Suojellaan Lapsia
Protect Children

Online Child Sexual Abuse and Exploitation: Current and Emerging Threats

Contribution to the Special Rapporteur on the sale and sexual exploitation of children's call for input: Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

Protect Children

May 2024

About this Statement

This Statement, written by Suojellaan Lapsia, Protect Children ry. (Protect Children), aims to inform the Special Rapporteur on the sale and sexual exploitation of children's forthcoming report to the 79th session of the UN General Assembly in October 2024. This report answers the call for input as set out by the Special Rapporteur on the sale and sexual exploitation of children.

The Statement examines the alarming escalation of child sexual abuse and exploitation in the digital environment. In order to do so, this statement outlines practices of sexual violence against children within the online environments, on the one hand; and provides practical solutions in reference to the questions posed in the Special Rapporteur's call for input, on the other hand.

The ultimate goal of this statement is to highlight the need to develop more effective prevention and intervention strategies, as well as to advocate for the immediate development of robust and comprehensive regulations that strengthen children's rights and ensure their protection from harm across all environments, including the digital sphere.

Protect Children

Protect Children is a non-governmental child-rights organisation based in Finland, working globally to end all forms of sexual violence against children. We adopt a holistic, research-based approach to address the issue from multiple angles, advocating for victims, survivors, and families; equipping children and young people with essential skills and knowledge to stay safe online and offline; developing offender-focused prevention measures; and conducting innovative research to better understand the issue.

Learn more about Protect Children: www.protectchildren.fi/en

Table of Contents

1. Introduction

The proliferation of online child sexual abuse and exploitation presents a serious threat to children globally. In 2023, the US National Center for Missing and Exploited Children (NCMEC) received over 36.2 million reports of suspected child sexual exploitation[i], which represents a 72% increase over the number of reports received in 2020, when NCMEC received more than 21 million reports.[ii]

One of the forms of sexual violence against children that has increased dramatically in recent years is the creation, distribution, and viewing of child sexual abuse material (CSAM). This is, images, videos, live-streaming and any other material depicting real or simulated child sexual abuse and/or exploitation.[iii] This type of sexual violence against children is particularly traumatic for the victims, since it contributes to their revictimisation every time the material is viewed and/or shared. Such material consists of a permanent record of the abuse and can have long-lasting consequences on victims and survivors.[iv]

Recent research conducted by Protect Children reveals that CSAM is easily accessible on the surface web, particularly on pornography websites and social media platforms.[v] This research has shown that offenders are using popular social media platforms and encrypted messaging applications to search for, view and disseminate CSAM.[vi] Furthermore, perpetrators are misusing and abusing different technologies and platforms, such as Artificial Intelligence (AI) or Extended Reality (XR), not only to create and share CSAM, but also to sexually abuse and exploit children online in other forms, such as grooming or sexually extorting children.[vii] Hence, emerging technologies are facilitating online harms and resulting in new and even worse forms of online child sexual abuse and exploitation.[viii]

This Statement analyses technological abuses for child sexual abuse and exploitation, answering Questions 1, 3, 4 and 7 of the call for input. Subsequently, in Annex 1, we provide actionable recommendations directed at relevant stakeholders from the tech industry, among other actors, to prevent the proliferation of CSAM on the Internet and effectively address online child sexual abuse and exploitation, thus answering Questions 2, 5, 7, 8 and 9 of the call for input.

2. Child Sexual Abuse and Exploitation in the Digital Age and Respective Challenges

2.1. The Surface Web, Social Media Platforms and End-to-End Encryption

Recent research has shown that CSAM is available on the surface web, including on social media platforms.[ix] In response to Protect Children's survey of individuals searching for CSAM on dark web search engines, 77% of the respondents reported that they have encountered the material or links to CSAM somewhere on the surface web, such as on a pornography website (32%), on a social media platform (29%), or on a messaging application (12%). The most frequently mentioned social media platforms used to search for, view and share CSAM were Instagram, X (Twitter), Discord, and TikTok.[x]

Recommendation algorithms, such as those on TikTok and Instagram, have been reported to promote 'self-generated'[1] CSAM and facilitate CSAM trading.[xi] Research has shown that

