Kids Online Health and Safety Request for Comment

Online sexual exploitation and abuse of children (OSEAC), one of the worst forms of online abuse, is growing exponentially year after year, with no end in sight. The National Center for Missing and Exploited Children (NCMEC) reported that, from 2021-2022, the number of CyberTipline reports of suspected CSAM rose from 29.4 million to over 32 million, continuing the upward trend seen over the last fifteen years.

There is also no clear line between online and offline sexual violence against children. The production of CSAM often involves hands-on abuse by family and trusted adults and some children that are groomed online are coerced into meeting perpetrators in-person, leading to offline offenses. A 2022 survey of dark web users conducted by Finnish nonprofit Suojellaan Lapsia Ry found that 37% of global respondents reported seeking direct contact with a child after viewing CSAM.

Similar to offline sexual violence, gender plays a large role in children's risk of experiencing OSEAC, as well as how that violence manifests. UNICEF's 2020 evidence review, *Action to End Child Sexual Abuse and Exploitation: A Review of the Evidence*, found that "support [for] male power towards women" was "the strongest predictor of accepting attitudes [towards child sexual abuse]." In INTERPOL's and ECPAT International's 2018 report, *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material*, an analysis of CSAM cases with unidentified victims recorded in the International Child Sexual Exploitation database found that 64.8% depicted girls, 31.1% depicted boys and 4.1% depicted both girls and boys. CSAM depicting boys was much more likely to feature the most severe forms of sexual abuse. According to NCMEC, between 2019 and 2021, reports of sextortion more than doubled, and HSI has reported that boys tend to be most affected by financial sextortion. Plan International's recent *Free to Be Online?* report also found that 58% of the 14,000 girls they surveyed experienced some form of online harassment. Early evidence shows that children that identify as LGBTQI+, belong to racial and ethnic minorities and/or have disabilities are especially vulnerable.

Even though there are strong efforts by the administration, law enforcement and civil society, current resources are not enough to keep up with OSEAC's rapid rise let alone prevent its further growth. For example, despite an increase in the number of leads, the number of federal prosecutions has seen a steady decline since 2016.

Investments in improving OSEAC prevention efforts, victim and survivor support, increasing and improving research and data and working closely with and holding the technology industry accountable for children's online safety are needed to effectively address online violence against children. Similarly, the adoption of a life-course approach that employs an intersectoral, intersectional lens for all prevention, healing, and justice interventions is critical, as children that experience violence, whether facilitated online or offline, in childhood are more susceptible to experiencing further violence in adulthood.

The administration's active engagement with the tech sector on this issue is of vital importance, and we have been encouraged by efforts over the last year to examine and prioritize children's safety online, including the inclusion of privacy and online protections for children and safety-by-design standards, in the "Principles for Enhancing Competition and Tech Platform Accountability, the establishment of the White House Task Force to Address Online Harassment and Abuse , the creation of the new interagency Kids Online Health and Safety Task Force and

most recently the inclusion of the need for efforts to prevent the creation of AI-generated CSAM in the President's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

We appreciate these efforts and are incredibly grateful for the opportunity to show support and offer suggestions for the National Telecommunications and Information Administration and the Task Force. The undersigned organizations respectfully submit the below comments and recommendations for your consideration.

Current and Emerging Risks to Children's Health, Safety and Privacy

While children's growing access to and use of the internet and online spaces can have important benefits including connecting them to educational opportunities, mechanisms to connect with their peers, platforms to share their ideas and new avenues for recreation, it is not without its risks. As the internet developed over the last couple of decades, children's best interests were rarely a factor in how new platforms were designed or operated, with some proving to be outright harmful and vulnerable to misuse by bad actors. Without proper safeguards and education, children may be exposed to disinformation, harmful content, threats to their privacy, negative impacts on their mental health and a number of other online harms, like cyberbullying, harassment and online sexual exploitation and abuse.

A number of U.S. government agencies are leading essential and valuable efforts to address OSEAC. While we are encouraged by efforts to increase interagency coordination and collaboration, including through the Kids Online Health and Safety Task Force, the lack of a single agency within the government tasked with leading efforts on children's online safety makes it nearly impossible to avoid duplication of efforts, overcome communication inefficiencies and inconsistencies and identify all opportunities for cross-governmental collaboration. An established office with the mandate to address and uphold all aspects of children's online safety, with adequate funding and an appointed, high-level staff position, would be able to play an interagency convening role and ensure a cohesive, efficient government response to this growing, complicated issue. The proposed office should hold regulatory power to support those efforts, including the ability to enforce takedown notices, and work directly with the tech industry to improve online safety efforts. It should also promote children's online safety by hosting resources, easy-to-use reporting mechanisms and links to counseling and support services on a centralized, accessible website; leading awareness campaigns aimed at the general public and children; and supporting ongoing online safety research.

Example of an effective, centralized government agency focused on children's online safety:

- Australia's eSafety Commissioner - The Australian government established the Children's eSafety Commissioner in 2015, and it serves as an independent regulator for online safety within the country. The eSafety Commissioner supports research and education programs focused on online safety, leads regulatory schemes and investigations, and works with the technology industry to support the development and implementation of user safety standards. The Commissioner also handles reports of image-based abuse, illegal online content, cyberbullying and adult cyber abuse. It's website also serves as a one-stop shop to find online safety resources, education and training materials; report online safety concerns; and access support services and counseling.

Threats to mental health

Approximately 95% of children aged 13-17 in the U.S. report using social media. However, a growing body of evidence, including information gained from recent social media platform whistleblowers such as Frances Haugen, shows that social media use by children has been linked to higher rates of anxiety and depression. There are also early findings that show social media use may lead to children and youth having lower self-esteem, a higher risk of disordered eating, and poorer sleep quality and duration. Many adolescents are also at risk of experiencing problematic interactive media use, which can have impacts on their mental health, education and relationships. This has resulted in the U.S. Surgeon General releasing an *Advisory on Social Media and Youth Mental Health* that urges key stakeholders, including policymakers, tech companies and families, to work together to improve the safety of social media platforms to ensure risk are mitigated and children and youth's mental health is protected. Attorney Generals from forty-two states also recently issued a lawsuit against Meta that alleges that its Facebook and Instagram platforms are knowingly designed to be addictive and ultimately harmful for children and teens.

Online harms can also have a severe and sometimes lifelong impact on children and youth's mental health and overall wellbeing. Survivors of online sexual exploitation and abuse of children are often exposed to ongoing harm and potential retraumatization due to the continued proliferation of child sexual abuse materials and the lack of effective avenues for them to seek recourse and removal of these materials. This may result in survivors experiencing social isolation, poor mental health, substance abuse, self-harm, suicide and other negative impacts.

Recommended responses

1. Continue research looking into the impact of children's use of social media and other online platforms on their mental health. - More research should be conducted that examines specifically how social media's recommendation algorithms and other internal functions negatively impact child users' mental health and wellbeing. Findings should then be used to inform online platforms' child safety features and requirements, as part of a safety-by-design approach, to ensure the risks to child users are minimized.

