CRIN CHILD RIGHTS INTERNATIONAL NETWORK

CRIN's submission for the report of the Special Rapporteur on the sale and sexual exploitation of children

This submission is made on behalf of the Child Rights International Network - CRIN (www.crin.org), May 2024.

1. CRIN is a human rights organisation focused on children's rights. Our approach is grounded in the UN Convention on the Rights of the Child. We work on the full range of children's rights, including the protection of children from sexual violence[1] and children's rights in the digital environment.[2]

2. This submission focuses on the existing and emerging sexually exploitative practices and abuse against children in the context of Artificial Intelligence (AI) and end-to-end encryption (E2EE). It draws in particular on our report *Privacy and Protection: A children's rights approach to encryption*,[3] which was informed by conversations with a wide range of stakeholders, including child protection, children's rights, digital rights, privacy and data protection, Internet regulation and the technology industry.

Challenges posed by AI and E2EE to children's protection from sexual violence

3. It is undeniable that AI and E2EE pose challenges to the protection of children from sexual abuse and exploitation.

4. AI can be used by perpetrators to adapt original child sexual abuse images or videos into new material, manipulate non-abusive content of children into abusive material, or create fully AI-generated child sexual abuse material. AI can also be used to create abusive content at scale, significantly increasing the volume of child sexual abuse material in circulation and making victim identification more difficult. Offenders can use AI to generate information on how to perpetrate abuse, as well as how to avoid prosecution by coercing the victims and tampering with evidence.[4]

5. E2EE, too, can facilitate sexual violence against children. Encrypted channels make it easier for perpetrators to access and disseminate child sexual abuse material online undetected. With regard to communications between perpetrators and children in the case of grooming, by keeping these exchanges private, encryption makes it more difficult to investigate and prosecute abuse. Encrypted platforms can also be used by child traffickers to facilitate the abduction, sale and trafficking of children.[5]

A children's rights approach

6. The evident challenges posed by AI and E2EE to the protection of children from sexual abuse and exploitation have led to a polarised discourse which is led by the

[1] https://home.crin.org/issues/sexual-violence

[2] https://home.crin.org/issues/digital-rights

[3] https://home.crin.org/readlistenwatch/stories/privacy-and-protection

[4] https://www.thorn.org/blog/generative-ai-principles/

[5] https://home.crin.org/readlistenwatch/stories/privacy-and-protection

Anglo-/Euro-spheres and which can obscure the full complexity of the issue. A divide has emerged regarding children's rights online between, on the one hand, approaches focused on child protection from sexual violence, and on the other hand, approaches focused on privacy, freedom of expression or digital rights more broadly. The emphasis in the debate has in some ways become framed around "privacy versus protection".

7. It is essential that a children's rights-respecting response addresses all of children's rights in this context and understands those rights as indivisible and interdependent. The applications of technologies such as AI and E2EE engage nearly all children's rights (protection from violence, privacy, free expression, non-discrimination, the right to life, the right to health etc.). The uses of AI and E2EE pose both risks and benefits to the rights set out in the UN Convention on the Rights of the Child, including the rights to protection from sexual violence and exploitation.

Opportunities created by AI and E2EE for children's protection from sexual violence

8. With regard to AI, it has been recognised that it presents "enormous opportunities to help tackle the threat of online child sexual abuse", and that it can "transform and enhance the ability of industry and law enforcement to detect child sexual abuse".[6]

9. Our report *Privacy and Protection* has centred on encryption. We have highlighted that encrypted services can protect children from being targeted for violence based on information they send or receive, especially where they are part of disadvantaged or marginalised groups. Access to children's personal data can make them vulnerable to grooming and exploitation, but encryption helps to keep the data secure. Children who are sexually abused or exploited, as well as trafficked children, can communicate securely through encrypted channels in order to ask for help, store or send evidence.[7]

Recommendations

10. Regarding AI, experts have proposed safety by design principles that can be used to prevent and mitigate the risks of child sexual abuse and exploitation.[8] A number of major industry actors have committed to these principles. We reproduce a simplified version below:

- At the development stage:
    - The datasets that are used for training AI models should be sourced responsibly and should be safeguarded from child sexual abuse and exploitation material.
    - AI models should be stress-tested for their ability to produce abusive material.
    - Content provenance solutions should be used to reliably identify whether content is AI-generated.

- At the deployment stage:

[6] https://www.gov.uk/government/publications/tackling-child-sexual-abuse-in-the-age-of-artificial-intelligence/joint-statement-tackling-child-sexual-abuse-in-the-age-of-artificial-intelligence

[7] https://home.crin.org/readlistenwatch/stories/privacy-and-protection

[8] https://www.thorn.org/blog/generative-ai-principles/

    - AI products and services should be safeguarded from abusive content and conduct, including by the incorporation of user reporting.
    - AI models should be responsibly hosted.
    - Developer creativity should be encouraged alongside a culture of ownership and responsibility.

