first place. And when it does happen, companies need to quickly detect and report the maximum amount of information so law enforcement can do their job. As governments replace offender impunity with offender accountability, that too will serve to prevent future harm by deterring a subset of offenders. Simply put, safety by design combined with effective justice responses can create a shield for children, exponentially increasing their protection online and in the real world – both before and after initial harm. The combination of these two responses can ultimately change societal norms when it becomes harder and more costly for offenders to find and create CSAM.

Today's phones, tablets, apps and platforms are not safe by design precisely because they are built without the technology to disrupt and deter the production and distribution of CSAM at the source. We should no longer take this reality for granted; we should no longer accept this perverse status quo, that our technology is at the full, unmitigated disposal of offenders to create new child abuse images, videos and livestreams without any friction. Congress should incentivize tech companies to build their products and platforms safe by design.

Scale of Harm's research finding that nearly half a million Filipino children were abused to create CSEM is a prime example of what happens when tech platforms have no guardrails. Without tech safeguards designed to prevent abuse, offenders operate with ease, anonymity, and impunity.

While internet service providers should block access to URLs hosting known CSAM and also ensure the CSAM is deleted or removed, other tools can prevent the upload of known CSAM online in the first place, as reported by the Internet Watch Foundation.[70] Such mitigation measures are critical to stemming the growing tide of child sexual abuse online.

In addition to detecting and removing CSAM already online, companies should move increasingly upstream to prevent CSAM production and distribution in the first instance, including though on-device ("client-side") technologies. These technologies can be privacy protective. With industrywide change, offenders can have nowhere to hide and nowhere online to abuse children with impunity.

---

[68] "*On These Apps, the Dark Promise of Mothers Sexually Abusing Children,"* Michael Keller, New York Times, Dec. 7, 2024, https://www.nytimes.com/2024/12/07/us/child-abuse-apple-google-apps.html?unlocked_article_code=1.fk4.RJ2i.dRBch4XE-_0O

[69] https://safetonet.com/harmblock/

[70] https://annualreport2022.iwf.org.uk/tech-rd/our-role-in-the-safety-tech-challenge/

The challenges are complex, but child protection solutions – in the justice, tech and financial sectors – already exist. It is time to prioritize broad deployment already available tools.

The status quo of allowing perpetrators to produce and stream child sexual abuse live without detection, reporting or disruption is technologically indefensible and enables crimes at a mass scale.

The good news is we do not have to tolerate a world where young children are defenseless to sexual violence and abuse online or where our internet sites and group chats are poisoned with child sexual abuse material.

We must demand an end to the status quo and work for a world where all children are safe, our apps and platforms are safe by design and our devices are incompatible with child sexual abuse material.

You have the power to challenge this global “wild west” of unbridled digital abuse. You have the power to shift the balance away from impunity to justice and protection. You must seize this opportunity to protect kids online. The time is now.

* * *

Annex I:

Case Examples: American Offenders Committing Online Child Sex Abuse, Including Livestreaming of Children in the Philippines.

The following case examples – from every U.S. state represented by members of the Senate Judiciary Subcommittee on Crime and Counterterrorism – demonstrate examples in which American offenders sexually abused and exploited children online, including Filipino children.

Texas

- Exploiting Philippine minor through Facebook lands Texan in federal prison: "BROWNSVILLE, Texas – A 47-year-old Harlingen man has been ordered to federal prison following his conviction of receiving child pornography, announced U.S. Attorney Jennifer B. Lowery… At the time of his plea, Machietto admitted that from Dec. 1, 2017, to June 1, 2018, he used Facebook to communicate with minor girls located in the Philippines."

- Corpus Christi man gets life for exploiting Filipino children
  "CORPUS CHRISTI, Texas – A 59-year-old local resident has been ordered to serve the rest of his life in federal prison following convictions for several child exploitation offenses including foreign travel to engage in illicit sexual conduct with three minors, announced U.S. Attorney Jennifer B. Lowery."