Example of research report focused on how social media's algorithms negatively impact children's mental health:

- Designing for Disorder: Instagram's Pro-eating Disorder Bubble – Fairplay released a report in 2022 that examined Instagram accounts that were part of a "pro-eating disorder 'bubble'", which including 90,000 accounts that promote pro-eating disorder messages and imagery to their followers. The report found that nearly a third of these accounts belong to children, with many claiming to be younger than 13, Instagram's minimum age for users.

2. Improve children's access to free, readily available, high quality mental health and counseling services. - The COVID-19 pandemic has had a devastating impact on children's mental health, increasing feelings of loneliness, depression and anxiety. An international survey conducted by UNICEF in 21 countries, including the United States, found that 1 in 5 participants, aged 15-24 reported feeling depressed or expressed a lack of interest in engaging in activities. Untreated or unresolved mental health issues in childhood can result in enduring

consequences and create vulnerabilities that place a child at serious risk both offline and online. Research conducted by the UK's National Society for the Prevention of Cruelty to Children found that children that have shared feelings of vulnerability online are at higher risk of being targeted and groomed by offenders online. Protecting adolescents from adversity, promoting socio-emotional learning and psychological well-being, and ensuring access to mental health care are critical for their health and well-being, and one of the best prevention tools we can provide to help reduce the risk of children becoming victims of OSEAC. Current barriers to children's access to mental healthcare include: intersectoral economic, racial, ethnic minority and disability-related barriers and discrimination within the healthcare system; lack of mental health professionals; low levels of mental health education and awareness; and social stigma related to mental health conditions. Potential avenues to increase children's access to mental health services could include providing additional funding for schools to hire counselors with specialized training, investment in helplines and online mental health services and grant programs to support the development of community-based mental health services.

Online sexual exploitation and abuse of children

a. Lack of understanding of the extent of OSEAC and its ever-changing nature

Overall prevalence rates of OSEAC and current research that examines the unique risk factors and online harm experiences of children from ethnic and racial minorities, children with disabilities, children who identify as LGBTQI+, victims of child trafficking and child runaways, is severely lacking. LGBTQI+ youth, for example, are 7.4 times more likely to experience acts of sexual violence than their heterosexual peers and are 3 to 7 times more likely to engage in survival sex. Up to 40% of homeless youth identify as LGBTQI+. According to a recent WeProtect intelligence briefing, "data detailing the incidence and scale of the online facilitated sexual abuse of children with disabilities is glaringly absent" despite children with disabilities being 3 to 4 times more likely to experience sexual and physical violence than their peers. For marginalized girls including Black, Native American and Latina girls, being a victim of sexual abuse and exploitation increases their risk of involvement with the justice system and child welfare. "Girls of color account for approximately 24% of the youth population but comprise approximately 62% of girls who are in residential placement."[1] Early evidence also suggests that these vulnerable groups are less likely to seek help and report online harms. This underreporting severely impacts our understanding of the prevalence of OSEAC and the populations most at risk.

Recommended responses

1. Conduct robust research that examines OSEAC risk and protective factors for all children, the effectiveness of existing prevention and response programming and new emerging trends in how OSEAC is manifesting. Research should include:

- **Level of risk faced by all children, including those with increased vulnerabilities, of experiencing OSEAC and the long-term impact of existing OSEAC-related interventions on reducing these risks –** Additionally, intersectional research should be conducted that examines how these vulnerabilities manifest in increased risks and experiences of online harms, as well as contributing factors behind lower rates of reporting of harms.

[1] Charles Puzzanchera, Anthony Sladky & Wei Kang, Easy Access to Juvenile Populations: 1990-2019 (2019); Melissa Sickmund, Anthony Sladky, Wei Kang & Charles Puzzanchera, "Easy Access to the Census of Juveniles in Residential Placement." (2019)

- **Long-term effectiveness of child and caregiver online safety education programs at reducing children's risk of experiencing OSEAC** - Research examining and comparing the effectiveness of online safety education programs at lowering children's rates of experiencing OSEAC would be hugely beneficial in determining which approaches work best and how education programs should improve and evolve over time. Assessments should also specifically examine how effectively these education programs reach and support children with increased vulnerabilities, including children from ethnic and racial minorities, children with disabilities, children who identify as LGBTQI+, etc.

b. Lack of awareness of online harms and risks.

Educating children and trusted adults in their lives on online safety is an important way to mitigate children's risk of experiencing online harms, including OSEAC. However, there are currently no national standards for online safety-focused curricula, which leads to inconsistent access for children and teachers to quality, evidence-based online safety education and training. This leads to many children, youth, caregivers and other trusted adults not fully understanding potential harms and being unaware of effective strategies and available safeguarding tools, which can increase children and youth's vulnerability.

Recommended responses

1. Develop national standards for online safety curricula for use in schools and training for school personnel and support awareness-raising campaigns, including PSAs, targeting children, youth and caregivers. - National standards should require curricula to employ an age-appropriate and multi-tiered approach that integrates social, emotional learning, resiliency development, digital literacy, healthy relationship development and empathy-based programs alongside modules focused on building awareness of online and offline risks. Online safety and anti-sex trafficking education curriculum requirements must also be sensitive to underserved and high-risk populations, including children with disabilities, children who identify as LGBTQI+ and children from racial and ethnic minorities. Research has also shown that, whenever possible, online safety education should be integrated "into already well-established and evidence-based programs currently addressing related offline harms" due to the considerable overlap between online harms and similar offline harms, including risk factors, and the more robust evidence base for long-standing programs originally targeting offline harms.[2] Additionally, there should be complementary standards for training programs for teachers that builds their understanding of online safety and provide techniques on how to identify potentially vulnerable students and how to report suspected cases of online or offline childhood sexual violence. Accompanying awareness campaigns should also be launched that highlight risks, promote children's autonomy and positive self-image and direct children, youth and caregivers to easily accessible, quality online resources and training.
Examples of promising online safety educational materials:

- Human Trafficking Youth Prevention Education (HTYPE) Demonstration Program: U.S. Department of Health and Human Services' Human Trafficking Youth Prevention Education (HTYPE) Demonstration Program provides funding to local educational agencies to develop skills training and education programs for students and school staff

[2] Finkelhor D, Walsh K, Jones L, Mitchell K, Collier A. Youth Internet Safety Education: Aligning Programs With the Evidence Base. Trauma Violence Abuse. 2021 Dec;22(5):1233-1247. doi: 10.1177/1524838020916257. Epub 2020 Apr 3. PMID: 32242503.

to support the prevention of human trafficking and create a trauma-informed, person-centered Human Trafficking School Safety Protocol to support school staff in understanding how to best respond to suspected cases of human trafficking. Through these programs, school staff learn how to identify students who may be experiencing human trafficking and the steps on how to report cases. Education programs for students aim to address risk factors and build students' resilience through increasing their understanding of human trafficking and supporting the development of healthy behaviors.