- At the maintenance stage:
    - Services should be prevented from scaling access to tools which infringe children's rights, such as tools used to "nudify" content depicting children.
    - Investment should be made into research and technology development to address the misuse of AI for online child sexual abuse and exploitation.
    - Child sexual abuse and exploitation material, including material generated by AI, should be combatted.

11. With regard to encryption, it is essential to have a thorough understanding of the functioning of encryption and the roles it plays in the digital ecosystem for rights-respecting interventions. Encryption cannot be addressed in isolation as a child protection issue - but must be seen as part of the digital environment, which is itself a part of the wider societal ecosystem.

12. We have proposed 10 principles for an approach that respects the full range of children's rights, which we reproduce in full below:

Framing and Process

> 1. Actions affecting the digital environment must respect the full range of children's rights. All interventions that affect the digital environment in general, and actions that engage encryption in particular, must respect the full range of children's rights, from protection from violence to privacy and freedom of expression.
>
> - Privacy and protection: Discussions should move beyond the dichotomy "privacy versus protection". All those involved in decision-making processes should recognise that all children's rights, including privacy and protection, are universal, indivisible and interdependent. This means that these rights apply to all children everywhere. There is no set of rights which is more important than others - all rights are equally important. These rights also support each other, with the fulfilment of each being necessary for the realisation of others.
>
> - Child rights impact assessments: All interventions that have a significant impact on children must be based on child rights impact assessments. This should involve pre-legislative scrutiny that assesses the impact of any law reform proposal on the full range of children's rights. Where an independent body is responsible for regulation, that regulator must include sufficient child rights expertise. Businesses with a significant impact on children's rights in this context should also conduct children's rights impact assessments, act on the outcomes of those assessments, and report on their implementation.

2. Interventions engaging encryption must be seen within a wider ecosystem. No single law, policy or technological development can protect children online or secure their human rights more broadly. Encryption cannot be addressed in isolation, but only as part of a wider ecosystem with a range of actors that can meaningfully interact, each with its own role that it can effectively and legitimately play.

- Start with the societal problem: Encryption should not be the starting point in debates around societal problems affecting children. Instead, policy-makers should identify the policy goal to be achieved and consider the range of options, of a technological nature or otherwise, that could be implemented for this purpose. In assessing possible solutions, policymakers should consider the variety of actors interacting in the societal ecosystem, including governmental agencies, law enforcement, health services, social services, schools, care centres and other institutions.

- Beware of techno-solutionism: Policy-makers and other stakeholders should avoid relying on one-size-fits-all technological fixes. Decision making should be based on a thorough understanding of the complex technological landscape, including in particular the multiple roles that encryption and other technologies play. Policies should be grounded in the reasonable capability of technology as it is, not as might be hoped for.

- Support the complete child protection ecosystem: Child protection requires human trust and meaningful interaction across solid infrastructures for knowledge-sharing and intervention. To the extent that laws, policies and other initiatives already exist for the purpose of child protection, they should be fully implemented. There should be an emphasis on prevention and education, and appropriate funding should be provided to the wide range of services interacting in the ecosystem, from law enforcement and the justice system, to social services and victim support. Particular emphasis should be given to staff training, which should include, where appropriate, digital evidence management, analysis and practice, in order to promote the investigation and prosecution of the perpetrators of technology-enabled violence against children. Physical and mental health support services for child and adult victims and survivors of child sexual exploitation and abuse must be a priority. The need for a multidisciplinary approach to protection should be emphasised in order to break down barriers to cooperation between disciplines and professionals.

3. All those with relevant expertise must be involved. All professionals with relevant knowledge must be able to engage in discussions and decision-making regarding children and the digital environment, including on encryption. They must be able to do so on an equal footing and in an environment of mutual respect. Conversations must include specialists working on child protection, technology and Internet regulation, data protection and privacy, as well as participants with more generalist expertise in children's rights, human rights and digital rights. The views of civil society, academia, government, law enforcement and the business sector must be

taken into account. Particular efforts should be made to include those working outside currently dominant Anglo- and Euro-centric spaces.

- Language: There should be a recognition of the extreme sensitivity of aspects of the debate around encryption and children's rights, particularly as regards online child sexual exploitation and abuse. Those involved in discussions should exercise empathy and pay special attention to the framing and language used, as well as the expectations that are being created for victims and survivors of abuse.

- Data: Emphasis should be placed on the importance of accurate data, in particular about the scale of abuse and the accuracy of content-detection technologies. All participants to discussions should strive to fully explain the ways in which they use data in support of their arguments, in order to help disaggregate between the various causes of problems and move the debate on solutions forward.