[1] The term 'self-generated CSAM' fails to adequately emphasise the unintended and non-consensual nature of such material depicting sexual violence against children, which often arises from grooming or

perpetrators take advantage of this by falsifying their profile age to appear as a child or adolescent, thus prompting the algorithm to suggest content from children and/or adolescents with similarly listed ages.[xii] Age falsification makes it easier for offenders to gain the trust of a child online, who assumes they are communicating with a same-age peer. Offenders are able to use social media to search for children in vulnerable situations to groom and sexually extort them, which can lead to further offences.[xiii]

Furthermore, research done by Protect Children has shown that messaging apps such as Telegram and WhatsApp are popular among CSAM offenders to view and distribute CSAM. These apps provide security and privacy due to end-to-end encryption (E2EE) which involves a closed connection between communicants, preventing outside monitoring of a conversation chain's content. Such features as secret chats, self-destruct messages, ability to edit and delete messages for all parties, private groups and channels[xiv] create a safe space for exchanging of CSAM and sharing information that can facilitate more sexual violence against children with a "minimal digital footprint".[xv] As such, CSAM on end-to-end encrypted platforms such as these is virtually impossible to detect, resulting in the reduced removal of CSAM and proliferation of CSAM dissemination.[xvi]

2.2. Artificial Intelligence

Artificial Intelligence (AI) has also created a very unique difficulty in identifying the victims depicted in the images, videos, and other depictions of sexual violence against children. Recent technological advancements have seen AI image-generation platforms, wherein a user inputs a prompt in text and the AI produces an image based on it. Perpetrators misuse AI in various ways, among which are manipulation of photos or videos of children, including existing CSAM, creation of completely new, AI-generated material depicting sexual abuse of children, 'nudification', i.e., altering clothed images of children so that they appear naked, and de-aging algorithms that can make people look younger.[xvii]

AI-generated CSAM is promoted within offender communities as a 'harm-free' approach much in the same way they may claim viewing CSAM is not harmful if it already exists and they are not actively contacting children and/or creating new content.[xviii] This is, however, false. AI-generated CSAM promotes sexual violence and abuse of children, normalizing it for offenders who view it as 'just a picture'. It often, however, is not just a picture: previous research by Protect Children shows that offenders who consume CSAM more frequently are more likely to attempt to contact a child[xix], making any argument of a 'lesser evil' baseless.

Additionally, AI algorithms have become so advanced that they can generate content indistinguishable from real photos and videos, even to a trained eye.[xx] This leads to wasted law enforcement resources. As the creation of AI-generated CSAM grows, law enforcement is spending an increased amount of time analysing images to identify children who do not exist. All these tools can be used to produce an unlimited number of images offline, so the offenders face no risk of being detected.[xxi]

2.3. Online Gaming

Online gaming platforms with player-to-player interaction features are also used by the offenders to establish contact and 'befriend' children. The dangers of online games are often

sexual extortion. As we explore a more appropriate term, we continue to use 'self-generated' CSAM providing additional remarks and acknowledging its drawbacks.

overlooked because children do not expect a real-life danger in a virtual world, so they feel the safest on these platforms.[xxii] This normalised communication with strangers online can be exploited by the perpetrators. Since it is not required to reveal any personal information, it is easy for the offenders to hide their real identity and deceive minors, which can result in grooming – a violence that is slow and difficult to spot – and then further lead to other forms of child sexual abuse and/or exploitation.

2.4. Anonymity on the Dark Web

Similarly to E2EE, by offering users anonymity and evading surveillance, the dark web provides a haven for illegal activities, including the proliferation of CSAM. 21 out of 26 Tor search engines were reported to provide CSAM results, with four of those engines actively promoting and advocating for this material.[xxiii] Approximately 20% of the unique websites hosted through Tor network share CSAM.[xxiv] Moreover, a significant portion of search sessions within these domains seek CSAM, amounting to 11% of the search queries.[xxv] Such a sheer volume of and demand for CSAM on the dark web has effectively overwhelmed law enforcement agencies, making it difficult to identify and remove all the CSA content without the use of technology. Additionally, forums within the dark web serve as hubs for like-minded individuals to connect, validate each other's actions, and share CSAM, which perpetuates sexual abuse and exploitation of children even further.[xxvi] To track down offenders while complying with legal and ethical standards to maintain the balance between protecting individual's right to privacy and combating illegal activities has become a significant difficulty for law enforcement.