- Project Connect - Project Connect was developed by the Carly Ryan Foundation, with support from the Australia Department of Social Services and the Government of South Australia and is an online safety education program that includes seminars for students in grades 5-12, their parents and their larger communities. The program is certified by the Australian government's office of the eSafety Commissioner and is being implemented nationally. The seminars take a holistic approach and cover topics including online safety, emotional intelligence, critical thinking, respectful relationships, resilience, and understanding the legal framework, among a wide range of other issues.
- NetSmartz - NetSmartz is an online safety education program created by NCMEC that features age-appropriate videos, interactive activities and other resources that aim to help children understand online risks and learn how to make safer choices to prevent potential victimization. Beyond the videos and online activities, NCMEC also developed a peer education mentoring kit, a sexting discussion guide, tip sheets and lesson plans to further support children's online safety education.
- iEmpathize Empower Youth Program - iEmpathize developed the Empower Youth Program, an exploitation prevention curriculum targeting youth, to provide students with the skills to recognize potentially exploitative and harmful situations, including those occurring online, and know how to protect themselves. The program combines exploitation awareness with training for students to support their development of empathy, which the organization believes will empower students to not only avoid being exploited themselves but to also help others avoid exploitation, too.
- CTIP Student Guide to Preventing Human Trafficking and accompanying Parent Resource Guide: The U.S. Department of Defense Combating Trafficking in Persons (CTIP) Program Management Office (PMO) and Joint Knowledge Online (JKO) recently developed the CTIP Student Guide to Preventing Human Trafficking and the accompanying Parent Resource Guide. The student guide targets teens in 10th-12th grade with a connection to the military to help them understand human trafficking and how it is occurring in schools and online spaces. Topics include an explanation of what human trafficking is, the potential warning signs of trafficking, how to recognize potential trafficking situations and how to seek help and report a potentially bad situation. The Parent Resource Guide was developed for military-connected parents and explains the student course and provides guidance for how parents can support students' understanding of human trafficking.
- Department of Homeland Security's Homeland Security Investigations' Project iGuardian training: Project iGuardian is an educational program led by Homeland Security Investigations that aims to inform the public about children's online safety. The presentations are led by HSI subject matter experts and are aimed at children, teens, parents and trusted adults. The presentations include strategies on how to mitigate online risks and how to report suspected abuse.
- ICAC prevention and education for parents and youth - Educating the public through the development and delivery of public awareness and prevention programs is one of the many important initiatives of the Internet Crimes Against Children (ICAC) Task Force Program. Since 1998, members of the ICAC Task Force program have delivered more

than 194,000 community outreach presentations to local communities across the nation. The ICAC Public Awareness Working Group develops resources for use by all ICACs and their affiliate law enforcement agencies. These resources are available for free for use by anyone accessing the ICAC Task Force website and can be found through the "Resources" and "Internet Safety" tabs. These resources are developed each year for Safer Internet Day in February and Internet Safety Month in June. In 2023, the program developed a Cyberbullying prevention video for Cyberbullying Awareness Month in October. The ICAC Task Force Public Awareness Working Group has developed a Prevention and Communication Plan that identified the need to create a collaborative approach with technology safety subject matter experts to develop additional safety prevention resources addressing some of the most pressing child exploitation issues, including self-produced sexually explicit material.

- Enough is Enough's Internet Safety 101® - Internet Safety 101® is a digitally-based internet safety resource designed to educate, equip and empower parents, educators and other adults with the knowledge and resources needed to protect children from Internet dangers including pornography, predators, cyberbullies and threats related to online gaming, social networking and mobile devices. Enough Is Enough is in the process of releasing its state-of-the-art digital curriculum "Internet Safety 101 Academy" based off the Emmy Award winning Internet Safety 101 program to include video-based content, resources, and train the trainer modules for law enforcement and the public.

c. Grooming

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." 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 produced material to blackmail the child to not report the experience and to produce additional materials and further escalate the exploitation and abuse.

Recommended responses

1. Improve efforts to respond to grooming behavior on online platforms. - Grooming detection is an important avenue to preventing OSEAC, but only 37% of technology companies currently employ grooming detection tools. Grooming detection tools should be utilized alongside CSAM detection tools by all online platforms to ensure they are minimizing risks faced by children on their platforms. Additionally, existing legal frameworks should be updated to ensure they prohibit online forms of grooming for the purposes of online sexual contact and enable law enforcement to act to intercept perpetrators before they are able to sexually exploit and abuse children.

Example of effective anti-grooming legislation:

- Australia Criminal Code Amendment (Protecting Minors Online) (Carly's Law) - Passed by Australia's parliament in 2017, Carly's Law targets online grooming by prohibiting adults from using online services with the intention of engaging in sexual activity with a child under 16. The law specifically cites adults misrepresenting their age, often a key strategy of groomers, as an example of a tactic used to target children.

d. Rise in self-generated child sexual abuse material (SG-CSAM)

Self-generated child sexual abuse material (SG-CSAM) is CSAM that at least has the appearance of being produced by the child depicted. The rate of SG-CSAM creation is rising exponentially every year. In its 2021 annual report, the Internet Watch Foundation noted a 168% increase in the number of actioned websites that contained SG-CSAM and that 59% of all its actioned reports were SG-CSAM that depicted 11-13-year-old girls. As Thorn found in its 2020 research report, *Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2020*, early evidence shows that the creation of SG-CSAM is often complex and may be the result of both "consensual or coercive experiences", including sexual exploration, grooming and coercion.

Recommended responses:

1. Conduct research that examines the driving factors behind the rise of self-generated CSAM (SG-CSAM) and children's increased vulnerability to OSEAC following the creation of SG-CSAM – Additional research is necessary to further understand the driving factors behind this rapid rise in SG-CSAM, as well as children's potentially increased vulnerability to OSEAC following the initial creation of SG-CSAM, including sextortion. Additionally, research that explores the experiences of young people that have created SG-CSAM with the criminal legal system would be beneficial to building understanding of the potentially harmful, unintended consequences current processes have on children and youth. Any data gathered through research on SG-CSAM should be disaggregated, at minimum, by children's age, gender, racial and ethnic background, as well as whether the child identifies as LGBTQI+ and whether the child has a disability.

e. AI-generated (AIG) CSAM

Artificial Intelligence-generated Child Sexual Abuse Material (AIG CSAM) is a growing area of concern. The Biden administration's recently released executive order on AI recognized the need for urgent action and creation of new safety and security standards, including those that would prevent the creation of AIG CSAM. Additionally, attorneys general from across the US in all 50 states are urging lawmakers to create a commission dedicated to studying the impacts of AI on child exploitation. Among the dangers lawmakers have highlighted include the creation of "deepfake" scenarios — videos and images that have been digitally created or altered with artificial intelligence or machine learning — of a child that has already been abused, or the alteration of the likeness of a real child from something like a photograph taken from social media, so that it depicts abuse.

