Testimony of John Tanagho, International Justice Mission
Before the
House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

"Children are Not for Sale: Examining the Threat of Exploitation of Children in the U.S. and Abroad"
September 13, 2023

Chairman Biggs, Ranking Member Lee – thank you for the invitation 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 authorities in 31 program offices in 16 countries to combat modern slavery, violence against women and children, and other forms of abuse. Since 1997, we have supported governments to bring victims to safety and wholeness, hold perpetrators accountable, and strengthen justice systems.[1]

IJM's Center to End Online Sexual Exploitation of Children protects children in the Philippines and scales the fight against this crime globally. The Center leverages and shares effective practices and models from IJM's Philippines program to enhance justice system and private sector responses to online sexual exploitation, resulting in sustainable child protection and offender accountability.[2]

I appreciate the opportunity to provide testimony at such a critical moment. Put plainly – we are at a crisis point when it comes to child sexual abuse and exploitation online.

At an alarming scale, child sex offenders from around the world seek out traffickers online in countries like the Philippines, paying them to livestream the sexual abuse and exploitation of specific children in specific ways as directed by these offenders in real time. And this represents just one form or modus operandi of child sexual abuse online, separate from financial sextortion, grooming, non-consensual sharing of intimate images, and other child abuse online.

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

[2] Learn more about the Center's work at ijm.org.ph/center and on LinkedIn. Contact us at endosec@ijm.org.

I spent seven years living in the Philippines, leading IJM teams to protect children from this particularly pernicious form of trafficking, where vulnerable victims are trafficked to produce new child sexual exploitation material, or CSEM[3], especially in livestreams.

In IJM's casework experience from 2011 to 2023, demand-side offenders, including from the U.S., use popular internet platforms with live video and chat functions to issue graphic and specific abuse instructions. This sexual abuse is livestreamed for the offender's sexual consumption and documented in photos and videos that create new CSEM. But this is no virtual crime. This is the in person sexual abuse of children by adults in the Philippines while foreign offenders watch and direct the abuse online in real-time for a fee.

This is basically pay-per-view CSEM, live on-demand.

Based on IJM's experience supporting over 342 Philippine government-led law enforcement operations, the abusive conduct usually includes forcible sexual penetration, constituting rape in the Philippines and many other jurisdictions. Children are forced to engage in sex acts with other children, sexually abused by an adult, and sometimes harmed in other degrading ways, such as in bestiality.[4] This is consistent with the severity of harm to children in extreme child sexual abuse material globally. In 2022, the U.K. based Internet Watch Foundation 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).[5]

In the Philippines, victims are abused for **two years** on average, in part because the abuse goes undetected and unreported online. According to a 2020 study published by IJM, the median age

---

[3] 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.

[4] 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

[5] 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/.

of victims is only 11 years old, and 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 sexually abused in a livestream. This is consistent with IJM's experience, and payment amounts typically increase with the number of children abused, the severity of abuse, and the younger age of victims.

Congress should make no mistake here: These are not just pictures or videos online. Behind every livestream is a real child, suffering serious emotional and physical trauma. Even after being brought to safety by law enforcement, there is no end to their continued exploitation and the invasion of their privacy, as offenders share and trade images and videos of child abuse in encrypted messaging apps and online.

I have heard from survivors of this abuse, who recount its devastating impact. Ruby*[6], who was sexually abused in livestreams as a 16-year-old, recalls how the abuse eroded her will to live:

> **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.**[7]

IJM *Scale of Harm* Study Measures the Prevalence of this Crime

With that backdrop, I will now share data on the prevalence of this crime in the Philippines. In 2021, International Justice Mission, together with the University of Nottingham Rights Lab, a world-leading human trafficking research institution, launched the *Scale of Harm* project to develop and implement a mixed-methodology producing prevalence estimates of trafficking of children to produce new CSEM, including via livestreaming, in the Philippines.

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.

