END OSEAC
COALITION TO PROTECT KIDS ONLINE

January 22, 2024

The Honorable Richard Durbin
Chairman
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Lindsey Graham
Ranking Member
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Durbin and Ranking Member Graham,

The End Online Sexual Exploitation and Abuse of Children (OSEAC) Coalition writes to voice our support for the upcoming hearing on online child sexual exploitation scheduled for January 31, 2024, featuring testimony from the CEOs of Meta, X, TikTok, Snap, and Discord. The End OSEAC Coalition is a coalition of over 30 organizations dedicated to advocating for federal policies and programs that address the online child sexual exploitation and abuse crisis. As organizations deeply committed to child protection, we are grateful for your leadership on this important issue.

According to a study conducted in November and December 2021 and published in the Journal of the American Medical Association, one in six people surveyed were victims of online child sexual abuse before the age of 18.[1] As organizations working on the front lines of this issue, we have especially seen an increase of online child sexual exploitation and abuse since the COVID-19 pandemic. In 2019, the National Center for Missing & Exploited Children (NCMEC) received 16.9 million reports of child sexual abuse material (CSAM) to their CyberTipline.[2] In 2022, just three years later, this number nearly doubled to over 32 million reports, marking the highest number of reports ever received in one year.[3] Unfortunately, thousands of child victims seen in these illicit images and videos have yet to be identified.

The U.S. technology sector plays a vital role in the global response to this horrific crime. Unfortunately, as whistleblower Frances Haugen recently described in The Hill[4], the tech sector's public acceptance of online safety legislation in the U.S. is belied by behind-the-scenes attacks on proposals — federal and state — to make the internet safer. Regulation can incentivize technology companies to identify and implement innovative solutions to prevent the growing crisis of child sexual abuse online. And the sector should embrace it because the status quo — individual companies making internal policy decisions or

[1] Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of online sexual offenses against children in the US. JAMA Open network, 5(10), e2234471. doi:10.1001/jamanetworkopen.2022.34471

[2] National Center for Missing and Exploitation Children. 2019 CyberTipline reports by country. (n.d.) https://www.missingkids.org/content/dam/missingkids/pdfs/2019-cybertipline-reports-by-country.pdf.

[3] National Center for Missing and Exploited Children, "EARN IT Act of 2022". January 8, 2022. https://www.missingkids.org/blog/2022/earn-it-act-2022.

[4] The Hill. November 2, 2023. "I blew the whistle on Facebook. Two years later, Big Tech hasn't changed." https://thehill.com/opinion/technology/4287305-i-blew-the-whistle-on-facebook-two-years-later-big-tech-hasnt-changed.

collaborating within the sector to determine if or how they address child sexual abuse on their platforms and apps — is not only ineffective but has also failed to mitigate significant harms faced by children around the world.

As the Committee hears testimony from five witnesses representing companies whose platforms are used by millions of Americans and billions of people around the globe, we hope you will address the following topics with the witnesses:

- Three bipartisan bills reported through the Committee in 2023 – EARN IT Act, the REPORT Act and the STOP CSAM Act – would require that reports of suspected child sexual exploitation submitted by electronic service providers (ESPs) to the CyberTipline should include information that would help law enforcement identify and locate the children exploited in CSAM and the perpetrators distributing this illegal content. Currently, federal law requires online platforms to report CSAM to the CyberTipline when they are made aware of its existence on their platforms. However, there are no requirements for the type of information that must be reported. Many reports submitted by tech companies are not actionable, and law enforcement is unable to properly conduct an investigation. According to the Department of Justice, "There are no industry best practices relating to the consistency, timeliness, or completeness of the information ESPs provide when reporting apparent CSAM to the CyberTipline. ESPs differ as to whether they include IP addresses, information relating to whether reported content has been viewed or categorized by the ESP, and if the CSAM content was distributed beyond the reported user. Sometimes ESPs report an old incident that it only recently detected or provide reports with minimal information that prevent any action by law enforcement. Other times, ESPs no longer have, or in violation of its statutory requirement, never preserved, data relevant to the offense, such as the IP address which is needed to trace the location where the crime is occurring."[5] These updates to the CyberTipline reporting requirements would ensure that law enforcement receives the information necessary to investigate these cases.
    - Questions for all witnesses: Do you support these proposed changes to the CyberTipline reporting requirements to assist with vital law enforcement efforts regarding the identification of children in harm's way and the apprehension of perpetrators committing such abuse? If not, why do you oppose these changes?

