Call for input: Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

By email to: hrc-sr-saleofchildren@un.org

About Netsafe

1. Netsafe is New Zealand's independent, non-profit online safety charity adjacent to government and law enforcement. Netsafe provides free support, advice and education seven days a week through a helpline, our website and face to face service delivery across New Zealand.

2. Netsafe is also the Approved Agency under New Zealand's Harmful Digital Communications Act 2015 (HDCA). One of the purposes of the HDCA is to deter, prevent, and mitigate harm caused to individuals by digital communications. Netsafe's functions as the Approved Agency are set out in section 8 of the HDCA. Those functions include:
    (a) to receive and assess complaints about harm caused to individuals by digital communications;
    (b) to investigate complaints;
    (c) to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints;
    (d) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of the Act; and
    (e) to provide education and advice on policies for online safety and conduct on the Internet.

3. In addition, Netsafe sits on Facebook's Global Safety Advisory Board, is an observer to the Global Online Safety Regulators Network and has relationships and memberships of a number of other organisations such as We Protect Global Alliance. Netsafe's Chief Online Safety Officer is also the interim President of Inhope.

4. Netsafe's comments are focused on our experiences dealing with online harms as both a not-for-profit agency and as the Approved Agency under the HDCA. Some of the recommendations are drawn from the Aotearoa Code of Practice on Online Safety and Harms[1] or from other expert recommendations which we endorse. We address only those questions or issues where we think we can add any value.

[1] https://thecode.org.nz/wp-content/uploads/sites/38/2023/06/THE-CODE-DOCUMENT-FINAL.pdf

Please provide information on how technologies are used to facilitate the sexual exploitation and abuse of children.

1. Netsafe has received reports and complaints or is otherwise aware of the following:
    a. Online grooming via social media, messaging apps, and online gaming platforms (including in app and in game messaging systems) to establish relationships with children: Perpetrators often pose as peers or authority figures to gain trust. Using fake profile pictures and other information, perpetrators strike up conversations, gain the trust of the child and then manipulate the child into sharing explicit images or engaging in sexual activities online. Images may be shared onwards or used to blackmail the child or young person to provide money or further images (sextortion).
    b. Deepfake apps/technology: apps and filters can "undress" or "nudify" a victim on the basis of a simple profile pic or otherwise harmless pictures shared on social media. Such images are then used to blackmail the child (sextortion), or otherwise used to bully or harass the victim such as in school or other peer settings.
    c. Live streaming: Perpetrators may use live streaming platforms to record or broadcast the sexual abuse of children in real-time. For example, children may be coerced, tricked or deceived into engaging in sexual acts via webcam through online grooming methods mentioned above.
    d. Virtual flashing or the sending of other objectionable or illegal material using anonymous communications technology such as Airdrop may include child recipients whether intentionally or recklessly.
    e. Possession and distribution of child sexual abuse material (CSAM) relies on encrypted storage and messaging technologies.

What practical recommendations would you propose for States, the technology industry and online service providers to prevent the sexual exploitation and abuse of children in the digital environment?

5. States should:
    a. enact and enforce comprehensive laws that criminalise child sexual exploitation both offline and online;
    b. allocate resources for specialised law enforcement units trained in investigating and prosecuting online crimes against children;
    c. collaborate with international partners to address cross-border issues and enhance information sharing, including agreeing on standard classification/taxonomies to ensure like-for-like comparisons;
    d. provide education and awareness campaigns to inform parents, educators, and children about online safety and the signs of grooming or exploitation;
    e. support victim-centered approaches, including access and funding for counselling, legal assistance, and other support services;
    f. make reporting to authorities or independent agencies as easy as possible.

6. The technology industry and online service providers should in addition to developing and implementing robust content moderation policies and technologies to detect and remove CSAM from online platforms:

a. incorporate default privacy settings that protect children as standard such as making follower lists private by default, and otherwise make privacy settings easy to use and regularly remind users to check/amend/update if necessary;
b. sign up to https://stopncii.org and https://takeitdown.ncmec.org;
c. incorporate filtering and pixelation technology as standard for suspected child nude images;
d. stop allowing sextortionists to use the same images and profile pictures across multiple profiles;
e. give content moderators appropriate tools to better identify sextortion or grooming accounts;
f. invest in moderation and hire more humans (rather than rely on AI) to undertake proper investigations;
g. invest in research and development of advanced tools and technologies to identify and combat online child exploitation;
h. provide transparency reports detailing efforts to combat online child exploitation and make more relevant data available for research;
i. support initiatives that promote digital literacy and online safety for users of all ages;
j. implement appropriate age verification mechanisms to prevent children from accessing age-inappropriate content or services;
k. facilitate easy reporting mechanisms for users to flag suspicious or abusive content, and respond promptly to such reports;
l. collaborate with industry peers, law enforcement, and non-governmental organisations to develop best practices and share information on emerging threats;
m. provide resources and support for victims of online exploitation, including helplines and referral services.

What are the remaining gaps that limit the effective implementation and application of existing laws, policies and guidelines to prevent, detect, report and protect children from sexual exploitation and sexual abuse online?