---

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

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

Prior externally validated IJM prevalence studies[8] on various forms of violence have proven that increased perpetrator accountability – through detection, arrest, and prosecution – can have a disproportionate impact on reducing crime within the context of a trauma-informed, holistic justice system and societal response. 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.[9]

IJM's *Scale of Harm* study is unique in that it employed survivor engagement throughout. Alongside delivering a national household survey, survivor engagement was a critical component. Survivor consultants and leaders informed and co-designed the survey by drawing from their lived experience of exploitation and community knowledge in the Philippines. This includes co-designing and enhancing research instruments such as the survey questionnaire and protocols. Survivor consultants also co-designed and facilitated two focus group discussions with Filipino survivor leaders from the Philippine Survivor Network.

IJM's *Scale of Harm* study reveals a significant and alarming national prevalence of trafficking of children to produce new CSEM.[10] In 2022, nearly **half a million Filipino children**, or 1 in 100 Filipino children, were sexually abused by adults 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. The *Scale of Harm* summary report provides additional findings along with our seven recommendations, co-developed with survivor leaders.

Governments Like the U.S. Must Address Demand-Side Offenders Who Fuel Ongoing Abuse

Governments must holistically address demand-side offenders within their jurisdictions. This includes requiring tech and financial sector detection and reporting, applying effective justice system responses, and implementing upstream offender prevention efforts.

---

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

[9] 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.

[10] 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 testimony, according to available data, the United States is the number one demand-side country of offenders paying for and directing abuse of Filipino children. According to a 2020 IJM study, 34% of Philippine cases involve U.S.-based offenders.[11] Moreover, according to an April 2023 report by the Philippine Anti-Money Laundering Council, since 2015, individuals in the United States have apparently 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.[12] This 18-month period saw nearly **$7.3 million in 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 what online sexual exploitation of children is and who is driving it. Online sex offenders direct and cause live sexual abuse by paying and instructing in-person traffickers to violate young children of specific ages, at specific times, in specific ways. They produce child sexual abuse material every time they watch and record the new abuse from the comfort of their homes. Plainly put, demand-side sex offenders are the minds and money behind the most horrific child abuse imaginable.

There can be a temptation to view these offenses as "image-based" or "online." But real, physical sexual abuse is often the result of the demand created by sexually motivated offenders, even if they commit the abuse from the comfort of their homes. Detective Inspector Jon Rouse APM, the 39-year veteran of Internet Crimes Against Children 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:

[11] 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.

[12] 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.

> **[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.[13]**

In IJM's 12-years of experience 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. Hiding behind their screens, they abuse the most vulnerable children around the world live in video calls. And in many countries, these offenders fail to be held accountable in ways commensurate to the harm they caused.[14]

Offenders who use the internet to abuse children overseas or view CSAM also pose a threat to commit hands on abuse in the U.S. and other countries. Recent research from the Australian Institute for Criminology suggests that individuals who view livestreamed CSAM have already crossed the psychological barrier to contact offending, by directing and watching the live sexual abuse of a child online – which is on par with abusing the children themselves.[15] 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.[16]

Nearly half of respondents to a recent survey in the Stanford Internet Observatory's Journal of Online Trust and Safety said they had sought direct contact with children through online platforms after viewing CSAM, and 58% reported feeling afraid that viewing CSAM might lead to them committing abuse in person. Moreover, according to research by Finnish NGO Protect Children who surveyed CSAM users, "nearly half (42%) of the respondents reported that they had sought direct contact with a child through online platforms after viewing CSAM, and 58% reported feeling afraid that viewing CSAM might lead to sexual acts with a child or adult."[17]

---

[13] 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

[14] International Justice Mission. *Falling Short: Demand-Side Sentencing for Online Sexual Exploitation of Children - Composite Case Review, Analysis, and Recommendations for the United Kingdom* (October 2020). https://paragonn-cdn3.ams3.cdn.digitaloceanspaces.com/ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf

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

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

[17] https://www.suojellaanlapsia.fi/en/post/redirection-final-report-3

Moreover, even those offenders who begin by viewing, possessing, and sharing CSAM – without producing – fuel the demand for new abuse of children. In their Exploiting Isolation report released in June 2020, Europol states:

> The demand for such [CSAM] material 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 victimization of children.[18]

Research by Michael Salter (Associate Professor of Criminology at New South Wales University) reveals strong links between viewing violent and extreme adult pornography and child sexual abuse across the U.S., U.K. and Australia.[19] Professionals at the UK-based charity Lucy Faithful Foundation who help men overcome viewing CSAM report that a common pathway to offending is heavy pornography use leading to habituation and desensitization. Analysis of qualitative data in a CSAM dark web survey by Finnish NGO Protect Children revealed that respondents may begin searching for CSAM when they are "bored", "unexcited" or "tired" of adult pornography.[20] In addition to achieving prevention through offender accountability leading to deterrence, governments should seek to go upstream to understand and disrupt some pathways to CSAM offending.