- Convicted Child Predator Sentenced to 30 Years for Possessing, Transporting CSAM Following HSI Houston Investigation

- Texas Man Who Bragged Online About Sexually Assaulting Minors, Sentenced to 30 Years for Producing CSAM

South Carolina:

- Seven Men Sentenced for Their Roles in an International Child Exploitation Crowdsourcing Conspiracy

  "Seven men from around the country were sentenced today and yesterday for participating in an international child pornography production conspiracy…"

- Beaufort Man Sentenced to 14 Years in Federal Prison for Possession of Child Pornography

  "CHARLESTON, SOUTH CAROLINA – Leonardo Rubio, 23, of Beaufort, South Carolina, was sentenced to 14 years in federal prison after pleading guilty to possession of child pornography."

- Pickens Man Sentenced to 10 Years in Federal Prison for Child Pornography Offense

  "GREENVILLE, SOUTH CAROLINA –Matthew Leon Arotin, 63, of Pickens, was sentenced to 10 years in federal prison after pleading guilty to possession of child

pornography. He was also ordered to pay $68,000 in restitution to the victims whose images he possessed."

Tennessee:

- Child porn operation raided in Philippine school

  "MANILA, Philippines (AP) — Government agents raided an Internet child porn operation based in a Philippine school and arrested its president and eight other people, investigators said Tuesday."
  "He said the Internet operation was owned by an American from Tennessee, who rented two rooms for 40,000 pesos ($900) in a bungalow separate from the classrooms but within the school compound."

Alabama:

- Alabama Man Sentenced to 160 Years of Imprisonment for Soliciting Videos and Webcam Shows of Filipina Children Being Sexually Abused

  "A federal judge sentenced an Alabama man today to 160 years' imprisonment for using internet applications to seek images and live transmissions of the violent sexual abuse of Filipina children as young as five years old."

Missouri:

- Sex Offender Indicted for Producing Child Porn Overseas, Distributing Child Porn Online

  "SPRINGFIELD, Mo. – Tammy Dickinson, United States Attorney for the Western District of Missouri, announced that a prior sex offender was indicted by a federal grand jury today for producing child pornography with five child victims in the Philippines and for distributing child pornography over the Internet."

- Man Convicted for Running Four Dark Web Child Sexual Abuse Websites

  A federal jury convicted a Missouri man yesterday for running four websites dedicated to sharing images of child sexual abuse.

- St. Louis County Man Accused of Paying to Watch Sexual Abuse of Children

  A man from St. Louis County, Missouri appeared in court this week to answer charges accusing him of coercing children overseas into engaging in sexually explicit conduct… A motion seeking to have Smajlovic held in jail until trial says Homeland Security Investigations identified traffickers in the Philippines who were providing access to pre-produced child sexual abuse material

Illinois:

- Chicago Man Sentenced to 30 Years in Federal Prison for Enticing Girls in the Philippines To Produce Sexually Explicit Images:

"A Chicago man has been sentenced to 30 years in federal prison for enticing at least nine girls in the Philippines to produce sexually explicit photos and videos of themselves and send them to him."

- Decatur Man Sentenced to 50 Years in Prison for Sexually Exploiting Minors:

  "At the sentencing hearing, the government presented evidence that Dial directed the sexual abuse of three minors, including a two-year-old child, and ordered that the abuse be recorded."

Minnesota:

- Ramsey County Man Indicted For Sexually Exploiting Children In The Philippines:

  "United States Attorney Erica H. MacDonald today announced a fourteen-count federal indictment charging ALAN DENNIS WOLFF, 56, with sexually exploiting children in the Philippines."

Delaware:

- Delaware Man Sentenced to 135 Months in Federal Prison for Second Conviction Involving Child Sexual Abuse Material

  "Law enforcement later found over 2,000 files containing CSAM on Janvier's phone. The files found on the device included images and videos of prepubescent minors, to include infants and toddlers, and materials portraying bondage and bestiality. "

Connecticut:

- Waterbury Man Sentenced to Prison for Child Exploitation Offense

  "The investigation further revealed that Bright had engaged in sexually explicit conversations with other minor females in the Philippines through Facebook, and that he sent one of those minor victims a nude picture of himself."

New Jersey:

- Mercer County Man, Former Pilot, Sentenced to 12 Years in Prison and Lifetime Supervised Release for Travelling to Philippines for Illicit Sexual Conduct:

  "A Mercer County, New Jersey, man … was sentenced today to 144 months in prison for illicit sexual conduct abroad, including production of child pornography… From as early as 2013, Maile traveled to the Philippines and had sexual contact with two minor sisters. Maile had extensive, explicit chats with the minors' pimp to arrange these meetings."

