Call for input

Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

ECPAT Sweden (hereinafter ECPAT) is a children's rights organization that works against all forms of sexual exploitation of children. Ms. Mama Fatima Singhateh has invited all interested parties to share information, documents, statements, analysis and input regarding sexual exploitation and abuse of children in the digital environment and ECPAT is happy to contribute to this important report from the Special Rapporteur.

ECPAT would like to highlight in particular that

- Children have rights online and have the right to explore the digital environment.
- Regulations need to demand that online platforms take responsibility and make the digital environment safe for children, as children have the right to safety in the digital environment.
- When it comes to sexual exploitation and abuse of children in the digital environment, it is often children that expose other children. It is therefore crucial that children get information regarding what rights they have online, both as victims and as someone who might have committed a crime, what mechanisms there are to report sexual exploitation and what is okay and not okay to do online.

How technologies are used to facilitate the sexual exploitation and abuse of children

Children have the right to explore the digital environment in a safe way. The internet is a fantastic place for children to get information, meet other people, explore their sexuality and more. From our standpoint different kinds of prohibition for children, for example age restrictions, are not something that will be of benefit for children and their wellbeing. From our perspective it is the online platforms that need to create a safe environment for children.

When it comes to sexual exploitation and abuse of children online it is common that children themselves expose other children. It is therefore crucial that when children are exploring the digital environment, they get relevant information about what rights they have, as a victim but also as someone who may have committed a crime against another child. It is important that information regarding what is okay and not is easily accessible for children and that there are different reporting systems that can be used by children.

One common phenomenon, where often children expose other children on the internet, is so-called expose accounts. These accounts, forums and threads are used to disseminate sexually degrading photos and exploitative content, mainly depicting girls. In many cases the person who the photo was initially sent to is the same age and a partner or someone with a flirtatious relationship. The

ECPAT Sverige
Garvargatan 20
112 21 Stockholm

08-59 89 20 00
info@ecpat.se
www.ecpat.se

child's name, age, school and social media accounts are often written amongst the sexually degrading photos that are disseminated. This makes it easier for others to identify the victim and contact and harass them even more.[1]

The algorithms of the social media platforms recommend expose accounts to children, which leads to widespread sharing in the children's environment. In certain instances, we have seen social media platforms taking swift and effective action to reduce the sharing of other types of problematic material. A couple of examples are materials that are linked to terrorism and disinformation during the pandemic. The question is why they can't implement similar measures to protect children and prevent them from becoming victims of serious sexual offences. We have seen that children want the platforms to be proactive and work with the authorities by reporting illegal content and helping the police to do their job, and that is an important step they can take to help child victims of online offences. It is completely unacceptable that platforms themselves are contributing to the abuse of children when they, for example, recommend expose accounts to children.

Another common phenomenon is financial sextortion, which the FBI, NCMEC and Canadian Centre for Child Protection also have reported about. The phenomenon seems to be similar around the world where young boys are usually targeted on online platforms like Instagram and Snapchat and are contacted by a perpetrator that pretends to be a child of the same age. That way the perpetrator is able to persuade the boys to send nude photos or videos of themselves. Thereafter the perpetrator starts to threaten to spread the photos/videos if they do not pay them money.[2]

We have seen indicators that this type of crime is internationally organized. There is much to suggest that financial sextortion is increasing rapidly and that the victims are getting younger and younger. It is also apparent that the perpetrators are adapting and changing their approach quickly to make it more difficult for children to find effective protection strategies. In many cases the perpetrators use the same photo when creating new fake accounts and the information needed to detect these accounts are therefore visible for online platforms. It is therefore unacceptable that the perpetrators are able to create these new fake accounts again and again.

Measures needed to prevent sexual exploitation and abuse of children in the digital environment

It is crucial that the states and online platforms take responsibility. Legislation that puts a heavy burden on children and their parents is not acceptable. We are contacted, through our helplines for children and adults, very often by children or parents who ask for advice when for example a child's nude image has been disseminated. It is important to educate parents and caregivers so that they have a better understanding of the digital environment, but children should not be dependent on their parents' abilities. The main burden should therefore lie on the state and online platforms to take measures to prevent sexual exploitation and abuse of children online.

[1] To read more about expose accounts see our report "I was just looking, I didn´t do anything bad – A report on children being exposed on expose accounts".
[2] To read more about sextortion see our report "Then "she" took a screenshot and it all began – A report on financial sextortion of children, with particular focus on the vulnerability of boys".

