Terre des Hommes
International Federation

Call for input: Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment - submitted by Terre des Hommes International Federation on May 15, 2024

Terre des Hommes International Federation, on behalf of its global network, welcomes the UN Special Rapporteur's initiative on combating the sale and sexual exploitation of children. We emphasise the urgent need of addressing the challenges posed by digital technologies, particularly concerning the safety, mental integrity and well-being of children online. Our submission offers insights into current and emerging sexually exploitative practices targeting children in the digital sphere.

I. Technological facilitation of child sexual abuse and exploitation: understanding how digital technologies enable the exploitation and abuse of children

As a children's rights organisation, our submission underscores the importance of amplifying children's voices to the Special Rapporteur. While digital advancements offer opportunities, they also present new avenues for exploitation, emphasising the need to prioritise children's perspectives for their safety. Our primary sources for assessing technology's role in facilitating online child sexual exploitation (hereafter "OCSE") are their voices and perspectives. Through two research studies - the Child Safety by Design Research[1] and the VOICE research[2] - we reveal that:

- **Children cherish online communication, especially social media, but are aware of associated risks**. They express concerns about the impact of online activities impact mental health and the potential real-life repercussions. Their concerns include encountering strangers, exposure of offline identity, and misuse of personal information, which could lead to harm. Children from Thailand, for instance, are especially worried about image exploitation, including AI manipulation for sexual purposes. Overall, children are mainly concerned about encountering sexual content and individuals with malicious intentions.

  "*There is a lot of content on the internet that can have a negative impact on us.*" (Child safety by Design, Child from Romania)

- **Children display a significant tolerance for online risk, potentially resulting in an underestimation of dangers and an overestimation of their ability to manage them**. They often prioritise social benefits over safety, particularly when

[1] Down to Zero Alliance, (2022). Child safety by design that works against online sexual exploitation of children.

[2] Eurochild, Ecpat International, Terre des Hommes Netherlands, (2024). Speaking Up for Change: children's and caregivers' voices for safer online experiences.

sharing intimate content.[3] Some children perceive risks as inherent to social media usage. This tolerance may arise from desensitisation to online risks, normalisation of harm, knowledge gaps or age-related factors.

"*If you want to be safe online, you shouldn't be on social media!*" (VOICE, Girl from the Netherlands)

"Y*ou get used to random men who want to connect with you on social media*" (VOICE, Girl from Malta)

- **About three-quarters of children in the VOICE research believed they could manage online harms**, primarily by using platform-based support tools. However, they had reservations about their effectiveness. Limited alternatives left children dependent on instincts, increasing vulnerability to digital harm. Caregivers provided secondary support, underscoring the need for conversations about online safety.

The increasing trend of **children self-managing online risks** is concerning. While educating them is crucial, it does not exempt governments and online platforms from ensuring a safe digital environment through child-safety by design and safety measures.

II. Prevention recommendations: actionable steps for States, tech industry and online service providers to prevent child exploitation and abuse online

Practical recommendations can be proposed for States and online service providers to prevent OCSE.[4]

For States:

- Establish harmonised **legal obligations for all platforms** to ensure child safety online, including effective age verification and detection/removal of child sexual abuse material.
- Allocate **sufficient funding to enhance the capacity of law enforcement and judicial officials** in detecting and investigating online sexual exploitation cases, ensuring children's access to justice.
- Mandate the adoption of **child-informed safe-by-design** approaches across all platforms.
- **Embed children's rights in digital policies**, with their active participation in implementation and review processes.
- Invest in **mental health support** for children affected by online interactions, including training for social workers, health professionals and law enforcement

[3] Down to Zero Alliance, (2022). Child safety by design that works against online sexual exploitation of children, p. 8.

[4] These recommendations are further highlighted in two Terre des Hommes Netherlands research: the VOICE research and the Child Safety by Design report.

officials to ensure a prompt, comprehensive and trauma-informed response to prevent the re-traumatisation of children.

- Expand **online safety education** in schools, considering children's diverse needs, cultural background and social contexts. Curriculum should cover prevention of online sexual violence, including harmful sexual behaviours among children.

