Position Paper on the proposed EU legislation on the detection, removal and reporting of child sexual abuse online and the establishment of an EU Centre

Key positions

1. The EU legislation should cover all illegal harmful content against children, not just child sexual abuse material (CSAM). At the minimum, it should comprehensively cover grooming, self-generated material, sextorsion and online child sexual exploitation.
2. All forms of abuse and exploitation as well as all means and services used for abuse and exploitation must be prioritised; not doing so will result in the flux of criminal material to shift from one service to another (wave effect).
3. The EU legislation should adopt safety by design requirements, which are recognised to be more effective and privacy compliant in addition to work in end-to-end encryption services.
4. Future proof and victim-centric EU legislation should place the rights, needs and concerns of child victims at the heart of its obligation, while being technology neutral.
5. Self-regulation means no regulation, where each company creates a different solution in a non-transparent manner, with its own bias and loopholes.
6. Mandatory reporting must accompany detection and removal to ensure that victims are identified and supported.
7. The EU Centre should be empowered with a strong mandate and capabilities to drive innovation, especially for preventative technologies, and prevention initiatives.

1. Cover all illegal harmful content against children, not just CSAM

The open public consultation (OPC) and the inception impact assessment suggest a strong focus on tackling child sexual abuse material (CSAM) and to a lesser extent on grooming. We recommend the explicit inclusion of other forms of child sexual exploitation (CSE) include live streaming, self-generated material, sextortion, non-consensual sexting, child sexual exploitation material and other forms of online child sexual exploitation e.g. through sex advertisement websites where children are offered for sexual services by third parties via sex work classified ads. A focus solely on CSAM will strongly limit efforts to eradicate all forms of online child sexual abuse and exploitation and available solutions.

First, the line between online CSAM and CSE can often be blurred. Material that sexualises and is exploitative to children without explicit abuse are often used for abusive purposes and can be part of a series that includes CSAM. CSAM, grooming and the various forms of CSE are interconnected, various forms of CSE may lead to or be carried along CSAM; both requiring urgent and coordinated efforts at EU level.

Second, it is commonly understood that different (online and offline) manifestations of sexual abuse and exploitation can be addressed through connected or similar approaches. Limiting the focus of the regulation to child sexual abuse will therefore be a missed opportunity for a comprehensive and efficient approach against all child sexual abuse and exploitation online and offline. Online CSAM and CSE are the result or the preparatory steps to offline abuse and exploitation.

Lastly, we recommend that the legislation has a sufficiently broad scope to cover new future forms of producing, sharing and obtaining CSAM and CSE online. This should entail adopting EU definition for child sexual exploitation material, grooming, sextorsion, live streamed child sexual exploitation and abuse, self-generated material, sextortion, non-consensual sexting and other forms of illegal harmful content and acts against children online.

2. All forms and means of abuse and exploitation must be equally prioritised

Several questions of the OPC imply that some prioritisation may be made in tackling child sexual abuse and exploitation, in terms of means of distribution, types of material, challenge to address, service provider or regulatory approach.

The questions asking to prioritise are problematic in that they fail to understand the interconnectedness of online child abuse and exploitation and its evolving nature. Distribution platforms evolve depending on the form of CSAM (sextorsion and grooming may be via apps or gaming platforms for instance, exchange of CSAM between ‘experienced’ abusers may be done more through the dark net, etc.). As technology constantly evolves and new apps or platforms enter the market, the distribution means and channels are continually evolving. If the regulation focuses on one platform/darkweb, the distribution will shift to where it is not controlled. The legislation will consistently be out of date. The legislation must be future technology development proof.

As mentioned above, the implicit prioritisation of CSAM is deeply problematic. Grooming and online child sexual exploitation are widespread and must be tackled by EU legislation. Moreover, EU based offenders have been known to pay for and direct in real-time the sexual abuse and exploitaiton of children through live streaming, often leaving minimal digital evidence in the form of photos or recorded videos

In addition, prioritising brings ethical and child safeguarding considerations. No form and means of distribution of abuse and exploitation should be tolerated; all must be regulated.

3. Safety by design rather than solely detect and remove

From the OPC questionnaire, the focus appears to be on detecting and removing CSAM rather than requiring service providers to build safety by design services that would prevent online child sexual abuse and exploitation to occur in the first place. A safety by design approach would require service providers to implement more effective age verification systems and, in addition to remove and report methods, use less privacy invasive preventative ('warn and suppress'[1]) methods empowering users by signalling potential risks of child abuse or exploitation.