Platforms whose services can be misused to sexually exploit children, and especially those that target their services to children, have a responsibility to ensure that they are safe for children to use. Today, the information on most platforms is incomplete or difficult to access. Platforms must inform children and young people using their services about the possibility of crime and other risks, but also about the perpetrators' modus operandi and easily accessible information on how children go about reporting crimes. Platforms also need to inform children about their rights as victims but also as someone who might have committed a crime, as it is common that children expose other children online.

If images have been disseminated on the platforms, the platforms must act promptly to remove the illegal content and not make it possible for accounts they suspend because they have committed child sexual abuse to open new accounts on the same platform or other platforms that the company operates. Platforms must also act preventively and put in measures so that it is not possible to create fake accounts and to disseminate child sexual abuse material. When it comes to, for example, financial sextortion the fake accounts usually in a short period of time contact many children and extort them on money before the accounts are closed by the platform. This has to change. Platforms also need to have a better cooperation with law enforcement.

Our standpoint is that the most important source of information regarding children's rights is the children themselves. It is therefore crucial that the platforms design their safety measures together with children, as it is the children themselves that have the best knowledge of their reality in the digital environment.

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

Regulation at national level, EU level and globally need to ensure that no digital services are being misused to commit sexual child exploitation and abuse. Companies' measures can no longer be only on a voluntary basis – they must take responsibility. Still, regulation must not be a hindrance for voluntary measures, it is not a question of either or, mandatory as well as voluntary measures are important. Our key demands when it comes to regulations to detection, reporting and removal of child sexual abuse and exploitation material (CSAM/CSEM) are that they are child-rights focused, technology-neutral and include known and unknown material as well as grooming. The duty to use detection technology must be based on a risk assessment of the service itself, not in relation to user behaviour in and of itself or previous suspicion of a committed offence. That is not a realistic approach to combating the dissemination of child sexual abuse material.

In order to work effectively against online sexual abuse and exploitation of children the states must ensure a proactive, global multi-stakeholder, cross-sector approach with the involvement of among others: civil society, law enforcement agencies, other government agencies, healthcare and education and all relevant companies to work together in a transparent and equal cooperation.

Existing challenges in the use of 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

As earlier mentioned, there are indicators that behind, for example financial sextortion, there is internationally organized crime. These crimes are difficult to investigate, especially when they are across borders. The perpetrators can be in different countries and use technologies that make it very hard to identify them. The investigations are not usually prioritized by the police and therefore take a very long time. The international system of legal assistance in criminal matters is not working as effectively as it should. Authorities must priorities these types of crimes and the cooperation between countries across the world must be better.

Important steps to increase law enforcement efficiency would include ensuring enough data retention and proactively work to prevent new regulations such as the e-Privacy regulation and similar regulations to impose hinders to investigations, detection and removal of child sexual exploitation material. Important steps to increase ICT efficiency and cooperation would include legal incentives to proactively prevent hosting of known illegal material as well as being in the forefront of technology to discover all forms of child sexual abuse or exploitation material.

Technical and regulatory measures that can be but in place by states, the technology industry and online service providers toward mitigating human rights risks associated of online child sexual exploitation and abuse, and ensuring the minimum harmonization across legal jurisdictions

Legislation needs to put children's right not to be exposed to sexual violence and the child's right to personal integrity first. From our perspective, sexual exploitation of children is a matter that justifies exceptions, but it is very important that the tools employed are not misused for other purposes, as this would risk harming our chances to retain such tools. It is also relevant for ensuring that the tools employed are sufficiently accurate.

Children have the right to be protected against sexual exploitation and abuse both online and offline. One aspect of the right to personal integrity is the right not to be subjected to crime. The digital environment needs to be safe for children and the online platforms need to take responsibility in making the environment safe. As mentioned above platforms must have sufficient and easily accessible information for children about the possibility of crime, about their rights and how they go on reporting crime. Platforms must act promptly to remove illegal content, work together with law enforcement and not make it possible for accounts they suspend because they have committed child sexual abuse to open new accounts on the same platform or other platforms that the company operates.

Children in the digital environment also have the right to privacy that needs to be respected when technical measures are put in place. The aim of the technical measures should not be to, for example, control or monitor children in the digital environment. Every child has the right to personal integrity,

both online and offline. Children have the right to explore the digital environment and different kinds of prohibitions, such as age restrictions, are therefore not acceptable from our standpoint.

Practical examples of internal monitoring, complaint and reporting processes

ECPAT has created a secure uploading tool that children can use if they want help with removing images or videos online. When the image or video has been uploaded, the hotline analysts will submit the images/videos into Project Arachnid, a tool that searches for the images/videos on the open internet, providing extra protection compared to only trying to remove material from the known online location. ECPAT also provides a platform guide, showing step by step how to report abuse on various platforms.