With such a significant demand-side offender problem, the United States should lead the way by ensuring that local, state, and federal law enforcement 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. It is therefore encouraging to see national governments stepping in. For instance, as part of a comprehensive partnership, IJM supported Philippine authorities through strengthening justice system responses to bring to safety over 1,100 victims and others at-risk. Justice system capacity to address these crimes in

---

[18] 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.

[19] https://www.linkedin.com/feed/update/urn:li:activity:7067105756017225729/?commentUrn=urn%3Ali%3Acomment%3A(activity%3A7067105756017225729%2C7067213251788374016)&dashCommentUrn=urn%3Ali%3Afsd_comment%3A(7067213251788374016%2Curn%3Ali%3Aactivity%3A7067105756017225729)

[20] https://www.suojellaanlapsia.fi/en/post/redirection-blog-02-russian-speaking-csam-users

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 four years of operation, the Philippines Internet Crimes Against Children Center, or PICACC, made possible the safeguarding of 644 individuals from online sexual exploitation and the arrest of 131 suspects. With more widespread global cooperation, imagine how much more could be done.

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

Protecting Children Globally Requires a Strong US Policy Response

As child sexual abuse online rages, governments can help reduce the production of first-generation child abuse materials, including livestreamed exploitation. Government legislation should create requirements or standards for tech companies to make their platforms and products safe by design. We need to expect more technological prevention from companies, not simply more reporting.

Unfortunately, global tech platforms, including those headquartered in the U.S., remain fertile ground for child sexual abuse and exploitation online, according to reporting from 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.[21]

It is encouraging, therefore, that as of this testimony, governments such as the UK, EU, and Canada are stepping up with their own attempts to pass online safety legislation to protect children. Without strengthened laws, child exploitation online is a global crisis spiraling out of control. For example, in 2022, NCMEC's CyberTipline received reports containing 37.7 million videos related to suspected child sexual exploitation, 8.3 million of which were unique.[22] To put that in context, there are about 649,692 movies[23] in existence in the world. This means there are

[21] 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.

[22] https://www.missingkids.org/test/cybertiplinedata-draft

[23] https://www.imdb.com/pressroom/stats/

roughly 1,177.53% more unique suspected child sexual exploitation videos reported to NCMEC in 2022 alone than movies produced throughout history.

As the host of major multi-national tech companies weaponized to abuse children, the U.S. has a critical role to play. That's why IJM supports the EARN IT Act, to change the incentives and ensure tech companies do everything in their power to prevent child sexual exploitation on their platforms.

Online child sexual exploitation is clearly a global crime, requiring a coordinated global response by government, civil society and the private sector. For instance, while NCMEC is a congressionally mandated, U.S.-based organization, of the 32 million reports that the CyberTipline received in 2022, nearly 90% resolved to a location outside of the U.S. The sheer amount of CyberTipline reports consistently outpace law enforcement's capacity to respond in almost every country, especially in developing contexts.

IJM has firsthand experience working alongside under-resourced law enforcement partners in responding to this challenge. In partnership with NCMEC and through funding by the U.S. State Department's Office to Monitor and Combat Trafficking in Persons, among other partners, IJM's Center to End Online Sexual Exploitation of Children 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, and the Philippines.

The extension of the preservation window for CyberTipline report contents, as proposed in both the EARN IT Act and the REPORT Act, will help give law enforcement much needed time to triage and respond to CyberTipline reports. Critically, these proposals will also improve the quality of reports electronic service providers (ESPs) submit, which can have a downstream impact of more victims identified and arrests made.