The Internet Watch Foundation (IWF), the UK organization responsible for detecting and removing child sexual abuse imagery from the internet, reported it had found nearly 3,000 AI-made abuse images that broke UK law. The IWF's latest report , *How AI is being abused to create child sexual abuse imagery*, shows an acceleration in use of the technology with its chief executive stating they are "seeing criminals deliberately training their AI on real victims' images who have already suffered abuse. Perpetrators can legally download everything they need to generate these images, then can produce as many images as they want offline, with no opportunity for detection. Various tools exist for improving and editing generated images until they look exactly like the perpetrator wants. Most AIG CSAM found is now realistic enough to be treated as 'real' CSAM. The most convincing AIG CSAM is visually indistinguishable from real CSAM, even for trained IWF analysts. Text-to-image technology will only get better and pose

more challenges for the IWF and law enforcement agencies. There is now reasonable evidence that AIG CSAM has increased the potential for the re-victimization of known child sexual abuse victims, as well as for the victimization of famous children and children known to perpetrators. The IWF has found many examples of AIG images featuring known victims and famous children. The IWF also has seen evidence of AIG images being sold online.

Recommend responses

1. Work with international partners to evaluate the risks posed by AIG CSAM and explore opportunities to align how this content will be addressed in varying jurisdictions and secure commitment to develop global collaboration.

2. Develop legislation and regulations that adequately respond to AIG CSAM, including outlawing the production and sharing of resources that outline how to produce AIG CSAM, and ensure producers of generative AI technologies conduct appropriate risk assessments and develop risk mitigation strategies to ensure their products cannot be used to create AIG CSAM, including outlining that the creation of AIG CSAM is prohibited under their terms of service.

3. Work with platforms that provide search services to ensure they are not promoting or linking to generative AI technologies that are known to have a connection to the production of AIG CSAM.

4. Conduct research to ensure the datasets feeding into generative AI technologies do not include CSAM.

5. Ensure law enforcement and the social service workforce receive appropriate training on AIG CSAM, including what it is and how to appropriately respond to it.

f. Sextortion

NCMEC defines sextortion as, "... a form of child sexual exploitation where children are threatened or blackmailed, most often with the possibility of sharing with the public a nude or sexual images of them, by a person who demands additional sexual content, sexual activity or money from the child." This form of exploitation occurs in online spaces, where children who have grown up around social media and video games, feel the most comfortable. What makes sextortion particularly dangerous is the emotional and psychological trauma it inflicts on victims. Perpetrators' threat of exposure and humiliation is often leveraged to keep victims in a state of fear, shame, and anxiety, making it a deeply distressing and harmful experience that can have long-lasting emotional, social, and mental health consequences for those targeted. As a result of the toll sextortion takes on victims, many children and minors have lost their lives to suicide. In a joint warning of sextortion schemes, the FBI, Homeland Security, and NCMEC report that more than 7,000 reports concerning the online sextortion of minors have been submitted to law enforcement agencies, leading to a minimum of 3,000 victims, with a predominant number being boys.

Recommended responses

1. Conduct research that examines the driving factors behind the rise of sextortion and children's vulnerability – Additional research is necessary to further understand the driving factors behind the rapid rise of sextortion, as well as the factors that increase children's

vulnerability to being targeted and victimized. Research should explore different types of sextortion, including sextortion that is motivated by a demand for additional CSAM and financially-motivated sextortion.

2. **Online safety education materials, including public awareness campaigns, should be updated to include sextortion** – These materials should be trauma-informed and should include common tactics used by perpetrators to target, groom and elicit CSAM, as well as available mechanisms to report suspected sextortion.
3. **Training materials for law enforcement and the social service workforce should be updated to include information on how to support victims of sextortion** – These materials should be victim-centered and trauma-informed to ensure law enforcement and social service professionals understand the dynamics involved with sextortion and are able to support victims and survivors appropriately.

g. Perpetration by children and youth (problematic sexual behaviors)

Exposure to sexual content, including online sexual content, has been included in research as a potential risk factor for problematic sexual behaviors (PSBs) in children and adolescents, and has been identified as an important avenue for research and intervention, particularly given the ubiquitous access to technology among children.

A new study utilizing the *Children and Adolescents With Problematic Sexual Behavior* survey notes that problematic sexual behavior (PSB) of youth constitutes "developmentally inappropriate, intrusive, and/or clinically concerning sexual behavior involving oneself or others." PSB has been classified as a type of interpersonal child sexual abuse (CSA) often involving siblings, cousins, other family members, or other known children. In the United States and UK, PSB accounts for more than one-third of child sexual abuse cases that reach the hands of law enforcement. Further, according to the National Children's Alliance, 20-25% of cases handled by Children's Advocacy Centers (CACs) in the US involve youth-initiated sexual behaviors.

This research focused on CACs because they utilize multidisciplinary teams (MDT) of law enforcement, prosecutors and legal professionals, forensic interviewers, social and child welfare services, medical and mental health professionals, family advocates, and educators to collaborate and coordinate responses for investigation, treatment, and prosecution of child abuse cases. The research indicated that CACs are optimal for addressing needs related to PSB due to their multidisciplinary team approach and reliance on evidence-based treatments. The National Children's Alliance provides extensive resources addressing youth and children aimed at CACs, partners, and caregivers.

Recommended responses

1. **Invest in evidence-based deterrence programs.** - An often-deprioritized aspect of prevention is deterrence programs focused on preventing CSAM from being viewed, produced or distributed. Current deterrence programs provide strategies, practical tools and support systems aimed at building resilience, impulse control and a sense of accountability to lower the risk of CSAM.

Example:

- Child Advocacy Centers (CACs) interventions with children and youth with problematic sexual behaviors - Between 20-25% of cases that CACs handle include a child or youth that has harmed another child. Some CACs, as part of their support services, implement interventions to manage, supervise and treat children and youth that have been identified as having problematic sexual behaviors (PSBs) to support their rehabilitation and lessen their risk to themselves and other children. Research has shown that the sexual recidivism rate for children and youth with PSBs that receive treatment is extremely low: "children ages 7-12 year have a 98% long-term success rate and youth ages 13-18 years have a 97% long-term success rate." However, there are currently inconsistencies across communities in responses to children and youth with PSBs and additional training and support is needed in order for all CACs to be able to provide effective interventions.

h. Lack of awareness of reporting mechanisms and access to justice and appropriate services

Every child victim of OSEAC and other forms of sexual violence deserves to be able to immediately feel comfortable reporting their experience to trusted authorities and receive free, easily accessible, holistic services to help them throughout their healing process. However, these crimes continue to be underreported, in part due to a lack of awareness of how to report online violence and fears on behalf of victims and survivors that they will be blamed or shamed for the harm they have experienced. The professionals that support victims and survivors along this journey and aid them in seeking justice, including social service providers, law enforcement and prosecutors, must also have access to the training, support and resources required to ensure they are able to provide high-quality, trauma-informed support throughout the process. The following recommendations will improve current efforts and ensure every child victim and survivor receives consistent care based on best practices.

Recommended responses

1. Increase funding for Child Advocacy Centers (CACs) - Child Advocacy Centers (CACs) provide support services to nearly 400,000 child survivors of abuse, including OSEAC, each year. CACs provide critical, evidence-based, trauma-informed programs that support child survivors' mental health and aid their recovery, including as they and their families navigate the justice system. Childhood trauma resulting from abuse and other types of violence has been shown to raise children's risk of experiencing lifelong negative effects on their physical and mental health and wellbeing, including depression, substance abuse, heart disease, cancer and stroke. However, these risks can be mitigated when child survivors are provided with comprehensive response services, like those provided by CACs. While CACs are partly funded by the Crime Victims Fund, ever-changing obligation caps placed on the fund make it difficult for CACs to provide consistent programming and services. Additional funding will further shore up CACs' budgets and allow them to expand their services to reach more child survivors.