In order to shift to safety by design approach, the EU legislation should specify service providers providing one-way or two-way data transfer and/or data storage should detect, warn users, remove, and report child sexual abuse and exploitation. This obligation should apply to all companies that have "communications", "data streaming", or "data storage" systems as part of their core business. This should include all media: video, image, audio, text (including metadata).

In addition to being more effective, a safety by design approach using 'warn and suppress' preventative methods can bypass encryption and be more privacy compliant. End-to-end encryption is becoming an industry standard and being deployed on many services. The EU legislation must ensure that its legal obligations apply to encrypted environments or provide specific obligations and safeguards for encrypted services. This includes ensuring device manufacturers enable on-device detection and blocking/disruption by ensuring safe by design when building their devices.

EU legislation should focus on preventative measures to 1) preventing CSAM and CSE from being produced, i.e. on device AI solutions and 2) preventing CSAM and CSE from being uploaded to platforms in the first instance, i.e. using solutions to detect, warn and, in some cases block, CSAM and CSE at the uploading stage, instead of focusing on dealing on the consequences and the harm to children has already been done.

4. Future proof and victim-centric legislation

A victim-centric approach and the best interests of the child as a primary consideration should never be optional and should be reflected throughout the legislation. A victim-centric approach in law places the rights, needs and concerns of child victims at the heart of its interventions. The legislative proposal should be analysed from the child victims' perspective and ensure that risk management and preventative measures are built through the legal requirements.

[1] See Page 26 Figure 4.2 - Prevention: https://respect.international/wp-content/uploads/2019/11/AI-Combating-online-sexual-abuse-of-children-Bracket-Foundation-2019.pdf . Automated on-device/in-browser methods make it possible to warn users or suppress distribution of content, even in an encrypted environment, without external access to the content.

We endorse EU requirements addressing online child sexual abuse and exploitation irrespective of the means, distribution method, environment or location in which it occurs. Technology continuously evolves with new apps or platforms entering the market and the popularity of those constantly evolving, the distribution means and channels are continually changing. If the regulation focuses on one platform or one layer of the web (i.e. darkweb), the distribution will shift to where it is not controlled. The legislation will consistently be out of date. The legislation must be future technology development proof.

5. Self-regulation is no regulation

Voluntary methods are proven insufficient in addressing online child sexual abuse and exploitation and they will not result in a significant change.

While some internet service providers have embraced them, voluntary measures are arbitrary, most of them proprietary and non-transparent. In addition, they are inconsistently applied. Voluntary measures mean that companies create their own systems to detect and block, each with their own failing, biases, suppression of legitimate content, and loopholes.

Legal requirements not only establish standards applicable across the industry, they will also drive companies to create common solutions. The EU should be a major driver in the development of technical solutions to ensure children are safe, their data kept private and fairness respected. In addition, EU regulation can support further transparency in the industry.

6. Mandatory reporting must accompany detection and removal

Mandatory detection and removal should be combined with mandatory reporting. Reporting is essential for monitoring criminal acts as well as for feeding into the proposed hash list database to be established by the EU Centre and continuing to detect and remove known CSAM. More importantly, reporting is crucial for victims to be identified and supported. Detection and removal is not sufficient in itself.

In combination with strong preventative measures, stringent mandatory reporting, detection and removal of new and known CSAM, grooming and child sexual exploitation should apply to problematic service providers such as adult content websites, big platforms and services with a high number of users and high number of users under 18.

Effective sanctions must accompany the legal requirements to report, detect and remove in order for the obligations to be meaningful.

7. EU Centre with a strong mandate and capabilities to drive prevention and innovation

Child sexual abuse and exploitation require multiple approaches and multi-stakeholder interventions to adequately fight it. The EU Centre should thus be empowered to:

A. Monitor the implementation of EU policies through a review process of the transparency reports combined with independent implementation assessments.

B. Monitor trends in child sexual abuse and exploitation.

C. Issue opinions and guidelines on the implementation of EU policies and on best practices.

D. Enforce through administrative measures in case of issues of compliance in the detection, reporting and takedown, as well as in relation to the transparency reporting.

E. Coordinate multi-stakeholder and multidisciplinary efforts preventing and tackling online child sexual abuse and exploitation, as well as identify which country and region7 require strengthened capacities and knowledge.

F. Facilitate cooperation between law enforcement authorities, (INHOPE) hotlines, service providers, children's rights organisations, data protection authorities and the EU, building on their expertise and creating synergies.

G. Drive the development of innovative preventative solutions through knowledge-sharing, research and funding.

This paper represents the positions of the following children's rights organisations:

Terre des Hommes Netherlands + Het Centrum tegen Kinderhandel en Mensenhandel + International Justice Mission + Defence for Children-ECPAT Netherlands

For more information, contact n.meurens@tdh.nl