  "*At school, they don't give us much information about how to use social media, [...] about who we should go [to] if we are victims of cyberbullying or [when] strangers write to us*." (VOICE research, Child from Bolivia)

- Implement ongoing **assessment of online risks** and resilience to harm through dialogue with children and risk assessments by online platforms.
- Foster **whole-of-government engagement,** which entails cooperation and coordination among different parts of government, for effective implementation from national to local level.
- Establish **multi-stakeholder collaboration** mechanisms involving civil society, academia and private sector to drive innovative solutions for children's online safety.

For online services providers:

- **Assess and mitigate risks** faced by children on their platforms.
- Establish **secure digital environments** ensuring the protection of children's personal data, including their images, videos and personal information from being misused.
- Implement **safety-by-design** approaches with accessible and child-friendly safety and privacy settings.

  "*We propose an application that only allows us to talk to known people and does not allow us to share photos with anyone*." (VOICE research, Children from Spain)

- **Engage children** in designing online services and safety features, offering multiple feedback opportunities.

  "*We should be included in designing a platform.*" (VOICE research, Children from Croatia)

  "*People of our age should participate in developing technology because some bad words are overlooked by older people*." (VOICE research, Children from the Netherlands)

- Offer comprehensive **information** and **transparency** about platform risks and safety measures, using child-friendly and age-appropriate language.
- Improve **caregiver support** with intergenerational educational videos or games to encourage open caregiver-child discussions.

III. Closing implementation gaps: addressing gaps in implementing laws and policies to protect children from online exploitation

Remaining gaps in effectively implementing and applying existing laws, policies, and guidelines to combat OSCE include:

- **A lack of awareness and a lack of effective reporting mechanisms.** Our partners flagged that children may lack awareness on how to recognise and report OCSE, resulting in underreporting of abuses (the Philippines, Cambodia).
- **The current child protection legislations are not adequately enforced**, leading to procedural and administrative challenges that discourage victims and survivors from pressing charges effectively.
- **There is a lack of capacity and knowledge among government and stakeholders regarding OCSE.** Our partners in the Philippines and Cambodia stressed their government's lack of capacity and expertise in addressing OCSE, citing deficiencies in resources, expertise and comprehension of online threats. They highlighted a pervasive culture of silence around OCSE, with many communities affected remaining silent.
- **Poverty and vulnerability exacerbate the situation**, serving as push factors. Our partner in the Philippines stressed that these factors drive Filipino families to exploit their children online and urged the adoption of targeted state social assistance programs to prevent further exploitation.
- **Social exclusion and discrimination based on gender and disability** (among other intersecting identity factors[5]) **contribute to OSCE and hinder reporting.** In the I-access MyRights project[6], participants noted heightened vulnerability among girls and children from disadvantaged backgrounds. Individuals with mental disabilities are also identified as subject to higher risks due to their isolation and susceptibility to manipulation.
- **There are remaining legal gaps in the EU legal framework,** particularly concerning online platforms. These include a lack of mandatory effective age verification mechanisms, of legal requirement for child safety by design and the absence of clear obligation for platforms to detect and remove CSAM and grooming content, given that only voluntary detections are authorised by the Interim Regulation.[7]

[5] For instance, in Nepal and the Philippines, governments prioritise LGBTQIA+ identifying children and address the risks they encounter online.

[6] Terre des Hommes Europe, I-access MyRights project.

[7] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse. The Interim Regulation allows for a period of three years for the continuing of voluntary detection of CSAM by internet service providers in the interest of protecting children from online child sexual exploitation.

IV. Law enforcement challenges: analysing obstacles law enforcement faces in tackling online child exploitation crimes

We have identified challenges hindering law enforcement agencies in effectively investigating, detecting, and combating CSAM and prosecuting offenders:

- **First**, the **high volume** of CSAM received. Law enforcement agencies are inundated with a very large volume of CSAM reports, leading to difficult decisions regarding investigation priorities due to resource constraints.[8]
- **Secondly**, law enforcement agencies, particularly in peri-urban and rural areas, face challenges in combating OSCE due to deficiencies in **technical capabilities, training and expertise**. Insufficient financial resources and staffing[9], along with inefficient IT systems for tackling CSAM and a lack of digital literacy, exacerbate these challenges. Additionally, the absence of mental health support for officials investigating online child sexual abuse cases contributes to high staff turnover rates, necessitating recurrent retraining efforts and demanding additional resources.
- **Thirdly**, law enforcement's ability to combat CSAM circulation is severely limited by the widespread adoption of **End-to-End Encryption** (hereafter "E2EE"), exemplified by Meta's recent decision to implement default E2EE across all personal communications on Messenger.[10] This reduction in intervention capacity poses significant concerns, jeopardising public safety and hindering law enforcement's ability to identify and report illegal activities effectively.[11]
- **Lastly**, the **transnational nature** of OCSE offences poses a significant challenge, as these crimes often cross national borders. Effective collaboration and coordination between enforcement agencies from different countries is essential. However, differing legal frameworks, jurisdictional complexities, and language barriers can impede effective cooperation.

V. Child support services challenges: obstacles child support services face in helping children who have undergone online sexual exploitation

Child support services face significant and various challenges in assisting children who have experienced OCSE.

[8] For instance, our partner in Kenya reported that the Kenyan law enforcement authorities received over 21.000 cases in 2023, yet only 17 resulted in court proceedings.

[9] However, when addressing the shortage of staff in law enforcement agencies, it's essential to consider the absence of mental health support for officials tasked with investigating cases of online child sexual abuse material. This lack of support may contribute to the high staff turnover rates observed in these agencies. The frequent turnover of staff necessitates recurrent retraining efforts, demanding additional resources each time.

[10] Meta, Launching Default End-to-End Encryption on Messenger, December 2023.

[11] Joint Declaration of the European Police Chiefs, p. 1.

One pressing issue is the **poor and inadequate capacity within child support services**, as highlighted by our partner in Bangladesh, due to insufficient resources and staff. Similarly, partners in the Philippines and Cambodia note limited awareness of inclusive practices among these services, hindering effective assistance to all affected children. Factors contributing to this **lack of inclusivity** include oversight of gender and gender identity differences, age-related challenges (lack of adolescent-friendly services[12]), and disability consideration. This capacity shortfall in child support services increases the risk of re-victimisation for child victims in the future. Compounding this, the absence of government-provided training leaves many child support services reliant on NGO training, which may not fully address the complexities of OCSE cases.

Child support services sometimes operate under the false assumption, stemming from a lack of training, that OCSE is somehow "less" harmful than its in-person counterpart. This misunderstanding underscores a broader issue: **the failure to recognise the severity and impact of OCSE**. Additionally, they may not acknowledge that online and offline exploitation exist on a continuum, blurring the lines between virtual and physical harm.

The limited accessibility of support services poses another challenge, particularly for vulnerable children who may hesitate to seek help due to fear or distrust. This reluctances underscores the importance of enhancing outreach efforts and tailoring approaches to meet the needs of each child affected by online sexual exploitation.

VI. Mitigating risks: exploring technical and regulatory measures to mitigate risks associated with online child exploitation and abuse

Technical measures:

Our partners in the Philippines, Bangladesh, and Cambodia identified technical measures like hotlines for reporting OCSE. However, these hotlines are **not exclusively dedicated to OCSE** and suffer from **insufficient training and awareness** among staff on what constitutes OCSE. This leads to potential mis-categorisation of cases. Our partners also noted a general lack of public awareness about the availability of hotlines. Addressing OCSE cases is time-consuming and requires coordination with multiple support services, posing further challenges.

Regulatory measures:

Child safety by design should be implemented as a legal requirement, emphasising a user-centred approach that prioritises user safety and rights in service and product

[12] Adolescents are frequently criticised rather than assisted for behaviours seen as risky or delinquent, which diminishes the likelihood of them reporting such incidents.

design.[13] Current EU legislation lacks comprehensive safety provisions, despite incorporating some elements of safety by design, such as transparent reporting mechanisms and parental control systems.[14] Yet, these measures have **limitations in their scope and effectiveness**, frequently placing the onus of reporting on children and heavily leaning on parental control. Findings from the VOICE research reveal the **inadequate preparedness of both children and caregivers** to report and ensure online safety respectively. In light of this, it is imperative to recognise that children and caregivers cannot shoulder the entire responsibility for ensuring online safety, underscoring the urgent need for regulatory interventions.