3. Conclusion

In summary, a global standard is crucial to combat the rising statistics associated with sexual violence against children online. Perpetrators are frequently accessing various platforms and applications that are 'hot spots' to communicate with children. These platforms are becoming increasingly dangerous for victimisation and are being protected by E2EE and a dearth of regulation.

Law enforcement agencies face various challenges due to the new technology. Particular areas of difficulty include but are not limited to online gaming, platforms which feature E2EE, the anonymity features of the dark web, abundant pre-existing sexual violence against children on the surface web, rapidly evolving AI, and limited access to livestreams.

The implementation of prevention and intervention measures and the development of a robust and comprehensive legal framework are crucial to ensure the removal and inaccessibility of sexual violence against children across all platforms. Through a multidisciplinary approach and effective collaboration and awareness, we can efficiently work towards combating sexually exploitative abuse against children and ensure the safety of vulnerable populations in digital environments.

References

[i] NCMEC (2024). CyberTipline 2023 Report. https://www.missingkids.org/cybertiplinedata

[ii] NCMEC (2023). CyberTipline 2022 Report. https://www.missingkids.org/cybertiplinedata

[iii] Greijer, S. & Doek, J. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse: Adopted by the Interagency Working Group in Luxembourg, 28 January 2016, ECPAT International & ECPAT Luxembourg. https://www.unicef.org/media/66731/file/Terminology-guidelines.pdf

[iv] Canadian Centre for Child Protection (2017). Survivor's Survey: Executive Summary 2017. https://content.c3p.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf; Canadian Centre for Child Protection (2017). Survivor's Survey: Full Report 2017.

[v] Protect Children (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[vi] Protect Children (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[vii] WeProtect Global Alliance (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/

[viii] Protect Children (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[ix] Protect Children (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[x] Protect Children (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[xi] Thiel, D., DiResta, R., & Stamos, A. (2023). Cross-Platform Dynamics of Self-Generated CSAM. https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf

[xii] Thiel, D., DiResta, R., & Stamos, A. (2023) Cross-Platform Dynamics of Self-Generated CSAM. https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf

[xiii] Protect Children (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[xiv] Telegram FAQ. (n.d.). Telegram. https://telegram.org/faq?setln=en#q-there39s-illegal-content-on-telegram-how-do-i-take-it-down

[xv] Protect Children (2024). Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry. https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

[xvi] Insoll, T. & Ovaska, A. (2023). Encrypted Services and Messaging Apps Are Being Used to Contact Children and Disseminate Child Sexual Abuse Material. Protect Children. https://www.suojellaanlapsia.fi/en/post/encryption-onlinechild-sexual-abuse-statement

[xvii] Internet Watch Foundation (2023). Prime Minister must act on threat of AI as IWF 'sounds alarm' on first confirmed AI-generated images of child sexual abuse. https://www.iwf.org.uk/news-media/news/prime-minister-must-act-on-threat-of-ai-as-iwf-sounds-alarm-on-first-confirmed-ai-generated-images-of-child-sexual-abuse/

[xviii] Internet Watch Foundation (2023). How AI is being abused to create child sexual abuse imagery. https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

[xix] Insoll, T., Ovaska, A., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk Factors for Child Sexual Abuse Material Users Contacting Children Online. https://www.suojellaanlapsia.fi/en/post/risk-factors-for-child-sexual-abuse-material-users-contacting-children-online

[xx] Nightingale, S.J. & Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. Proc Natl Acad Sci USA. https://pubmed.ncbi.nlm.nih.gov/35165187/

[xxi] Internet Watch Foundation (2023). How AI is being abused to create child sexual abuse imagery. https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

[xxii] WeProtect Global Alliance (2023). Global Threat Assessment 2023. https://www.weprotect.org/global-threat-assessment-23/#full-report

[xxiii] Nurmi, J., Paju, A., Brumley, B., Insoll, T., Ovaska, A., Soloveva, V., Vaaranen-Valkonen, N., Aaltonen, M., & Arroyo, D. (2024). Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy. https://www.nature.com/articles/s41598-024-58346-7