In this session of Congress alone, there have been five bills introduced in the House of Representatives with the aim of protecting children from online sexual exploitation: EARN IT Act, Project Safe Childhood Act, Preventing Child Sex Abuse Act, REPORT Act and Child Online Safety Modernization Act. (Relevant legislation in this issue area introduced in the Senate this session includes the STOP CSAM Act and Kids Online Safety Act, which do not have House companions at the time of this hearing.) These legislative initiatives encompass a range of provisions, all geared toward promoting greater transparency within the tech industry, expanding the scope of detection and reporting of CSAM, implementing safety by design principles, extending the period for preserving content, and reducing the time it takes to remove illicit material from online platforms. These bills, though distinct in their approaches, share a common goal: safeguarding children in the digital realm.

While none of these bills is a silver bullet that will entirely eliminate the issue, they each offer a significant step forward in providing enhanced protection and preserving the dignity of children worldwide. By supporting and implementing these measures, we have the potential to foster safer online communities – not only for our nation's children but also for children across the globe. While we welcome all legislative efforts to protect children online, IJM believes that the EARN IT Act presents the most promising opportunity to cultivate safer online communities. By establishing a commission of diverse experts charged with collaboratively formulating best practices, this legislation has the potential to guide NGOs, tech companies, civil society organizations, and government bodies toward the most effective approach to addressing online sexual exploitation of children. It will ensure that tech companies are doing everything in their power to prevent child sexual exploitation on their platforms, and even enhances the reporting and preservation requirements for tech companies to the CyberTipline.

From IJM's experience in training international law enforcement partners on CyberTipline investigations,[24] it is clear that updates are desperately needed to the existing reporting framework. IJM supports the enhanced reporting requirements in the EARN IT Act that will improve consistency, quality and timeliness in reports of suspected child sexual exploitation sent from online service providers to the CyberTipline.

Moreover, a recent report from the Organization 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.[25] We urgently need this type of transparency from tech companies to hold them accountable for their actions and 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.

Privacy vs. Child Protection 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 companies, with

[24] https://www.missingkids.org/blog/2022/online-child-abuse-has-no-borders-ncmec-training-out-of-africa

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

no established standards or action. That is why online safety legislation is essential, to create industrywide standards for child protection and consumer safety online.

But why, as of this testimony's date, has U.S. Congress, the United Kingdom, European Union, Canada and others not already passed such online safety legislation? Globally, proposed online safety legislation has been lobbied against by a host of actors. Most of them lobby against online safety legislation under the so-called banner of data or user privacy or free speech. But take the case of Australia, a well-respected democracy and Five Eyes' nation, which passed an online safety bill in 2021 requiring tech transparency and safety by design.[26] Free speech and privacy are alive and well in Australia. And if Congress passes online safety legislation to protect kids, the sky won't fall here either.

While privacy is essential, innovative solutions exist and can be further developed to make data protection and child protection compatible, striking the right balance.

Crucially, debates about online safety bills have lacked survivor voices and balance. They have been marked by hyperbole and exaggerated claims. In considering how best to regulate digital spaces in a post-pandemic world, it is essential that governments listen directly to survivor leaders, including those from the Global South who are speaking out about the issue. Survivor leaders, such as from the Philippines Survivor Network, have unique expertise and credibility to advise on building a digital landscape that gives no opportunity for exploitation. They have already consulted on both the UK Online Safety Bill and[27] the World Economic Forum Global Principles for Digital Safety,[28] and have advocated for passing of EU legislation.[29]

Case-in-point in 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.[30] International Justice Mission, through its Center to End Online Sexual Exploitation of Children, applauded Apple for its proposed child safety initiatives related to iCloud Photos and Messages specifically. Two years later, Apple faces criticism from child safety advocates and investors calling on Apple to do more to protect children from

---

[26] https://www.esafety.gov.au/newsroom/whats-on/online-safety-act

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

[28] https://www3.weforum.org/docs/WEF_Global_Charter_of_Principles_for_Digital_Safety_2023.pdf ("Our thanks to Ruby, Liberty and Joy (pseudonyms), International Justice Mission IJM, Philippines Survivor Network").