Another example is NCMEC's service TakeItDown, which allows children to submit images to a NCMEC database which will make circulation of the images more difficult on the participating platforms. Facebook and Instagram are examples of participating platforms in TakeItDown.

Another example of a reporting mechanism is trusted flaggers. They are special entities that are experts at detecting certain types of illegal content online, such as CSAM/CSEM. The notices submitted by them must be treated with priority as they are expected to be more accurate than notices submitted by an average user. ECPAT has status as a trusted flagger on various online platforms such as Snapchat. The EU´s Digital Service Act has made it possible for entities to apply for status as a trusted flagger at the National Authorities. Other jurisdictions should also, similar to what the EU has done, establish formal trusted flaggers so that removing CSAM/CSEM and accounts that spread that kind of material becomes even more efficient worldwide.

Challenges regarding Artificial Intelligence and end-to-end encryption

AI-generated CSAM/CSEM is a violation against the rights of all children and normalizes child sexual abuse and exploitation. The existence of AI is a challenge that needs to be addressed holistically, by states and industry together. There needs to be zero tolerance, meaning that AI cannot be misused for any forms of sexual exploitation or abuse of children.

In ECPAT Sweden's hotline, we have seen the development of generative AI used for creation of child sexual abuse and exploitation material. The quality of the material has improved, and we have also noticed how the creators have started to add grain and other techniques to make the images less perfect and more realistic.

In the creation of AI-generated or manipulated CSAM/CSEM, we have seen how images of known victims have been used to create new images. This means an added layer of exploitation for the victim. We have also seen how images of children who are not victims of CSAM/CSEM have been used to create CSAM/CSEM images. This creates new victims and can also be used by offenders for the purpose of, for example, sextortion. We have also seen CSEM/CSAM images with what we believe is completely AI generated children. Furthermore, AI can be used by offenders in, for example, grooming processes. AI can also be used by offenders to manipulate texts, images and even live video when contacting a child.

End-to-end encryption (E2EE) is an ongoing challenge for law enforcement and content moderators in ICT. Communication channels can be used to send CSAM/CSEM and to contact children. Companies are hindered from using tools to detect illegal material and cannot report to the police. Every child has the same right to protection from sexual abuse and exploitation, and this should not depend on the platform. Any company using E2EE must ensure that CSAM/CSEM and attempts to contact a child for sexual purposes are detected and reported to law enforcement.

Examples of proactive measures taken to facilitate consultation and participation with a broad range of stakeholders

As earlier mentioned, ECPATs standpoint is that the most important source of information regarding children's rights are the children themselves. ECPAT has conducted, for four years in a row, *Nude online* – an online survey aimed at children and young people aged 10-17. The aim is to understand children's sexual vulnerability – especially on the internet – based on the children's own experiences and attitudes. *Nude online* is a story-based inquiry. This means that the children read a short story about a young person in a sexually vulnerable situation. Then they answer what advice they would give to the person in the story. *Nude online* is a unique opportunity for ECPAT to learn from those who know best about children's lives and who are experts in it – the children themselves. The children also play an important role in interpreting the responses from the survey. By allowing children to form analysis groups and help us in the analysis of the answers, we want to ensure that the children's perspectives and interpretations are heard. The survey also gives children a possibility to express their opinions and thoughts in a safe way and they can do it from wherever in the world. *Nude online* has responses from approximately 7 000-13 000 children per year.

Mechanisms put to 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 harmonization and mainstreaming across domestic and regional efforts when combatting this phenomenon

ECPAT has two coalitions with companies from the tech industry and finance industry that aim to work actively together to stop the exploitation of children online. The coalitions are initiatives that will help lead development forward, to find new solutions to stop widespread crime and to increase the knowledge of employees and other societal actors.

ECPAT’s Tech Coalition, which is the collaboration between companies in the tech industry, has developed a blocking cooperation in which, on a daily basis, members of the coalition block countless attempts to access websites deemed by the police to contain child sexual abuse material.

ECPAT’s Finance Coalition, which is the collaboration between companies in the finance industry, has a project that has focused on identifying indicators related to payments made for livestreamed CSAM and how these indicators could be implemented in banks AML-systems and working methods.

The work focuses on benchmarking and information exchange, but also external monitoring, statistics collection and technology development.

Anna Karin Hildingson Boqvist

The secretary–general of ECPAT Sweden

Stockholm the 15th of May 2024