VII. Best practice sharing: showcasing effective strategies and procedures to safeguard children online

As highlighted in the VOICE research, a best practice is to prioritise the **direct involvement of children in decision-making process and policy development**. The implementation of digital nudging by online service providers, which consist in guiding user behaviours through warnings, design and information without restricting their freedom of choice[15] is also recognised as a good practice. However, such approaches (e.g. nudging) must be combined with additional approaches, such as adequate age verification, CSAM/grooming detection, adequate moderation, child-friendly reporting mechanisms, high privacy by default, etc. Addressing the issue requires a toolbox of solutions, as there is no one size fits all easy solution.

Our partners stressed the importance of developing **child safeguarding policies** and **increasing awareness of hotlines** for reporting abuse. They also mentioned, as a good practice, the implementation in schools of online safety programmes and the involvement of various stakeholders, such as LGBTQIA+ rights groups and OCSE technical working groups to effectively address the multifaceted challenges of child online protection.

VIII. AI and encryption challenges: identifying challenges and solution in dealing with AI and encryption's role in child exploitation and abuse

On generative AI:

Children in the VOICE study expressed concern about offenders using generative AI tools. They fear their pictures or videos could be manipulated by AI for sexual purposes or

[13] Down to Zero Alliance, (2022). Child safety by design that works against online sexual exploitation of children, p. 9.
[14] See Directive 2010/13/EU on audiovisual media services (Audiovisual Media Services Directive).
[15] For example, Apple recently launched their Communication Safety system as part of this approach.

exploitation.[16]

"*I am concerned my photos and videos [are] being used for pornographic purposes, [or] exploitation*" (VOICE, Child from Thailand)

Through informal discussions with stakeholders, law enforcement agencies expressed already having encountered instances of CSAM generated by AI. This trend is highlighted in the latest annual report from the Internet Watch Foundation.[17] In 2023, IWF investigated its first reports of CSAM generated by AI, and **no less than 51 URLs[18] processed contained actionable AI-generated images of child sexual abuse**, most of which looked like 'real' images. Recent research led by Protect Children[19] warns about how AI is used to dehumanise and exploit children's images, perpetuating a culture of violence.

About Generative AI, our partners in the Philippines highlighted that their Government had limited understanding of what AI was. While the Philippine Council for the Welfare of Children cautioned parents against sharing unnecessary photos of children online[20], the **predominant focus remains on parents**. AI companies should take proactive measures to prevent the misuse of their tools, while platforms should implement safeguards against the misuse of imagery depicting children. To mitigate this excessive burden on parents, the Philippine National Police (PNP) has initiated efforts to develop tools for detecting and combating AI-generated CSAM, as outlined in a recent press briefing.[21]

On End-to-End Encryption (E2EE):

Recent research led by Protect Children[22] shows that E2EE messaging apps are used to search for, view and share CSAM, Telegram being by far the most popular messaging app mentioned, followed by WhatsApp. Protect Children highlights that these messaging apps are often favoured by offenders due to the security and privacy offered by E2EE, which allows them to commit crimes without fear of detection or law enforcement presence.

In the same survey, Protect children shows that ⅓ of respondents admitted actively using mainstream media platforms to access and share CSAM, alongside their dark web activities.[23] The research further highlights that there is a clear overlap between social media platforms most used for viewing and sharing CSAM and the platforms most popular

[16] Eurochild, Ecpat International, Terre des Hommes Netherlands, (2024). Speaking Up for Change: children's and caregivers' voices for safer online experiences, p. 28.
[17] Internet Watch Foundation. Annual Report 2023.
[18] These URLs figures do not reflect AI generated child sexual abuse images posted on a dark web forum. For a full overview, see Internet Watch Foundation, "How AI is being abused to create child sexual abuse imagery".
[19] Protect Children, "Tech Platforms Used by Online Child Sexual Abuse Offenders", February 2024, p. 13
[20] C. Chi, "Parents urged to avoid posting 'unnecessary' photos of children due to AI misuse", 7th February 2024.
[21] Presidential Communication Office, "PNP braces against use of AI-generated child exploitation materials in PH", 25th April 2024.
[22] Protect Children, "Tech Platforms Used by Online Child Sexual Abuse Offenders", February 2024.
[23] Instagram emerges as the most used platform for searching, viewing and sharing CSAM, followed by X (Twitter), Discord, Facebook and TikTok.

