**Draft General Comment No. 25**

**Children’s rights in relation to the digital environment**

We welcome the draft General Comment, No. 25: Children’s rights in relation to the digital environment, which brings a much-needed children’s rights focus to considerations of internet governance and digital regulation. This is an especially important area for nation state legislation and policy given that one in three internet users are under 18; we know the online world poses significant threats to children on a global scale; and that more recent discussion about human rights based approaches to content moderation have paid insufficient attention to children.[[1]](#footnote-2)

As the United Kingdom’s leading children's charity preventing abuse and helping those affected to recover, the National Society for the Prevention of Cruelty to Children hopes to highlight in this comment the need for robust regulation of digital environments and accompanying legal frameworks that provide direction to businesses to tackle online child sexual abuse, and makes suggestions for how this draft General Comment could best be considered and implemented at a nation state level to enable this.

Within this response, we suggest additions that could strengthen the framework in the draft General Comment to implement the rights of the child in a digital environment. Our analysis focuses on how these general measures can provide a frame for a national response to prevent online abuse, and the need for independent regulation of online business through a robust legal framework. The key areas of focus are:

Safety by design: Business in the digital environment should consider embedding a safety by design approach in all aspects of their work, at the design and innovation stage, to support the delivery of the best interests of the child. States should consider their role in providing businesses with the appropriate legal and regulatory frameworks to protect those rights from the initial conception of digital processes. This will be explored throughout and in paragraphs 13, 39 and 78.

Transparency reporting: businesses and States should work together to ensure the proactive monitoring of the protection of these rights, and set obligations for businesses to act accordingly. Transparency reporting will support the ongoing protection of children’s rights by requiring businesses and non-state actors to carry out and disclose to the public both impact assessments and the measures taken to innovate in the best interests of children. This will be further explored in paragraph 32.

Sanctions: Should be proportionate and targeted to ensure that these rights are effectively upheld, which may include criminal and financial accountability measures. Whilst proportionate to the size of the business and the harm, sanctions on a state level would provide incentives for global technology firms and businesses to act, thus impacting the scale of a global threat. We explore this further in our comments on paragraph 45.

User advocacy arrangements: Whilst the note recognises the importance of including the voice of children and young people in the protection of their digital rights, we feel this can be expanded much further to represent children’s individual and collective interests. Promoting user advocates at a state level will ensure that children’s right to be heard is amplified, delivering the strongest possible outcomes for children at a variety of levels. User advocacy is expanded upon below in paragraphs 19 and 35.

**V. General measures of implementation by States (art. 4)**

**Overarching Comments**

The general measures are of particular importance for this general comment, because they help shape the conditions through which nation states create legislation. Legislation in this area will help make sure that states have the right laws and commitments in place to uphold children’s rights in a digital world. In this respect, we would like to highlight the interplay between children’s rights, state’s obligations to uphold these rights, and businesses as non-state actors protecting against child rights violations. The role that online businesses play in influencing the scale of harm that children face online is vital. Whilst the extent of criminal prosecution of online harms varies from state to state, tackling the harm at a domestic level in respect of services that are likely to be used by children in that country, by appealing to a positive obligation to promote, fulfil and respect children’s rights in the private sector will be a highly effective way to tackle digital child rights violations on a global scale.

Whilst we acknowledge that the draft general measures of this comment focus on respecting, protecting and fulfilling children’s rights in the digital environment, it is important to consider where this sits in relation to the scale of the global criminal threat of child abuse online, and the vast differences in criminal action to tackle this internationally.

Data from the 2019 WePROTECT global threat assessment report shows that 750,000 individuals are estimated to be looking to connect with children across the globe for sexual purposes online at any one time.[[2]](#footnote-3) There were 18.4 million referrals of child sexual abuse material by US technology companies to the National Centre for Missing and Exploited Children in 2018[[3]](#footnote-4). With an 100% increase in the number of photos of children being sexually abused reported by tech companies[[4]](#footnote-5), and an estimated 3.5 billion social media users globally,[[5]](#footnote-6) 1 in 3 of which are children, it is clear the scale, severity and complexity of online child sexual abuse material is increasing at a fast pace that clearly requires a systemic approach to harm reduction. WePROTECT highlight an urgent need for Governments, law enforcement, the technology industry and third sector organisations to work together to step up their collective response.[[6]](#footnote-7)

In the United Kingdom, it was only in 2017 that it was made illegal to make sexual communication with a child online, after a concerted efforted by the NSPCC through our Flaw in the Law campaign. While differences in domestic laws exist, it proves increasingly difficult to infiltrate growing criminal networks that are not confined to state borders, and facilitated by the hitherto unregulated social networks and online businesses that take no responsibility for the harm happening on their sites. The differences in law enforcement between countries means that criminal sanctions differ, and in most cases, targets the offenders rather than the platforms that enable abuse. Without concerted international efforts to navigate the relationship between child rights, state action and the responsibility of non-state actors online, the scale of criminal action and child rights offences will remain unseen.

States have a positive obligation to regulate corporate activities and to take effective enforcement measures that investigate, adjudicate and redress violations of children’s rights when they occur, protecting against human rights violations by third parties including businesses, both nationally and internationally.[[7]](#footnote-8) The general principle for the best interests of the child can provide a basis for an effective regulatory response, based around a duty of care, that requires companies to demonstrate they have acted in the best interests of the child. It is clear that the statutory regulation of global tech firms through legislative frameworks that protect children’s rights online should be implemented by individual states, based on their obligation to protect children from harm by non-state actors. Regulatory action taken at a nation state level can therefore have an impact both domestically and internationally.