[xxiv] Nurmi, J., Paju, A., Brumley, B., Insoll, T., Ovaska, A., Soloveva, V., Vaaranen-Valkonen, N., Aaltonen, M., & Arroyo, D. (2024). Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy. https://www.nature.com/articles/s41598-024-58346-7

[xxv] Nurmi, J., Paju, A., Brumley, B., Insoll, T., Ovaska, A., Soloveva, V., Vaaranen-Valkonen, N., Aaltonen, M., & Arroyo, D. (2024). Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy. https://www.nature.com/articles/s41598-024-58346-7

[xxvi] Huikuri, S., & Insoll, T. (2022). Peer-Support of Child Sexual Abusers in Darknet Online Communities. https://www.suojellaanlapsia.fi/en/post/darknet-online-communities-of-child-sexual-abusers

Annex 1

Suojellaan Lapsia
Protect Children

Actionable Recommendations for the Tech Industry

Annex to the research report:
Tech Platforms Used by Online Child Sexual Abuse Offenders

Suojellaan Lapsia, Protect Children ry.
February 2024

AI-generated image

#ReDirection

Safe Online
TECH COALITION

Protect Children

Protect Children is a non-governmental, non-profit organisation based in Helsinki, Finland, working globally to end all forms of sexual violence against children. We adopt a holistic, research-based approach to address the issue from multiple angles, advocating for victims, survivors, and families; equipping children and young people with essential skills and knowledge to stay safe online and offline; developing offender-focused prevention measures; and conducting innovative research.

Learn more about Protect Children: www.suojellaanlapsia.fi/en

Authors

This report is written by Tegan Insoll, Head of Research; Valeriia Soloveva, Specialist; Eva Díaz Bethencourt, Specialist; Anna Ovaska, Deputy Director; and Nina Vaaranen-Valkonen, Executive Director.

Funding

The research presented in this report was conducted within Protect Children's Primary Prevention to Protect Children research project which is funded by the Tech Coalition Safe Online Research Fund.

Safe Online is the only global investment vehicle dedicated to keeping children safe in the digital world. Through investing in innovation and bringing key actors together, Safe Online helps shape a digital world that is safe and empowering for all children and young people, everywhere. The Tech Coalition Safe Online Research Fund is a groundbreaking collaboration fuelling actionable research and uniting the tech industry with academia in a bold alliance to end online child sexual exploitation and abuse.

Learn more: https://safeonline.global/tc-safe-online-research-fund/

Acknowledgements

Thank you to our project partners, Red PaPaz, Helsinki University Hospital, Dr. Juha Nurmi, Ahmia.fi; and Professor of Criminology, Mikko Aaltonen, University of Eastern Finland; to the UK Online CSEA Covert Intelligence Team for providing crucial information for this report; and to Simon Bailey, CBE, QPM, DL, MSt (Cantab), for your guidance and feedback on this report in your role as Expert Advisor to Protect Children. We would also like to extend a warm thank you to all our global colleagues who have provided their expertise and translated the research surveys mentioned in this report, and to Webropol Oy for continuing to support our work by hosting our research surveys.

Suggested citation: Suojellaan Lapsia, Protect Children ry. "Actionable Recommendations for the Tech Industry" Annex to the research report: Tech Platforms Used by Online Child Sexual Abuse Offenders. (2024).

This publication has been produced with financial support from the Tech Coalition Safe Online Research Fund. However, the opinions, findings, conclusions, and recommendations expressed herein are those of the author Protect Children and do not necessarily reflect those of Safe Online or the Tech Coalition.

Key Findings

1. CSAM is easily accessible on the surface web, particularly on pornography sites and social media
   - Most respondents have encountered CSAM on the surface web
   - The surface web provides information on how to access CSAM on the dark web
2. Offenders view and share CSAM on popular social media and encrypted messaging apps
   - Social media platforms are used to search for, view & share CSAM
   - End-to-end encrypted messaging apps are used to search for, view & share CSAM
3. Perpetrators seek contact with children on social media, encrypted messaging apps, and online games
   - Many respondents have sought contact with children on social media
   - Offenders use online gaming platforms to seek contact with children
   - Encrypted messaging apps are used by perpetrators to contact children

Actionable Recommendations

The findings presented in this report highlight key issues that require urgent action by the tech industry, among other actors. On the basis of the findings of this research, alongside insights from our work, we have developed five actionable recommendations for the tech industry.