2. Identify and establish more sustainable sources of funding for the Crime Victims Fund and improve ease-of-access for victims to utilize the fund. - The Office for Victims of Crime in the Department of Justice oversees and disburses funding from the Crime Victims Fund to states and NGOs to support survivors of crime, including child survivors of sexual abuse and exploitation, through assistance and compensation programs like Child Advocacy Centers. Despite the growing need and demand for these support programs, Congress has continued to lower the obligation cap for the Crime Victims Fund each fiscal year. While the passage of the VOCA Fix to Sustain the Crime Victims Fund Act of 2021 last year opened new revenue

streams to support the fund, it is vitally important that the administration continue to push for an increase to the annual obligation cap and to continue to explore new sources of funding to ensure the fund remains solvent. It is also vitally important that child survivors and their families, including foreign survivors of OSEAC who were exploited at the hands of U.S. perpetrators, are not only aware of how to seek restitution and services supported by the fund but also that the process involved is as unburdensome and expeditious as possible.

3. Provide holistic support to victims and survivors and improve access to civil remedies - In addition to mental health and counseling services, victims and survivors should have easily attainable access to comprehensive services that include legal, medical and housing services, programs that support life skills development and development of practical strategies to help them navigate their healing process, as well as advocacy services, including training to support self-advocacy. Additionally, victims and survivors should have additional avenues to seek civil remedies to support their recovery.
Example legislation that would increase survivors' access to civil remedies:

- The Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act (H.R.2732; S.1207) - Creates targeted exceptions to Section 230 of the Communications Decency Act of 1996 to remove blanket immunity from civil and criminal liability under child sexual abuse material laws.
- Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Maltreatment (STOP CSAM) Act (S.1199) - Expands protections for child victims and witnesses in federal court. Facilitates restitution for victims of child exploitation, human trafficking, sexual assault, and crimes of violence. Expands the federal civil cause of action for child victims to also permit victims of online child sexual exploitation to bring a civil cause of action against tech platforms and app stores that promoted or facilitated the exploitation, or that host or store CSAM or make it available.

4. Ensure policies and programs effectively respond to survivors' needs and experiences, through the establishment of a Survivor Advisory Council. - The administration should conduct regular consultations with survivors of OSEAC to discuss their experiences, ideas and solutions and provide the opportunity for them to feed into the development and evaluation of strategies, policies, and programming. Best practice for effective, meaningful consultations should include the establishment of a Survivor Advisory Council, made up of survivors of diverse backgrounds, including those of varying ages, ethnic and racial backgrounds, socioeconomic statuses, as well as survivors with disabilities and survivors that identify as LGBTQI+. Advisory board participants should serve specified terms and be provided with compensation and access to trauma-informed support and clear, age-appropriate safeguarding at all times. Participants should also be provided with technical assistance and training on the existing U.S. federal legal framework and systems, as well as the basics of policymaking and program development within the U.S. government and Congress.

Examples of successful survivors' councils and advocacy groups include:

- The Phoenix 11 - The Phoenix 11 was formed in 2018 and consists of a group of young women survivors of child sexual abuse that was recorded and, in most instances, shared online. Phoenix 11 members, who maintain their anonymity, advocate stakeholders to prioritize ending and addressing the production and distribution of CSAM online. The group is supported by the Canadian Centre for Child Protection and NCMEC.
- ECPAT-USA Survivors' Council - ECPAT-USA's Survivors' Council consists of women and men survivors of sexual exploitation and human trafficking from across the U.S. Survivors serve as subject matter experts that share their expertise with ECPAT-USA to

help guide the organization's efforts. Survivors are treated as valued consultants and receive compensation for their participation.

- The Brave Movement's Survivor Advocates Globally Empowered (SAGE) - SAGE consists of fifteen survivors of childhood sexual violence who are public advocates calling for catalytic solutions to prevent other children from experiencing similar violence. SAGE members lead and guide the Brave Movement's strategy and are the public-facing representatives of Brave's mission.
- The Keep Kids Safe Movement - The Keep Kids Safe Movement (KKS) is a U.S.-based survivor-led movement of nonprofit organizations dedicated to addressing child sexual abuse online and offline through prevention, healing, and justice. KKS' policy advocacy agenda and call-to-action, the U.S. National Blueprint to End Sexual Violence Against Children and Adolescents, was developed in close collaboration with adult survivors of childhood sexual violence, who informed and guided the drafting of its contents.
- Global Survivor Network (GSN) - Global Survivor Network is an international group of survivor leaders who desire and pursue safe communities through justice systems that protect vulnerable people. Members are survivors of violence, including online sexual exploitation, slavery, violence against women and children and police abuse of power. Local GSN chapters, such as the Philippine Survivor Network, facilitate opportunities for leadership development and advocacy involvement in the community and nationally, and a network that allows for shared learning, programming and curriculum globally.
- The Army of Survivors (TAOS) - The Army of Survivors is the only national organization advocating for child athlete survivors of sexual violence. Founded and led by athlete survivors, TAOS' mission is to bring awareness, accountability, and transparency to sexual violence against athletes at all levels. This mission is supported by three advocacy pillars: advocacy, education, and resource creation.
- The END OSEAC Coalition Survivors' Council - Members of the END OSEAC Coalition Survivors' Council are survivors of OSEAC or live experience experts who serve as an advisory body to inform and guide the END OSEAC Coalition's advocacy and broader efforts. This includes reviewing legislation and contributing to external messaging and the coalition's strategic direction.

5. Advocate for the replacement of the term "child pornography" with "child sexual abuse materials" in all legal statutes and non-legal contexts. - Use of the term "child pornography" is generally recognized by experts as outdated, inaccurate and even harmful to victims and survivors, as it can not only be stigmatizing but also mask and undermine the abusive and exploitative nature of the crime itself and child victims' lack of consent. The preferred term is "child sexual abuse materials" or CSAM, as it more accurately describes the nature of harm conducted against the child or children depicted in these materials. To limit victims' and survivors' retraumatization, Congress should pass legislation that will replace the term "child pornography" with "child sexual abuse materials" in all federal legal statutes and "child sexual abuse materials" should be used in any relevant U.S. government-produced materials.

6. Regularly update training requirements for social services, law enforcement, prosecutors and other professionals that support child victims and survivors to ensure implementation of victim-centered and trauma-informed services. – Professionals at all levels of the child protection and justice system, including the social service workforce, law enforcement, prosecutors, CACs' staff and other relevant professionals, should participate in training and capacity-building sessions on a consistent basis to ensure they remain up-to-date on the latest best practices and developments in the field in order to provide the best support to child victims and their families and minimize their risk of further traumatization.