- Essex County Man Sentenced to 30 Years in Prison for Producing Child Pornography in New Jersey and Abroad

  "An Essex County, New Jersey, man was sentenced today to 360 months in prison for producing multiple videos depicting the sexual assault of children… Further investigation revealed that on multiple occasions, Del Prado sexually assaulted children

in the Philippines and transmitted video recordings of those assaults into the United States."

Annex II:

Additional Case Examples: Livestreamed Child Sexual Abuse, CSAM Production

Below are additional case examples where offenders sexually abused and exploited children, including directing and consuming the abuse in real-time via live video. Most livestreaming cases are never identified or prosecuted and others are likely unreported in the news. These are "live crime scenes" committed daily on common, popular messaging and video-chat applications easily available on Apple and Google app stores.[71]

Date	Abuse Description	Age of victim(s)
Livestreaming		
07/19/19 Man gets 30 years for making child porn using kids in PH | Inquirer	US-based offender directed Filipino facilitators to perform sexual acts on children (infants to age 10) while he watched via Skype, in exchange for money.	Infant to 10 years
04/08/2022 District of South Carolina | Beaufort County Man Sentenced to 30 years for Production of Child Pornography | United States Department of Justice	US-based offender admitted to assaulting a 22-month-old victim approximately five times between September 2019 and December 2019 and live streaming these assaults over Skype to an offender in the UK.	22 months
11/15/2021 British pensioner, 68, jailed for 12 years relating to sexual exploitation of child in Philippines | Daily Mail Online	UK-based offender admitted to 67 separate offences, including using Skype to contact the mother of the child in the Philippines and making online payments in order to facilitate the sexual exploitation of the child victim and sending images of the abuse.	6

[71] https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

Date	Abuse Description	Age of victim(s)
Livestreaming		
11/05/2021 Southern District of Ohio | Shelby County man sentenced to 27 years in prison for sending money to Filipino mothers in exchange for child pornography | United States Department of Justice	Over a 3-month period, US-based offender directed Filipino facilitators over Skype to share sexual images and videos of their children in exchange for payments via MoneyGram.	7
08/08/19 Office of Public Affairs | Kansas Man Sentenced for Producing Child Pornography | United States Department of Justice	US-based offender travelled to the Philippines to film himself engaging in sex act with minor females as well as communicating via Skype with a child's mother and directing her to livestream CSEM depicting an 8-year-old female.	8
05/23/2022 Twisted paedo 'used Fornite & Call of Duty to prey on kids & force them to pose naked as cops find 2,000 abuse images' | The US Sun (the-sun.com)	Previously convicted Spain-based offender made 81 payments to at least 26 victims between the ages of eight and twelve using online gaming platforms, then convinced them to appear naked on Skype.	9
05/23/2019 Ex-British army officer jailed for online child sex abuse in PHL | GMA News Online (gmanetwork.com)	Over a 2-year period, UK-based offender made nearly 50 payments to direct and view livestreamed child sexual exploitation material (CSEM) of multiple Filipino children via Skype.	9
12/18/20 Businessman admits paying for online child abuse from Philippines (bbc.com)	Over a 2-year period, UK-based offender directed an adult facilitator for livestreamed abuse of Filipino children (as young as 10 years old) via Skype, in exchange for over £5,500.	10