4. Children and other directly affected communities must be heard and their views given due weight.

Children's right to have their voices heard and given due weight must be upheld in all decision-making processes which concern them. Other directly affected communities, such as the adult victims and survivors of child sexual exploitation and abuse or those disproportionately affected by policing, surveillance, intelligence gathering or other intrusive data practices, must also be meaningfully included in these processes. Assumptions should not be made about the outcomes these groups may want. Not all children or members of a community have the same experiences, views or concerns. Decision-making processes should therefore aim to include diverse voices.

5. Policy-makers engaging with encryption must address the impact beyond their own jurisdiction.

The digital environment is interconnected and regulation in one jurisdiction is very likely to cause ripple effects in others, or even globally. Policy-makers must work to understand these links, including by engaging in conversations with those working in different jurisdictions, especially where they are not part of the dominant Anglo- and Euro-centric debates.

Substance

6. There should be no generalised ban on encryption for children.

If encryption were removed from all services that children use, far from protecting them, this would leave them vulnerable to a wide range of exploitation and abuse. It is possible to regulate the applications of encryption, however this must be consistent with children's rights.

7. Interventions engaging encryption must be context-specific.

Measures should be tailored to the diverse experiences of children as full rights-holders, including children from disadvantaged and marginalised groups. Interventions must consider and address specific political, economic, social and cultural contexts and the varied ways in which children relate to the State, businesses, and their community and family.

- Real-world uses of the digital environment: Those involved in decision-making should promote a better understanding of the variety of real-world uses of the digital environment, including communications involving medical information, legitimate political organisation in repressive environments, or the routine reliance on particular platforms where there is limited accessibility to other services. More efforts should be made to include perspectives which are not necessarily consistent with the expectations of those within the Anglo- and Euro-centric contexts.

- The repurposing of technology: There should be a recognition that technologies for content detection in the digital environment can be repurposed. The nature of the content that needs to be identified is not technology-specific, but policy-specific. Tools used to detect illegal content, such as child sexual abuse material, could also be deployed to identify legitimate content and infringe the rights of those accessing it.

8. Measures engaging encryption must be legal, necessary and proportionate.

Interventions engaging encryption should respect the principles of legality, necessity and proportionality. These principles apply to the content of communications, but also to the collection, sharing and retention of metadata. Measures should be provided for by law and should be sufficiently clear and precise. They should be limited to achieving a legitimate policy goal and should be the least intrusive way of doing so. Interventions must be necessary and proportionate limitations on children's qualified rights such as privacy, therefore they must strive for a high degree of specificity, instead of applying indiscriminately.

9. Policy-making should address the role of business.

Regulation and policy should mandate more transparency around how platforms prevent and remedy violations of children's rights, including by requiring clear, accessible and child-friendly terms of service. Platforms should receive guidance on how to improve the design of services, especially user reporting for children. Businesses whose activities have a significant impact on children's rights should be encouraged to invest in researching, developing and sharing findings on new technologies, as well as in supporting the efforts of others working in this area.

- Reporting to authorities: Where businesses obtain knowledge of the existence on their services of illegal content such as child sexual abuse material or illegal activity such as violence against children, they should take action under their terms of service, and expeditiously report this to law enforcement or other appropriate authorities.

- Transparency: Companies should publish transparency reports regarding the scale of online child sexual exploitation and abuse on their services that comes to their knowledge, detailing the types of content and behaviour identified and the actions taken as a result. Efforts should be made to reach as much specificity as possible, disaggregating events into individual instances of abuse, analysing the prevalence of revictimisation through the sharing of identical or altered content, and indicating the context in which the events took place if relevant for ascertaining the intention of the users involved (e.g. consensual image sharing between children, or content shared in outrage).

10. Children must have access to justice.

Free, effective and child-friendly complaint mechanisms, both judicial and nonjudicial, must be in place to ensure that children are able to access remedies, in a timely manner, for all violations of their full range of rights in the digital environment. There must be independent oversight mechanisms to ensure the lawful and rights-respecting implementation of measures engaging encryption.

- User reporting: Confidential, safe and child-friendly user reporting tools should be made available to ensure that children are able to report material and behaviour on services they use, and seek action. “Trusted flagger” mechanisms should also be considered. The decision following user reporting should be made in a timely manner, and it should be based on a clear and transparent process, giving users the possibility to resort to appeal mechanisms. Transparency reports should be produced to enable the scrutiny of systemic policy and practice around user reporting, while protecting the rights of users, as well as victims and survivors.

- Content detection accuracy: An overreliance on automated tools risks errors in the detection process and the wrongful removal of content, as well as other potential negative consequences such as the banning of users’ accounts. Automation may support but cannot replace human content moderation. Any inadvertent outcomes due to errors from automated processes must be reversible through human support.

We would welcome any opportunity to share further information, resources and expertise with the Special Rapporteur should this be useful during the development of the report.