Examples of latest standards of practice:

- Child Advocacy Center National Standards of Accreditation - Every five years, the National Children's Alliance (NCA) reviews its national standards of accreditation for Child Advocacy Centers (CAC) operating across the U.S. These standards are updated to reflect the latest research and best practices to ensure children and families receiving support from CACs receive consistent, quality care no matter where they are located. There are currently ten accreditation standards, which include: a multidisciplinary team standard; a diversity, equity and access of services standard; a forensic interview standard; a victim support and advocacy standard; a medical evaluation standard; a mental health standard; a case review and coordination standard; a case tracking standard; an organizational capacity standard; and a child safety and protection standard.

Example legislation that would improve coordination between law enforcement and federal prosecutors:

- Project Safe Childhood (PSC) Act (H.R.2661; S.1170) - Modernizes the investigation and prosecution of online child exploitation crimes. Makes improvements to how federal prosecutors and law enforcement work together and use new technology to go after predators. Requires federal prosecutors to coordinate with law enforcement and experts to develop training materials and strategies to remove child victims from harm while quickly arresting offenders

7. **Increase funding for staffing and training of law enforcement investigating cases of online sexual exploitation and abuse.** - Current allocations for investigations are inadequate to respond to OSEAC's exponential growth. Despite the number of NCMEC CyberTipline reports increasing year upon year, the number of federal OSEAC-related prosecutions for OSEAC declined between 2016 and 2020. The sheer volume of reports and limited staffing in combination with the high level of specialized expertise, cyber skills, and continual training on technological advances necessary to thoroughly investigate these crimes severely constrains current efforts. Additional funding specifically to increase the number of child exploitation investigators and support the Internet Crimes Against Children (ICAC) Task Force Program would increase capacity to interdict child sexual abuse image offenders, identify children seen in these images who remain unidentified and remove these children from harm.

8. **Improve access to mental health and counseling services for professionals that work directly with victims and survivors.** - Social service providers, law enforcement and other professionals that support victims and survivors of OSEAC are especially vulnerable to vicarious trauma and burnout due to the severe nature of victims' abuse and exploitation. It is vitally important that everyone - from investigators who review CSAM as required by their investigations to social service providers who provide mental health and counseling support to incredibly traumatized and vulnerable children – have easy, free access to mental health services as needed; regular, required psychological wellness checks; and training to develop strategies to mitigate the impacts of their work and support their resilience. Not only is this important for these professionals' personal wellbeing, but it also lowers the risk of high turnover rates of highly trained and specialized staff.

9. Increase funding to support ongoing adoption of existing and development of new technologies that support the identification and investigation of CSAM. - Digital evidence plays a critical role in the identification of child victims and offenders, as well as supports criminal prosecutions. With digital technologies and encryption becoming more and more sophisticated and the number of CyberTips of suspected OSEAC continuing to grow exponentially, it is critical to invest in the development of new tools and techniques to gather

critical digital evidence that helps investigators build cases against the manufacturers, possessors and traders of CSAM. In order to keep pace with technological innovation and effectively combat child exploitation at scale, investigators require access to state-of-the-art equipment. Cutting-edge technology devices and software, including high-quality equipment for storing and processing data, enable investigators to operate the equipment that many criminals use in perpetrating child abuse and exploitation crimes. Continuous training on new tools and emerging technologies is also imperative.

10. Increase and improve coordination and collaboration between U.S. law enforcement and international law enforcement, including appropriate information-sharing, training and joint investigations - Despite the exponential increase in the online sexual exploitation and abuse of children globally over the past decade, many governments around the world do not have the infrastructure and capacity necessary to adequately respond to and investigate suspected cases. Given the global and transnational nature of OSEAC, it is incredibly important for the U.S. government to support other governments' capacities to respond to this crime and coordinate and share information about victims and perpetrators and conduct joint investigations as appropriate to ensure as many victims are removed from harmful situations as possible, and perpetrators are brought to justice. This includes the promotion of cross-industry collaboration via data-matching detection systems. Opening regulations to explicitly allow for cross-industry data collaboration for the purposes of detecting and reporting crimes against children would also aid in quickly identifying victims and offenders of livestreamed abuse. IJM and partner NGOs are developing a data-matching platform that will allow tech and financial sector companies to securely match information associated with suspicions of online trafficking-related conduct, which currently remains largely undetected.

Example of strong inter-governmental coordination and collaboration:

- International Child Sexual Exploitation (ICSE) Database - The ICSE database is the sole international hub for specialized law enforcement investigators across the globe to share information and de-conflict their work with child sexual abuse material (CSAM) in a combined effort to identify children and offenders. The ICSE database has assisted numerous international and national investigations and, as of January 2022, includes information relating to over 27,700 identified and rescued child victims of sexual abuse, along with media relating to tens of thousands of victims yet to be identified or rescued. There are currently 2.7 million child abuse images and videos in the ICSE database.
- State Department's Child Protection Compact (CPC) program - CPCs are multi-year commitments, including up to $10 million in U.S. foreign assistance, between the State Department's Office to Monitor and Combat Trafficking in Persons (JTIP) and partner governments to collaborate to reduce child trafficking. CPCs support the sustainable development of partner governments' capacity to prevent and respond to child trafficking, including OSEAC. The Philippines, a global OSEAC hotspot, was party to a CPC from 2017-2021 that supported the government in increasing its capacity to identify victims of online sexual exploitation and abuse, provide effective and appropriate child protective services, identify perpetrators and bring them to justice and improve OSEAC prevention.
- Philippines Internet Crimes Against Children Centre (PICACC) - PICACC is a collaboration between the Philippine National Police (Women and Children Protection Center, the National Bureau of Investigation), Anti-Human Trafficking Division, the Australian Federal Police, UK National Crime Agency, the National Police of the Netherlands, and IJM. Since its inception in February 2019, PICACC has conducted 179 operations, leading to 113 arrests and the rescue of 526 victims of online sexual

exploitation. PICACC's work continued despite the challenge of COVID-19 lockdowns, with 48 operations conducted during the height of the pandemic.

Current and Future Industry Efforts to Mitigate Harms and Promote Benefits

The technology sector, as the proprietors of the online platforms upon which OSEAC is occurring, have a responsibility to take action to ensure they are mitigating the risks children are experiencing online. This should include taking clear, concrete steps to improve and expand efforts to prevent and respond to online sexual exploitation and abuse of children. Actions the technology sector should take in the future include:

1. Improve identification and handling of child sexual abuse materials (CSAM) – Of the more than 32 million reports made to NCMEC's CyberTipline in 2022, over 31 million were submitted by electronic service providers. To prevent their services from being used to manufacture and distribute CSAM and to decrease the volume of existing CSAM on their platforms, the technology sector should commit to taking the following actions:

a. Proactively scan platforms for known and unknown CSAM and live-streaming of OSEAC using the latest available technologies. - Under current U.S. law, online platforms are only required to report CSAM once they become aware of it and are not obligated to proactively scan for these materials. Without a clear commitment to proactive scanning, it is impossible to know the true scale of the creation and proliferation of CSAM on online platforms. Of the 32 million CyberTipline reports mentioned above, nearly 27 million were submitted by Meta-owned platforms - Facebook, Instagram and WhatsApp. In contrast, other large technology companies, like Google, Twitter and Amazon, with similarly large user bases only submitted a fraction of reports, suggesting that a high level of CSAM is likely not being detected by current efforts. Groundbreaking artificial intelligence tools and other detection methods exist to protect children from this violent harm and persistent trauma. Proactive scanning should include the use of automated tools to identify existing CSAM through photo hash-matching against relevant databases like NCMEC's hash database, and machine learning to detect new CSAM that has not yet been submitted to these databases. Deploying these or similar tools will make online communities safer, improve detection of abuse and support law enforcement's efforts around the world to identify and protect children suffering ongoing sexual abuse, but only if platforms prioritize detection, disruption, and reporting of CSAM as an essential business function.