The recommendations should be considered holistically, as one approach alone is not adequate to tackle the enormous scale of the problem of online child sexual exploitation and abuse. All actors have a responsibility to address sexual violence against children and keep children safe in all environments.

1. Build and develop platforms with a children's rights-by-design approach
2. Ensure availability and accessibility of online safety resources and information for children
3. Effectively detect, report, and remove CSAM and combat OCSEA
4. Implement deterrence and perpetration prevention measures
5. Ensure robust and proportionate age assurance measures

Suojellaan Lapsia
Protect Children

Safe Online

TECH COALITION

RECOMMENDATION 1

Build and develop platforms with a children's rights-by-design approach

We urge service providers to place children's safety and rights at the forefront of technological development and ensure that digital environments are designed to prioritise children's rights.

We recommend tech companies to design platforms with a children's rights-by-design approach.[1] Child safety must be prioritised in the development of services that are available to children and can influence their safety or well-being. Technology companies should enrich safety-by-design by incorporating children's voices and providing accessible, child-friendly, and effective reporting tools with a meaningful response system.

End-to-end encryption should not be implemented without appropriate safeguards. Encrypted platforms are quickly becoming a safe haven for child sexual abuse offenders. The rollout of end-to-end encryption on tech platforms, without appropriate safeguards, directly undermines a children's rights-by-design approach, as it hinders law enforcement efforts to identify and rescue victims, prevents identification of grooming, and prevents tech companies' ability to detect child sexual abuse material. This puts children at increased risk of abuse and exploitation and continues the cycle of revictimisation of survivors. As such, we urge tech companies not to implement end-to-end encryption on their services unless they put in place further safeguards to ensure access to evidence by law enforcement and maintain the ability to detect and report child sexual abuse material.

Avoid misuse of functionality provided by the platform. Technology companies must subject all updates to thorough trials to engineer out the possibility to abuse its tools to harm children, always with guidance from children's perspectives. One of the ways to address misuse of the platform's functions is to limit opportunities for contact and interaction between adult and child users, i.e., by making accounts of child users invisible for adult users.

Monitor and address emerging threats. Technology companies must take a proactive approach in maintaining child safety by design by continuously monitoring and eliminating emerging risks. This includes constant improvement of existing filtering algorithms, age verification systems, and any other safeguarding mechanisms in place.

Follow good practices when using AI technologies. Online service providers must invest in good practices when using AI technologies and elaborate clear guidelines for privacy, personal data protection and information, and user safety. In addition, service providers must implement robust measures to reduce or eliminate the risk of AI being misused or abused, for example to generate CSAM. At the same time, we encourage tech companies to invest resources in AI technologies that contribute to preventing harm, and to train AI algorithms with a focus on child protection and a human rights-based and intersectional perspective, to avoid discrimination and bias.

Any platform that can be accessed by children or influence their safety and well-being must be built with a children's rights-by-design approach. Children must be provided with an opportunity to meaningfully participate in the product development and share their experiences through an effective reporting system. Children's inherent vulnerabilities must not be exploited for profit.

RECOMMENDATION 2

Ensure availability and accessibility of online safety resources and information for children

We call on online platforms to ensure that online safety resources and information are provided in a comprehensive and accessible manner for all children, families, victims, and survivors.

As evidenced by the research report, social media, instant messengers, and online games are all being used to commit crimes of sexual violence against children. As such, internet service providers have the responsibility to ensure that the rights of the child are respected on their platforms. Moreover, internet service providers must ensure sure that children understand the rights they are entitled to online, understand how their rights are protected, and be well-informed about the safeguarding mechanisms at their disposal.

Inform children about their rights online. Tech companies must take effective measures to guarantee children's right to information on their platforms. All information and resources must be comprehensive, available, and accessible to all children and young people. The right to information expands to children and young people's families, as well as to victims and survivors. Internet service providers should offer age-appropriate information in all languages and the information should be culturally adapted to ensure equal access.