- The EARN IT Act and REPORT Act would require reporting companies to preserve the contents of CyberTipline reports for one year, as opposed to the current 90-day requirement, providing law enforcement with desperately needed additional time to pursue these cases.
    - Questions for all witnesses: Do you support this proposed increase in the retention period for contents of CyberTipline reports to assist with vital law enforcement efforts to support the identification of children in harm's way and the apprehension of perpetrators committing

[5] Department of Justice, "Unique Resource and Enforcement Issues". Retrieved January 17, 2024 from https://www.justice.gov/d9/2023-06/unique_resource_and_enforcement_issues_2.pdf.

such abuse? If not, what impact would this proposed change have on your company? What resources would be needed to increase the retention period for these reports so that there is more time to investigate them?

- Sextortion is an emerging form of online child sexual exploitation that occurs on many gaming and social media platforms, in which an individual is threatened with the dissemination of intimate, sexual images or videos to coerce the victim into providing additional intimate, sexual materials or money and/or other forms of payment to the extorter. An analysis by the Canadian Centre for Child Protection revealed that children, especially boys, are increasingly being targeted for sextortion on Instagram and Snapchat.[6] Due to the global connectivity these platforms provide, perpetrators may be located internationally. This means that perpetrators across the globe have access and the ability to victimize children in the U.S. We saw this recently in Michigan when a teenage boy died by suicide after being sextorted via Instagram by perpetrators located in Nigeria. The perpetrators allegedly used Instagram accounts to pose as young women to lure teenage boys and young men.[7]
    - Question for Mr. Zuckerberg and Mr. Spiegel: What measures are you taking to prevent and address sextortion on your companies' platforms?

- According to International Justice Mission's recent study "Scale of Harm," nearly half a million Filipino children were sexually abused to produce new child sexual exploitation material in 2022, especially in live video calls.[8] Many of these abuses occur on online platforms with live video features, including Facebook Messenger. According to the Basic Online Safety Expectations "Summary of industry responses to mandatory transparency notices" published by the government of Australia's eSafety Commissioner in December 2022[9] and October 2023[10], Meta, Skype, Apple, and Discord are not detecting the live transmission of CSAM – the broadcasting of acts of sexual exploitation or abuse of a child in real-time on video calls between people anywhere in the world, sometimes in exchange for payment. Yet, we know that U.K.-based safety tech company, SafeToNet, has developed technology called SafeToWatch that can detect and block child sexual abuse in real-time, in live video, and even on E2EE apps – so this type of abuse is entirely preventable.

[6] Boys aggressively targeted on Instagram and Snapchat, analysis of Cybertip.ca Data shows. protectchildren.ca. August 4, 2022. https://www.protectchildren.ca/en/press-and-media/news-releases/2022/sextortion-data-analysis.

[7] NBC News. Nigeria hands over two suspects in sextortion case linked to suicide of Michigan high school athlete. August 14, 2023. https://www.nbcnews.com/politics/justice-department/us-extradites-nigerians-sextortion-linked-suicide-michigan-teen-rcna99795.

[8] Scale of Harm: Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines. October 2023. https://www.ijm.org/studies/scale-of-harm-estimating-the-prevalence-of-trafficking-to-produce-child-sexual-exploitation-material-in-the-philippines.

[9] 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.

[10] Basic Online Safety Expectations: Summary of industry responses to mandatory transparency notices. October 2023. https://www.esafety.gov.au/sites/default/files/2023-10/Full-transparency-report-October-2023.pdf

- Questions for all witnesses: Is your company using existing safety technology to detect and prevent live video child sexual abuse on your platforms and apps that allow users to stream or share live video? If not, why not? And if you aren't, what are you doing?