Examples of existing technology that supports proactive scanning:

- PhotoDNA - PhotoDNA was created in 2009 by Microsoft in partnership with Dartmouth College. PhotoDNA assigns an identifying "hash" or digital signature to CSAM images. Once a new CSAM image is identified it is assigned a hash and imported into relevant databases, like NCMEC's. Entities like law enforcement, civil society organizations and technology companies can then use these hashes to find additional copies of these images without having to review the same images multiple times. The process of creating the hash is not reversible and CSAM cannot be recreated.
- Shield by Project Arachnid - As part of their Project Arachnid, a set of tools that support the automatic detection of CSAM, the Canadian Centre for Child Protection created Shield that offers a no-cost API to electronic service providers to support proactive CSAM detection.
- Safer - Created by Thorn, Safer utilizes machine learning algorithms to support online platforms efforts to identify both known and unknown CSAM. Safer also provides content

moderation tools designed with consideration to moderators' wellbeing, supports the secure storage of identified CSAM as it is reviewed and reported and supports the development of new "hashes" that are shared with the broader community.

b. Once CSAM is detected, immediately submit a report to NCMEC's CyberTipline and permanently remove the flagged files. - Under current U.S. law, technology companies are required to report identified CSAM on their online platforms. However, the removal of these materials when flagged by users, victims and survivors and civil society can sometimes be a slow and frustrating process. In its 2022 CyberTipline report, NCMEC recorded the time it took between the organization sending electronic service providers notifications on flagged images and videos and the removal of these materials. While the average time was less than two days, many prominent online platforms took significantly longer. Facebook, for example, averaged over four days before the content was removed and Instagram averaged over three days. Slow removal times not only contribute to the continued retraumatization of children and older survivors depicted in these materials, but it also allows for the materials to continue to be downloaded, shared and reuploaded by perpetrators, furthering their spread. Once notified by NCMEC, law enforcement, and other relevant outside parties, platforms should remove suspected CSAM within at most 48 hours. If platforms report suspected CSAM to NCMEC, they should remove that reported material immediately from their platforms. Additionally, reports should be categorized to reflect the urgency of the crime. For example, live-streamed abuse, which is currently on the rise, presents urgent and ongoing harm that needs to be addressed more quickly.

Examples of legislation that would place new requirements on online platforms to improve the reporting and removal of CSAM:

- Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Maltreatment (STOP CSAM) Act (S.1199) - Empowers victims by making it easier for them to ask tech companies to remove child sexual abuse material and related imagery from their platforms and by creating an administrative penalty for the failure to comply with a removal request. Permits victims of online child sexual exploitation to bring a civil cause of action against tech platforms and app stores that promoted or facilitated the exploitation, or that host or store CSAM or make it available and creates a criminal provision that prohibits the same conduct. Strengthens current CyberTipline reporting requirements.
- Revising Existing Procedures on Reporting via Technology (REPORT) Act (H.R.5082; S.474)- Requires websites and social media platforms to report violations of federal crimes involving child sex trafficking (e.g. ads selling children for sex) and online enticement or coercion of children; increase the fine (up to $850,000) for websites and social media platforms that knowingly and willfully fail to report child sexual abuse material and online child sexual exploitation; and increase the time that websites and social media platforms are required to preserve evidence for reports that they submit to the CyberTipline, giving law enforcement more time to investigate and prosecute.
- Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act (H.R.2732; S.1207)- Creates new reporting requirements for online platforms to the National Center for Missing and Exploited Children (NCMEC)'s CyberTipline for online service providers and increases the length of time providers must preserve contents of CyberTipline reports from 90 days to one year..

  Related:
  - Child Online Safety Modernization Act (COSMA) (H.R.5182) - Identical to the House version of the EARN IT Act, with the exception of the amendments to Section 230.

- END Child Exploitation Act (H.R.6246) - Increases the length of time online service providers must preserve the contents of the report submitted to the National Center for Missing and Exploited Children (NCMEC)'s CyberTipline - from 90 days to 1 year.

c. Improve collaboration and coordination with law enforcement to support OSEAC investigations. - To better support law enforcement's OSEAC investigations, technology companies should prioritize rapid responses to information requests and warrants and retain vital data included in reports made to NCMEC's CyberTipline on secure, internal servers until law enforcement is able to utilize the data to support their investigations**.** Improving response times to information requests and warrants not only supports law enforcement's efforts to more quickly identify perpetrators but also identify victims and potentially remove them from ongoing abuse and harmful situations. Retention of critical data is also central to investigations. Currently, electronic service providers are only required to retain data included in their CyberTipline reports for 90 days. However, with the number of reports continuing to rise exponentially every year, this time period is often too short for law enforcement to start investigations, which risks critical information about victims and perpetrators being lost. Extending the time period in which this data is retained by electronic service providers will ensure law enforcement has sufficient time to utilize it in their investigations.

See examples of legislation that would improve collaboration and coordination with law enforcement above.

d. Invest in the development of new tools to detect, report and remove CSAM, particularly alongside encrypted environments. - In addition to utilizing existing tools, the technology sector should also invest in the development of new technologies that advance current capabilities to detect and remove CSAM and commit to sharing these new technologies with relevant, trusted actors from other technology companies and law enforcement. This should include exploring and developing tools that allow for the identification of CSAM even within applications and messaging services that utilize end-to-end encryption. Encryption is a vital tool to ensure users', including children's, privacy. However, without appropriate tools that allow for scanning of messaging and file sharing in encrypted environments, either prior to encryption or through another process, a significant portion of CSAM will remain undetected. In 2019, when Meta (then Facebook) announced a plan to adopt end-to-end encryption throughout its platforms, NCMEC estimated that the plan would result in loss of up to 70% of Meta's (then Facebook's) annual reports. With Meta continuing to be the leader in detecting and reporting CSAM found on its platforms, that would represent the vast majority of reports made to NCMEC each year. Tools that enable client-side image detection technologies have already been created by SafeToNet and DragonflAI, but have not been used broadly. These technologies detect CSAM before it can enter an end-to-end encrypted environment. Use and refinement of these tools and others could support the continued detection of CSAM while still allowing for the implementation of stronger privacy protections. It is incredibly important that alongside conversations related to improving users' privacy, whether through government regulation or voluntary actions by platforms, that this critical aspect of children's privacy and safety, the detection and removal of CSAM, is not lost.

e. **Update digital policies and voluntarily filtering child sexual abuse material (CSAM) on public WIFI.** – Companies that provide free WIFI services should put into place policies that align with industry best practices and outline how the service should be utilized by their patrons, as well as filters for CSAM that prevent users from accessing it via their network. This will prevent patrons, guests and staff from being exposed to CSAM; prevent children and teens from

bypassing parental controls and filters when using free WIFI services; and prevent perpetrators from accessing CSAM in public spaces.