7. Jurisdictional challenges and disjointed approaches within and across borders: the borderless nature of the internet makes it difficult to enforce laws and regulations across jurisdictions. Perpetrators may choose to operate from jurisdictions with weak legal frameworks or from jurisdictions that lack extradition agreements, hindering efforts to investigate and prosecute offences. Similarly, laws, policies and practices related to online child sexual exploitation vary between countries, creating inconsistencies in how offences are defined, investigated, and prosecuted. Encouraging harmonisation or minimum standard between jurisdictions would help to address inconsistencies and improve international cooperation.

8. Technological advancements: perpetrators adopt, adapt to and rely on technological advancements, making it challenging for law enforcement agencies and online platforms to keep pace. End to end encryption in particular poses challenges for detecting online child exploitation. Similarly, disappearing message technology may result in the inability to detect and successfully prosecute perpetrators.

9. Education and awareness gaps: many children, parents, educators, and caregivers lack the knowledge and skills needed to navigate the digital world safely. Comprehensive education and awareness campaigns are needed to empower individuals to recognise and respond to online

threats effectively, including how to use the day to day technology, and apps they rely on to communicate.

10. The large global tech platforms/actors often do not have an effective local presence in each jurisdiction in which they provide their platforms or services making information and localised data sharing, cooperation and/or enforcement ineffective or impossible.

What are the challenges that exist in the use of these digital technologies, products or services, that inhibit the work of law enforcement across jurisdictions in their work to investigate, detect, remove child sexual abuse materials online and prosecute these crimes?

11. Legal barriers and jurisdictional complexity: variations in laws and regulations between jurisdictions create barriers to investigating and prosecuting. Mutual legal assistance treaties and other international cooperation mechanisms may be slow, delaying the exchange of vital evidence and information. Coordinating investigations across different legal systems, languages, and cultural contexts presents significant challenges for law enforcement agencies.

12. Encryption and anonymity: encryption and anonymisation technology makes it difficult for law enforcement to track and trace perpetrators and/or gather sufficient evidence for successful prosecution.

13. Volume of data: the sheer volume of data generated and shared on the internet presents a significant challenge. Sorting through massive amounts of digital content to identify and prioritise potential instances of CSAM requires substantial time, resources, and computational power.

14. Advances in technology: rapid advancements in technology present an ongoing challenge. Perpetrators exploit emerging technologies to evade detection and prosecution.

15. Resource constraints: law enforcement agencies may face resource constraints, including limited funding, staffing shortages, and outdated technology infrastructure or expertise.

What technical and regulatory measures can be put in place by States, the technology industry and online service providers (legislative, regulatory, administrative, institutional and others) towards mitigating human rights risks associated of online child sexual exploitation and abuse, and ensuring the minimum harmonization across legal jurisdictions?

16. Legal frameworks should incorporate human rights, including the right to privacy, freedom of expression, and the best interests of the child, while also providing necessary safeguards to protect children from harm. However, rights to privacy and freedom of expression should not trump a child's right not to be exploited or abused.

17. States should establish mechanisms for transparency and accountability including regular reporting on efforts to combat online child sexual exploitation and abuse, as well as mechanisms for independent oversight and evaluation of these efforts.

Are there any other practical examples of internal monitoring, complaint and reporting processes; establishment of regulatory bodies and interventions; remedial pathways; robust safeguarding procedures; children's rights' due diligence and risk assessments; and technical standard-setting processes to ensure safety and inclusivity by design?

18. Independent organisations separate from Government may provide a better or more appropriate mechanism to encourage the reporting of CSAM and online child sexual exploitation. Reporters may lack trust in government or official institutions and may therefore be reticent in disclosing exploitation or abuse or may fear criminal prosecution or other action in cases where they have shared their own underage explicit images. In Netsafe's experience, making the reporting process as easy as possible, allowing anonymous reporting or optional demographic or identity information to be provided encourages reporting.

What kind of mechanism could be put in place to best support and coordinate the joint public and private industry participation at the international level on existing and emerging threats that digital technologies pose to children in order to ensure harmonisation and mainstreaming across domestic and regional efforts when combatting this phenomenon?

19. International task forces and working groups, including multi-stakeholder dialogues and summits: Establishing international task forces and working groups comprising representatives from governments, law enforcement agencies, technology industry stakeholders and civil society organisations would facilitate collaboration and information sharing. Such a mechanism could draft best practice guidelines and model laws for example. Netsafe is already an observer to the Global Online Safety Regulators Network and benefits from information sharing that Network offers.

20. Standardised reporting mechanisms: Developing standardised reporting mechanisms, including standardised classification and taxonomies for online child sexual exploitation incidents can streamline the process of reporting and responding to offences across jurisdictions.

21. Global awareness and education campaigns: Launching and funding global and/or targeted awareness campaigns to educate children, parents/caregivers, and educators about online safety and the risks of digital technologies is vital.

Thank you for the opportunity to provide input.

Netsafe

15 May 2024