among children and young people.[24] According to the findings of the VOICE research, which involved children from 15 different countries, the top platforms among them are Snapchat (25%), TikTok (18.5%), and Instagram (14%).[25] Regarding the specific cases involving online sexual interaction where a child believed they were communicating with an adult, 15% of these interactions occurred on Snapchat, followed by 13% on Instagram, 11% on WhatsApp, 10% on Facebook, and another 10% on Messenger.[26]

Analysing NCMEC volume of reports[27] submitted by online service providers exposes a notable contrast between those employing E2EE, such as WhatsApp, and those that do not, like Facebook and Instagram (prior to Meta's encryption decision[28]). In 2023, WhatsApp reported 1,389,618 instances, whereas Facebook and Instagram reported 17,838,422 and 11,430,007, respectively.

Online service providers must take **measures to combat CSAM even if using E2EE**. In the EU, there are ongoing debates regarding the exclusion of E2EE services from CSAM detection efforts, a position we find deeply concerning. Services using E2EE must actively engage in efforts to eliminate CSAM and ensure the protection of children online, using privacy-preserving detection tools and other measures.

IX. Stakeholder engagement: highlighting proactive approaches to engage stakeholders in combating online child exploitation and abuse

To effectively combat OCSE, proactive stakeholder engagement is essential. Proactive measures should be implemented to facilitate consultation and participation across a broad spectrum of stakeholders:

- **Development of proactive networks** was suggested by our partner in Bangladesh, which mentioned the Bangladesh Shishu Adhikar Forum[29] (BSAF) as a nationwide movement for rights of the child in Bangladesh. Further networks should be developed.
- **Include diverse stakeholders in legislative developments,** including children and child-rights organisations. The SCROL project[30] implemented by Terre des Hommes Netherlands can serve as an example, as the project engages States and the private sector.

[24] Protect Children, "Tech Platforms Used by Online Child Sexual Abuse Offenders", February 2024, p. 11.

[25] During the Focus Group Discussion, children participating in the VOICE research were asked what was their most used app or social media. For further methodology details, see Eurochild, Ecpat International, Terre des Hommes Netherlands, (2024). Speaking Up for Change: children's and caregivers' voices for safer online experiences, p. 16 and following.

[26] Thorn (2021) Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking.

[27] NCMEC, 2023 CyberTipline Reports by Electronic Service Providers.

[28] Meta, Launching Default End-to-End Encryption on Messenger, December 2023.

[29] For further information, see BSAF website.

[30] Terre des Hommes Netherlands, Safety for Children and their Rights OnLine (SCROL).

- **National action plans**, **which outline strategies for prevention, intervention and prosecution should be adopted.** These plans should incorporate budget allocations for their implementation, along accountability mechanisms to ensure their effective execution.
- **Funding should be increased to enhance the** capacity of stakeholders involved in combating OCSE. This can include funding training or research.
- **Institutionalise and allocate resources to multi-stakeholder mechanisms** aimed at enhancing accountability and fostering innovative systemic change approaches.

X. International collaboration mechanisms: discussing strategies for global collaboration to tackle digital threats to children

Given the global and borderless nature of online crimes, such efforts should be led by international organisations, particularly the UN, to ensure **harmonisation and mainstreaming across domestic and regional initiatives**. Regional initiatives, such as SAIEVAC[31] (South Asian initiative to end violence against children) or the European Better internet for kids initiative[32], can serve as models for coordinated action. **Collaboration between civil society members** is also essential for sharing expertise, resources and best practices. Additionally, **cross-learning from regions** that have already implemented effective laws and regulations, such as Australia[33] and the United Kingdom[34], is essential.

Terre des Hommes International Federation is dedicated to preventing online violence against children and ensuring their well-being. We advocate for child rights, protect them from harm, and influence policies. For more information, contact Nathalie Meurens, EU Advocacy Officer on Child Sexual Exploitation and Abuse, at n.meurens@tdh.nl.

[31] Mentioned by our partner in Bangladesh. For further information, see SAIEVAC website.
[32] For further information, see Better Internet for Kids website.
[33] Australian Federal Register of Legislation, Online safety Act 2021.
[34] UK Parliament, Online Safety Bill 2023.