2. Increase transparency on tech companies' internal efforts to prevent and respond to OSEAC on online platforms. – The technology sector should commit to improving their transparency around how they are addressing online risks to children on their platforms. Currently, most online platforms share very little about their internal processes, which makes it difficult for child users and caregivers to make informed decisions about whether a platform is safe for children. Online platforms should produce annual reports conducted by independent third parties that outline how they assess risks on their platforms, any risks to children they have identified and their mitigation strategies for addressing these risks. This should include their practices to proactively identify and prevent OSEAC on their platforms, including grooming behaviors, the production and distribution of CSAM and livestreaming of children's abuse and exploitation. These reports should be made public to ensure child users and their caregivers fully understand the risks posed by online platforms and can make informed decisions about their use. Law enforcement and researchers from academia and civil society should also be given more detailed, secure access to platforms internal processes and reporting to support greater understanding of OSEAC's prevalence and how offenders are utilizing online platforms to target children. While the Tech Coalition's recently released Voluntary Framework for Industry Transparency, created in partnership with a number of prominent online platforms, is a positive step, it lacks an effective mechanism to hold online platforms accountable to their commitments under the framework and allows platforms a lot of leeway in determining how they are implementing the framework. This will lead to inconsistent application of the framework and continue to make it difficult for policymakers, civil society and the general public to assess the effectiveness of platforms' risk mitigation efforts.

Examples of promising legislation that would require online platforms to improve their transparency and accountability include:

- Kids Online Safety Act (S.1409) - In addition to mandating important safety-by-design standards (outlined below), the Kids Online Safety Act would also require online platforms to release annual reports based on third-party audits that describe any identified risks to children that use their services and the platforms' mitigation efforts.
- Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Maltreatment (STOP CSAM) Act (S.1199) - Requires large tech companies that are subject to the CyberTipline statute to submit annual reports describing their efforts to promote a culture of safety for children on their platform;

3. Adopt a safety-by-design approach that centers children's best interests and embeds child safety tools within platforms. - Technology companies' adoption of a safety-by-design approach would strongly support the prevention of OSEAC and the targeting of children on their online platforms. Ideally, these standards should be consistent across all platforms to ensure children experience the same level of protection across the internet.

These standards should include (but aren't limited to):

- Default safety, privacy and data protection settings that do not require a child user or a parent to "opt-in" or activate. These features should support the prevention of child users' access or exposure to harmful material; prevent interactions between children and unknown adult users; and limit the collection, use and retention of children's data
- Age estimation tools to ensure children are not able to access and use platforms inappropriate for those under 18\

- Prominent, easy-to-access and child-friendly resources and reporting mechanisms that include links to resources that explain what OSEAC is, how children can protect themselves, how to discuss an upsetting incident with a caregiver or trusted adult, and child-friendly instructions on when and how to submit a report
- Methods for detecting, reporting and removing adult users who target and/or pose a risk to children on online platforms. This could include the use of AI technology and human monitors to identify grooming and other inappropriate behaviors of adult users towards child users.

Examples of legislation that would require technology companies adopt a safety-by-design approach include:

- Kids Online Safety Act (S.1409) - The Kids Online Safety Act would create a duty of care for online platforms to act in children's best interests and to prevent and mitigate harms to children under 18. It would also require platforms to enable parental tools and provide strong protective settings by default for users under 18. These settings would limit the ability of adults unknown to the child user from being able to contact the child; limit public access to children's public data; restrict the use of platforms features meant to encourage users' continued use of the platform; allow child users and parents to opt-out of personalized recommendations; restrict the use of child users' geolocation; limits for child users' time on the platform; and allow for the deletion of child users' accounts and personal data. It would also require online platforms to provide parents and child users with easily accessible means to report any harms experienced by the child user that platforms will be required to respond to in a timely manner.
- Eliminate Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act (S.1207) - Establishes the National Commission on Online Child Sexual Exploitation Prevention, which will develop best practices for online service providers to prevent, reduce, and respond to the online sexual exploitation of children.
- California Age-Appropriate Design Code - The law in California applies to businesses that provides an online service, product, or feature likely to be accessed by children under the age of 18 and meet one or more of the following criteria: have $25 million or more in annual gross revenue; buy or sell the personal information of 100,000 or more users; or derive 50% of annual revenue from selling or sharing consumers' personal information. Under the CA law, these companies must 1) stop selling personal information of children or using it in a way that they do not have express permission for and must default to the highest privacy settings for children and communicate privacy notices in an age appropriate manner; 2) stop profiling kids and instead design the user experience based on age; 3) stop collecting personal information on children; 4) make it easier to report privacy concerns; 5) stop tracking the location of children unless it is an essential part of the service; 6) let children know when they are being monitored or tracked; 7) establish the age range of users with a reasonable level of certainty appropriate to the risks involved to children; and 8) conduct a risk assessment of how children's data is used.
- UK Age-Appropriate Design Code**:** The UK Age-Appropriate Design Code includes 15 standards that online services that children under age 18 are likely to access need to follow to meet the requirements of the data protection law to protect children's data online. The online services that are covered by the code include apps, programs, search engines, online messaging or voice over internet phone (VOIP) services, social media platforms, online marketplaces, content streaming services, online game services, news or educational websites; any websites offering other goods or services to users over the internet, and toys or devices that connect to the internet. The standards require any online service provider to provide a Data Protection Impact Assessment to the

Information Commissioner's Office (ICO) that identifies the risks to children, ways to mitigate the risks, and balances the competing interests of access for children of various age groups. To adequately assess the risk, the online service must be able to accurately determine age, which requires some type of assurance system be in place such as self-identification, artificial intelligence, third party verification, or government ID. To protect children's privacy, online services are also limited to collecting only the amount of information necessary to provide the core service being offered without specific opt-ins by the users. The privacy information and the ability to opt-in must be communicated to the user at an age-appropriate level. All service providers will be held accountable for the information that is provided to the ICO.

Conclusion

We applaud the administration for the creation of the Kids Online Health and Safety Task Force, its growing public acknowledgement of the increasing risks facing children online and its commitment to take action. While online sexual exploitation and abuse of children is a complex issue, it is not one that is insurmountable. Addressing key gaps in prevention, support for children and youth's mental health, victim and survivor services, research and data collection and technology sector accountability will have a substantial impact in improving children's online safety.

We are grateful to the Task Force for allowing the submission of recommendations as it determines its next steps on how to address this crisis. We are hopeful this will be the start of ongoing consultations and discussions between the administration, civil society, survivors and online platforms to discuss how we can improve the prevention of and response to OSEAC. We are happy to provide additional support to these efforts and offer ourselves as a resource to the Task Force as your efforts continue to develop and are underway.

Sincerely,