Offer comprehensive information about safeguarding mechanisms. Over three quarters of respondents to our survey reported that they have encountered CSAM on the surface web, highlighting that CSAM is widely accessible and available on common online platforms and websites. As a result, involuntary exposure to harmful material among children and young people is prevalent. Internet service providers must provide clear and age-appropriate information about what constitutes illegal behaviour or content with relevant examples. Internet service providers must ensure that support and safeguarding mechanisms are easily accessible and well explained, so if a child or young person is concerned about their safety, they know how to access appropriate support. This contributes to prevent discrimination and re-victimisation in case of child victims.

We encourage internet service providers to offer relevant, country-specific, and accessible information for children on where to seek support in cases when a child feels that the platform negatively influences their well-being, when exposed to harmful or illegal content, or when subject to online sexual violence. Internet service providers should inform children what cases must be reported to the police and explain the procedure of reporting. We encourage internet service providers to offer information about available support after a child user blocks another user or flags inappropriate content.

Adopt an intersectional approach. Children belonging or identifying themselves with minority groups are at greater risk of being exposed to online child sexual abuse and exploitation, according to WeProtect Global Alliance.[2] As such, internet service providers must take measures to effectively combat sexual violence against children from all angles. Adopting an intersectional approach means recognising the differences between children and understanding the co-existence of multiple forms of discrimination among them, based on gender, race, ethnicity, gender identity, sexual orientation, disability, class, and other grounds of discrimination. Through an intersectional approach, internet service providers can ensure that their platforms are adapted and accessible for all children. Ultimately, this would help to ensure that children can stay safe in the digital environment.

RECOMMENDATION 3

Effectively detect, report, and remove CSAM and combat sexual violence against children online

We urge all internet service providers to take active steps to detect, report, and remove child sexual abuse material from their platforms, and to eliminate all forms of sexual violence against children.

Our research results find that child sexual abuse material is widely accessible and available on the surface web, especially on pornography sites and social media platforms. The circulation of child sexual abuse material online leads to the continuous revictimisation of survivors of sexual violence. In addition, the accessibility of the material increases the risk of exposure to harmful material to children and young people, which has been found to be associated with an increased risk of harmful sexual behaviour.[3]

Proactively detect child sexual abuse material. Reactive detection of child sexual abuse material based on user reports is an important measure to ensure the removal of abusive material from online platforms. However, this alone is inadequate to address the proliferation of CSAM online, and efficient proactive detection measures must be adopted. In 2022, electronic service providers sent more than 31.8 million reports of suspected child sexual exploitation to NCMEC's CyberTipline.[4] These reports are essential for helping law enforcement prioritise the most urgent cases, for identifying and rescuing victims,[5] for preventing the further victimisation of children, for empowering survivors, and for discovering trends that can assist in preventing these crimes.[6] We recognise the significant efforts of companies who currently proactively detect and report CSAM and encourage them to continue their efforts to combat child sexual abuse and exploitation.

However, only 236 electronic service providers submitted CyberTipline reports in 2022 and just five companies (Facebook, Instagram, Google, WhatsApp, and Omegle) accounted for more than 90% of the reports.[7] Most tech companies around the world still choose not to proactively detect and report child sexual abuse and exploitation on their platforms.[8] Thus, we urge all companies that host user-generated content, particularly social media platforms, messaging platforms, and file-sharing platforms, to begin proactive detection and reporting of CSAM with urgency. By both proactively and reactively detecting child sexual abuse material, tech companies have an important role in contributing to the removal of the material, thus ending the cycle of revictimisation for victims and survivors.

Cooperate with law enforcement and report information. Internet service providers must forge efficient collaboration with national and international law enforcement agencies and report any form of sexual violence against children. Law enforcement agencies must be allowed to conduct searches on the platform to ensure removal of reported, detected, or suspected child sexual abuse material. Furthermore, to facilitate ongoing investigation, it is advisable to provide relevant law enforcement agencies with access to visual and written content exchanged between the perpetrator and the victim that facilitated or constituted sexual violence against children, as well as to any other content or data collected and processed by the service provider about the victim and the perpetrator. Additionally, reporting is key to ensure the effective protection of children from abuse or exploitation and to avoid revictimisation. We urge internet service providers to report to national law enforcement agencies and national reporting hotlines any form of sexual violence against children immediately when brought to their attention.

RECOMMENDATION 4

Implement deterrence and perpetration prevention measures

We urge all internet service providers to implement effective deterrence and prevention measures for persons who are at risk of committing crimes of sexual violence against children on their platforms.