Date	Abuse Description	Age of victim(s)
Livestreaming		
10/06/21 Jail for Victorian man who exploited girls in the Philippines (theage.com.au)	Australia-based offender directed 13-year-old Filipina girl over Skype to undress and perform lewd acts in exchange for money. Other victims were aged 11 and 12.	11, 12
02/01/2022 Winnipeg man wanted in Philippines for allegedly paying to watch child sex abuse: search warrant | CBC News	Canada-based offender is wanted for wiring thousands of dollars to traffickers in the Philippines for child exploitation offenses including livestreaming the sexual abuse of children via Skype. This is also the case of "Daisy's Destruction" (the video series of an 11-year-old girl being raped, tortured, and murdered).	11
02/28/2022 Ex-DJ Mark Page 'arranged sex with Philippine children' (bbc.com)	UK-based offender is charged with multiple child exploitation offenses that occurred from 2016 – 2019, including directing Filipino children to perform sexual acts over Skype in exchange for money.	12
06/30/2018 Five years in jail and worldwide travel ban for British teacher who wanted to abuse young Filipino children - National Crime Agency	UK-based offender sent at least 15 wire transfers to adult facilitators in the Philippines for images and livestreamed videos of children being sexually exploited; in addition, he attempted to arrange travel to the Philippines over Skype conversations.	12, 13 (he describes wanting to exploit children ages 4, 6, 9).
02/06/2022 Brooklyn Porn Arrest: Instagram, Skype Used to Target Kids, Feds Say – NBC New York	Over a 4-year period, US-based offender engaged in sexually explicit Skype communications with at least eight underage victims, in the U.S. and abroad, between the ages of 13 and 17. He was charged with producing child pornography after prosecutors alleged, he directed children to send him sexually explicit images and videos after targeting them via Skype.	13 through 17
11/10/2021 Man paid $40 to watch Filipino child abuse | The West Australian	On multiple occasions, Australia-based offender used Skype to direct livestreamed shows of girls under 16 in the Philippines in exchange for money. The 57-year-old Victorian man was later told that the girl, aged between 13 and 15, had to be taken to hospital after the first recording.	13, 15

Date	Abuse Description	Age of victim(s)
Livestreaming		
02/21/2019 Eastern District of New York | Queens Man Sentenced to 15 Years' Imprisonment for Producing Child Pornography | United States Department of Justice	In two months, this US-based offender paid and directed Filipino traffickers to sexually abuse children in live video calls, recording over 50 abuse videos, some livestreamed via Skype.	Children, NA
12/14/2023 Office of Public Affairs | Man Sentenced to 25 Years in Prison for Paying Philippine Sex Trafficker to Live-Stream Child Sex Abuse | United States Department of Justice	A Maine man was sentenced to 25 years in prison for producing and distributing child sexual abuse material (CSAM) depicting a minor in the Philippines. The defendant frequently recorded livestreamed video calls which he used to instruct others to sexually abuse children during their own calls.	Children, NA
07/25/2019 Man jailed for streaming child sex abuse from Philippines (bbc.com)	A sales advisor who was the first person in Scotland to be convicted of live streaming abuse of children has been jailed for nine years. "Bell has instructed said abuse to take place by verbal and written communication to persons in the Philippines via internet message services."	Children, NA
01/25/2024 Sydney Man Faces Charges for Remote Child Abuse Orders | Mirage News	A Sydney man has appeared in the Downing Centre Local Court after being charged with allegedly paying to watch online as a child overseas was sexually abused.	Children, NA
10/14/2022 Man appears in court charged with sending money to Philippines to live stream child sexual abuse - Manchester Evening News	The 71-year-old was charged with arranging/facilitating the commission of a child sex offence and making indecent photographs of a child. The National Crime Agency (NCA) received information that the suspect had made an "illicit money transfer" to the Philippines.	Children, NA

Date	Abuse Description	Age of victim(s)
Livestreaming		
05/16/2019 Convicted child sex offender behind bars again for illicit Skype relationship with Filipino children under the age of 12 (smh.com.au)	Over a 4-and-a-half-year period, Australia-based offender paid a Filipino family over $26,000 for continued livestreamed CSEM of two sisters (age 2 and 7 when the abuse began) via Skype.	2, 7
05/17/2017 'Dreadful' Devon child abuser jailed for 18 years - BBC News	UK-based offender paid Filipino facilitators and directed them via Skype as he watched and recorded 102 hours of livestreamed sexual abuse of up to 46 child victims.	2 through 15 years
10/19/21 Retired South Australian public servant Ian Schapel, 67, sexually exploited kids in the Philippines | Daily Mail Online	Australia-based offender directed adult Filipina women over Skype to perform sexual acts on children in exchange for money; he had at least 13 victims aged between three and nine years old who were abused on 74 occasions.	3, 9
07/29/29 Paedophile who paid Filipino mums for pictures of naked daughters is jailed | Metro News	Over a 3-year period, UK-based offender communicated with traffickers in the Philippines via Skype and provided 36 payments for CSEM of girls aged 5 to 12 years old.	5, 12
04/12/2019 Paedophile directed child abuse films on Skype 7,000 miles away from his home | Metro News	Over a 3-year period, UK-based offender paid 8 traffickers to carry out sex acts and livestream the abuse of female children (aged 6 and 9) in the Philippines via Skype.	6, 9