- The Luxembourg Guidelines define grooming as "the process of establishing/building a relationship with a child either in person or through the use of the internet or other digital technologies to facilitate either online or offline sexual contact with that person."[11] Perpetrators often use online platforms to target vulnerable children, as noted above, with the intention of later sexually exploiting and/or abusing the child. If CSAM is produced as a result of grooming, perpetrators often use the material as blackmail to prevent the child from reporting the experience and to coerce production of additional materials and further escalate the exploitation and abuse. Grooming detection is an important avenue to preventing OSEAC, but only 37% of technology companies currently employ grooming detection tools.[12] Grooming detection tools are highly effective and accurate[13] and should be utilized alongside CSAM detection tools by all online platforms to ensure they are minimizing risks faced by children on their platforms.
  - Questions for all witnesses: Is your company using language analysis tools to detect grooming activities? If not, why not? What investments will your company make to develop new or improve existing tools?

- In December, members of this coalition joined leading voices and experts from the child advocacy community in calling for Meta to reconsider plans to implement end-to-end encryption (E2EE) on Messenger and Facebook, which will prevent the detection of CSAM on those platforms. In light of this internal policy change, Meta has a responsibility to advance emerging technical solutions such as encryption algorithms that can perform image hashing on encrypted data. Some options include enhancing the detection of high-risk behaviors via artificial intelligence, hash matching, text-based analysis, and making homomorphic encryption viable. Such technologies require more development from global tech leaders, like Meta, to be rolled out at scale.
  - Question for Mr. Zuckerberg: what investments will your company make in technical solutions to detect CSAM in E2EE environments?

- Currently, tech companies' internal processes for assessing and responding to online risks and harms faced by children using their platforms are opaque, making it difficult to know what

[11] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Adopted by the Interagency Working Group in Luxembourg, January 28, 2016. https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf.

[12] Survey of technology companies. (n.d.). WeProtect Global Alliance. Retrieved January 17, 2024 from https://www.weprotect.org/survey-of-tech-companies.

[13] Gunawan, Fergyanto & Ashianti, Livia & Sekishita, Nobumasa. (2018). A Simple Classifier for Detecting Online Child Grooming Conversation. Telkomnika (Telecommunication Computing Electronics and Control). 16. 1239-1248. 10.12928/TELKOMNIKA.v16i3.6745.

efforts, if any, individual companies are taking to keep children safe. Companies that operate a social media platform should develop and share annual reports that outline how they assess risks on their platforms, disclose any risks to children they have identified, and describe mitigation strategies they are or plan to put in place to address these risks. Existing efforts like the Tech Coalition's Voluntary Framework for Industry Transparency are ineffective, as they allow platforms too much leeway in determining how they will implement the framework, leading to inconsistent and ineffectual application of its provisions. The STOP CSAM Act would instead require companies to produce an annual transparency report that meets consistently applied requirements, allowing for appropriate stakeholders to assess individual companies' existing efforts and better hold them accountable.

- Questions for all witnesses: Do you support this proposed requirement to develop annual transparency reports? Do you believe that such reports would help establish best practices in online child safety standards and support adherence across the sector to these standards? If not, why not?

We applaud the Senate Judiciary Committee for holding such a critical hearing and look forward to hearing from Mr. Zuckerberg, Ms. Yaccarino, Mr. Chew, Mr. Spiegel, and Mr. Citron about their respective company's efforts to address the growing scourge of online sexual abuse and exploitation.

Sincerely,
End OSEAC Coalition

End OSEAC Survivors' Council
Anti-Human Trafficking Intelligence Initiative (ATII)
Brave Movement
ChildFund International
Children's Justice Fund
Child Rescue Coalition
Enough is Enough
Global Hope 365
International Justice Mission
National Center on Sexual Exploitation
National Child Protection Task Force
National Criminal Justice Training Center
PACT
Protect Young Eyes
Raven
Rights4Girls
The Carly Ryan Foundation
Thorn
Together for Girls
RAINN