It is vital to implement effective deterrence and prevention measures for potential and actual perpetrators of crimes of sexual violence against children, to prevent offending before it occurs. As demonstrated by our research results, child sexual abuse material is widely accessible and available on the surface web, where it is not only viewed, disseminated, and procured by persons actively seeking to engage with the material, but children themselves are also being exposed to the material involuntarily. A majority of current CSAM offenders were first exposed to the material as children themselves. Finally, 40% of CSAM offenders report having sought contact with a child after viewing the material. A clear escalation within the offending pathway is visible, which underlines the importance of effective deterrence and prevention measures for people who search for and view child sexual abuse and exploitation material.

We encourage online service providers and tech companies to make available resources for individuals who are worried about their thoughts and who fear they might commit or recommit harmful acts against children. All tech companies should promote a space of respect for the rights of the child, and of safety and good practices focused on child protection. In addition, online service providers and tech companies should encourage users to report any suspicious, abusive, or harmful content involving children. The reporting processes should be simple and accessible.

All platforms that allow for image or video sharing, in particular pornography websites, must prohibit all search terms that refer to any form of child sexual abuse and exploitation and include deterrence messages to appear when searches are conducted using such terms. Deterrence messages should educate individuals about the repercussions of searching for CSAM, by clearly informing about the real-life consequences on the child victim, as well as the legal consequences of searching for and viewing CSAM or committing any other form of sexual violence against children. Deterrence messages should additionally refer individuals to relevant perpetration prevention resources for individuals at risk of committing or recommitting offences against children. These deterrence messages should appear on all platforms whenever a user searches for CSAM, attempts to contact a child, or carries out any other harmful activity online.

To keep all children safe from sexual violence comprehensively and effectively, prevention efforts must include potential offender-focused prevention and intervention measures at a low threshold.

RECOMMENDATION 5

Ensure robust and proportionate age assurance measures

We call on service providers to assure the age of all users meaningfully and consistently, using robust and proportionate measures to create a safer online experience for children and young people.

The adoption of robust age assurance measures is essential to limit opportunities for grooming, and prevent children from accessing harmful content, by regulating access of users to specific content, services, and communication with other users. Service providers should introduce robust and mandatory age assurance mechanisms for all users.

Age assurance must constitute a recurring process rather than a one-time verification to limit opportunities to circumvent the system. Based on the results of age assurance, the users should receive access to age-appropriate content and services offered by the service provider. The users should be clearly informed how and why their age influences access to particular services provided by the platform. If the platform hosts adult content, age assurance must additionally concern every person depicted in the content.

> “In my case, sexual violence has mostly happened online. I used to have free access to the internet because my parents are not very familiar with technology. It started with kid-oriented platforms, where grown men pretended to be kids and got me to give them my phone number and send them pictures of myself.”
> **Survivor of childhood sexual violence responding to the global #OurVoice survivor survey**

Technology companies must regularly monitor and eliminate opportunities to abuse the age assurance systems. They should clearly inform the users about the consequences of circumventing the age assurance system and the risks that it can cause to their safety. We also advise platforms to develop effective sanctions for circumventing age assurance system that can affect the user’s access to the platform. Users who violate the age assurance system should be identified and removed from the platform.

The age assurance measures must respect the right to personal data and privacy of communications. As implementing an effective international age assurance system that does not compromise users’ personal information constitutes a challenge, we strongly recommend supporting the research and development of new-age verification systems.

References

[1] Child rights by design. Digital Futures Commission, 5RIGHTS Foundation. https://childrightsbydesign.digitalfuturescommission.org.uk/.

[2] WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/#full-report.

[3] Mori, C., Park, J., Racine, N., Ganshorn, H., Hartwick, C., & Madigan, S. (2023). Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis. Child Abuse & Neglect, 143. https://doi.org/10.1016/j.chiabu.2023.106255.

[4] National Center for Missing & Exploited Children. (2023). CyberTipline 2022 Report. https://www.missingkids.org/cybertiplinedata.

[5] "The Child Victim Identification Program began in 2002 after NCMEC analysts repeatedly saw images of the same child victims in their reviews and began tracking which victims had been previously identified by law enforcement. So far, more than 19,100 children have been identified." National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.

[6] National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.

[7] National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.

[8] National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.