[29] https://globalsurvivornetwork.org/stories/philippine-survivors-urge-eu-parliament-and-union-council-for-stronger-legislation

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

sexual abuse online, after having pulled their proposals. IJM is a proud signatory to the HEAT Initiative-led open letter calling on Apple to do more, as they initially promised.[31]

While Apple's proposed initiatives were imperfect – and significant room exists across the tech sector to improve detection, disruption, and reporting of child sexual abuse – Apple's proposed moves were a positive step forward.

Strong opposition to Apple's announcement – and to online safety actions more broadly – are primarily presented under the banner of "privacy." Common objections describe a slippery slope toward government abuses and mass surveillance. To be clear, the child safety solutions proposed by Apple have not been corrupted for such dire ends.

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 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. But we do know from *Scale of Harm*, that nearly half a million Filipino children are estimated to have been sexually abused to create image, videos, and livestreams for sale to offenders.

At the same time, 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.

The current conversations surrounding proposed tech online safety actions and bills risk elevating the hypothetical corruption of child safety solutions over the known and rampant misuse of existing technology to harm children. As a survivor-centered organization, IJM deeply respects what survivors of child sexual abuse tell us and others in this space: Children are entitled to have every image memorializing the most painful and dehumanizing moments of their lives detected, reported, and removed from illegal circulation.

In contrast, offenders have no legal or privacy right to illegally create, possess, or share child sexual exploitation material. In fact, these acts undeniably violate the privacy of victimized children. Unlike the hypothetical harm critics fear, the global crisis of child sexual abuse and exploitation is all too real.

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

In the face of privacy arguments against Apple's child safety measures, a group of child sexual exploitation survivors, the Phoenix 11, have rightly identified this advocacy in the name of privacy as incomplete:

> **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.**[32]

While others have provided more technical reviews of Apple's plans, the voices of survivors have not been sufficiently prominent. 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.

Since 2011, IJM has supported law enforcement in the Philippines to safeguard over **1,180 victims and at-risk individuals** from sexual exploitation by in-person traffickers whom online sex offenders pay for new abusive content. Among those protected are children like Joy, Ruby, Cassie, Chang, and Marj.

Joy,* a survivor leader, 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 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.**

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 just 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:

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

> **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.**

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[33]: Survivors are harmed first by the abuse they suffer, and then repeatedly through the violation of their privacy by offenders who share images and videos depicting their sexual exploitation. As explained more 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.

While Apple's situation is exemplary, this is not about any single company. Improving the 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.

Fortunately, child safety leaders within the tech sector have expressed commitment to address this abuse, with the Technology Coalition's Executive Director writing in its first-ever annual report:

> We are resolved to drive forward the improvements in technology and systems that will ultimately eradicate the online sexual abuse and exploitation of children on our platforms.[34]

Child safety announcements by Technology Coalition members, including Apple, TikTok, Meta, and Google, are steps in the right direction, with much more to be done. Yet the past and ongoing backlash against these efforts and online safety legislation could discourage the development and adoption of additional real-world protections for children. That is why online safety legislation is urgently needed, because children cannot rely on individual companies to successfully navigate these child safety debates.

---

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

[34] The Technology Coalition Annual Report (2021). https://www.technologycoalition.org/annual-report

And for victims and survivors, none of this is hypothetical; instead, it is very real and urgent. There are plain reasons why the wheel of child sexual abuse online is spinning fast: there is minimal detection, reporting, mitigation or disruption and impunity is the norm. Offenders are not afraid of being detected by police as they hide their abuse in encrypted messaging apps and video calls, and they know that online platforms do little to detect or prevent their ongoing abuses. And this is where the debate about the details of online safety legislation is very practical for victims. Maybe if all platforms deployed tools to detect and report new or "first-generation" CSAM, children would be spared dozens or hundreds of specific acts of sexual abuse and exploitation. Maybe victims would be identified and brought to safety weeks or months after abuse, instead of years later.

Conclusion: Justice & Tech Solutions Exist, Ready for Deployment at Scale

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

Companies must 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.

At the same time, the sheer scale of child sexual abuse material necessitates technological prevention in video-chat and messaging apps. 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, such as SafeToWatch, already exists.[35]

A safety by design approach can play a central role in *preventing* harm from ever taking 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. In other words, 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 to find and create CSAM online and more costly for offenders to do so.

[35] https://safetonet.com/safetowatch/

We must come to a realization: Today's phones and apps are not "**safe by design**" precisely because they are built without any technology intended to prevent child abuse images and videos from being taken, streamed or shared. We should no longer take this reality for granted; we should no longer accept this perverse status quo, that phones, tablets, and computers should be at the full, unmitigated disposal of offenders to create new child abuse images, videos, and livestreams without any friction. Just as we have demanded child and consumer safety in all types of products from cars to car seats, to cribs and playgrounds – to make children safer – Congress and the U.S. public should demand that tech companies build their products and platforms safe by design, anticipating through expert consultation how they can be abused, and building in safety as a priority.

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.**

Imagine cars without seatbelts, airbags, or antilock brakes? Or imagine if we routinely allowed daycare workers, teachers, coaches, and others who work closely with children to do so without undergoing background checks and safeguarding training? Or imagine if we had no government regulations or requirements for infant car seats, playground safety, and the other safety standards governments require in the physical world to keep children safer? Congress and the American public would never stand for it. We consider such safety features as common sense and good practice in the offline world, and the same should apply to digital platforms.

It is critical that individual companies clearly understand and appropriately respond to the scale of harm occurring on or via their platforms, which is why IJM's Center to End Online Sexual Exploitation of Children collaborates with industry on improved detection, disruption and reporting. In November 2022, I spoke passionately at the Singapore FinTech Festival,[36] the largest financial tech gathering in the world. I called on tech and financial sectors to embed child safety into their platforms and products, encouraging them to partner with NGOs working to make communities safer.

But what can companies do when the abuse happens in "real-time" and how can privacy concerns be addressed? Safety technology, such as SafeToWatch[37] and others, promises to technologically prevent and disrupt the production and sharing of new CSAM, even in end-to-end encrypted environments.[38] Such real-time threat detection tools are designed to disrupt

[36] https://www.youtube.com/watch?v=xia8H781yu0

[37] https://safetonet.com/safetowatch/

[38] https://safetonet.com/safetowatch-commentary-wired-magazine/

the display of child sexual abuse happening live on video conferencing platforms. Implemented on devices or in apps, such technology could prevent child sexual abuse material production without unfairly invading someone's privacy. If used for purely preventative or disruption reasons, no reports need be submitted to law enforcement.

Use of this type of technology could help remedy the phenomenon of livestreamed sexual abuse, whether for-profit or in grooming and sextortion contexts. So far, tech companies are doing next to nothing to address livestreamed abuse. For example, in 2022, Australia's eSafety Commissioner issued legal notices to seven tech companies requiring them to report on how they are tackling child sexual exploitation on their platforms. The report revealed "that the providers are neither taking action to detect CSEA in livestreams (insofar as any of these could be regarded as livestreaming services) or taking action to detect CSEA in video calls or conferences."[39] All companies should voluntarily use the best available technology to combat CSAM in images and recorded/live video, and if not, then Congress should require it.

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).[40] Such mitigation measures are critical to stemming the growing tide of child sexual abuse online.

While still reacting to harm by detecting and removing CSAM already online, companies should move increasingly upstream to prevent CSAM production and distribution in the first instance, including testing of emerging, sophisticated on-device ("client-side") technologies. These technologies can be privacy protective. With industry-wide change, offenders can have nowhere to hide and nowhere online to abuse children with impunity.

To stem the growth of these violations of children's rights, it will take a coordinated global effort among legislators, criminal justice systems, tech and financial sectors, civil society and survivor leaders. The challenges are complex, but child protection solutions – in the justice, tech, and financial sectors – already exist. It is time for key stakeholders to prioritize broad deployment of these comprehensive child protection systems.

---

[39] 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.

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

Just as urgent global collaboration and resource investment helped curb the COVID-19 pandemic, a global, urgent multi-sectoral response can so too protect millions of children from offenders eager to harm them online and in person.

In closing, there are just some words that should never go together:

livestreamed child sexual abuse
child sexual exploitation material

The opportunity for Congress is to help make those phrases history. Now.

***