**A) Legislation (Art. 4 Section A)**

Paragraph 24 outlines that States should review and update national legislation to ensure the digital environment is compatible with the rights in the Convention. In line with comments above, any obligation to update national legislation should consider how an independent regulator of online businesses and accompanying legislative frameworks would help protect children in each state from harm caused by non-state actors and businesses.

For example:

24. States should mandate the use of independent regulation of online businesses operating within the State, protecting children from harm that occurs on these sites using the child rights impact assessment to inform the development of legislation.

**C) Coordination (Art. 4 Section C)**

Paragraph 28 calls for a Government body to coordinate policies and programmes related to children’s rights in the digital environment. We believe that in addition to this there should be an independent regulator that monitors, protects and enforces online businesses in each state to uphold child rights through a duty of care model.

For example:

28. States should ensure these coordinated policies and programmes also include an online regulatory body, that coordinates with the work happening at different levels of Government, to ensure strong and robust digital regulation in the best interests of the child.

**F) Independent monitoring (Art. 4 Section F)**

Paragraph 32 discusses how to address complaints from children and their representatives. In line with our suggestions for States to implement regulation of online businesses, we believe that independent monitoring of online businesses should include transparency reporting and investigation powers to ensure these rights are consistently upheld in line with the expanding rate of technological change in each state.

For example:

32. States should put in place legislation that allows for the independent monitoring of online businesses that operate in their state. Mandatory corporate reporting will support safety by design in application, by encouraging businesses to build the best interests of the child into their approach.

**H) Cooperation with civil society (Art. 4, Section H)**

Paragraph 35 tells that States should systematically involve civil society in the monitoring and evaluation of these laws, policies and plans to protect children’s rights. This cooperation with civil society should also include processes for user-advocacy arrangements, to ensure that children’s voices are heard and amplified.

For example:

35. States working with civil society to monitor these laws and policies should create user-advocacy arrangements that work to amplify and protect the voices of children who experience harm online, working to protect their digital rights.

**I) The business sector (Art. 4 Section I)**

Paragraphs 36 to 39 explore the responsibility of businesses to prevent their sites from being misused for purposes that threaten child safety. To strengthen this response, legal and regulatory frameworks should be implemented in the nation state context, so that understandings of how to protect children’s rights in the digital environment are distilled down to businesses and firms who can prevent this harm. States need to work to process higher level regulation that protect children’s rights into manageable frameworks for businesses.

For example:

39. States should encourage businesses to take measures to innovate in the best interests of children. Safety by design, and innovation from the design stage of a digital product will mean that businesses must take measures to consider the risks a child might face and how this would impact their rights from inception.

**K) Remedies (Art. 4, Section K)**

Paragraph 45 calls for appropriate and effective remedial judicial and non-judicial mechanisms for the violation of children’s rights relating to the digital environment. However, in addition to these remedial mechanisms, States need to ensure that online businesses are held accountable for instances when they violate children’s rights in this environment, through sanctions that will give strength to regulation and provide incentive for businesses to act.

For example:

45. These remedial mechanisms should be accompanied by proportionate and targeted sanctions to ensure that these rights are effectively upheld, which may include criminal and financial accountability measures.

**III. General principles:**

**B) The best interests of the child (art. 3, para. 1)**

Paragraph 13 states that the best interests of the child is a dynamic concept that requires specific contextual assessment. In the context of the digital environment, it would be relevant here to refer to safety by design approaches to technology and children’s rights. Safety by design means creating the site or platform with the best interests of the child in mind, including risk assessments of new services, and taking reasonable mitigations to prevent harm in existing services.

For example:

13. The best interests of the child shall be the primary consideration. The regulation and design of the digital environment should be underpinned by a safety by design approach, incentivising businesses to proactively mitigate risks to children through their sites.

**D) The right to be heard (art. 12)**

Paragraphs 18 and 19 suggest it is the States responsibility to ensure children’s voices are heard. However, to ensure that this voice is balanced alongside that of global technology firms, a user advocacy agreement should also be drawn up by states to help ensure children’s voices are amplified, protected, and accounted for.

For example:

19. States should ensure that providers of digital technologies actively engage children and give their views due consideration when developing their services. User advocacy arrangements, in place through the regulatory body and civil society, will ensure that child users are empowered and that their views are given sufficient weight.

**VI. Civil rights and freedoms**

**E) Right to privacy (art. 16)**

Paragraph 73 discusses legislative measures to respect children’s right to privacy. This section uses end to end encryption as an example of privacy by design. We take issue with this example, as the use of end to end encryption is a huge safety concern, because this encryption facilitates access to secure channels for perpetrators to hide from law enforcement.

“The growing availability of advanced anonymization tools and end-to-end encryption peer-to‑peer (P2P) file-sharing networks is enabling offenders to have easier, more secure access both to vulnerable children and to the networks of people who share a sexual interest in children. There appears to be a link between large-scale membership of these online ‘safe‑havens’ (the UK’s National Crime Agency has identified 2.88 million registered accounts across the ten most harmful Dark Web sites) and the growing commodification and industrialisation of child sexual abuse material.”[[8]](#footnote-9)

We recommend removing this example, in acknowledgement of the risk this poses both to children’s right to be protected from harm, and the abused children’s right to privacy. An important aspect not yet covered in the note is how to protect the rights of children who have been abused, exploited or groomed online. For example, the scanning and detection of child sexual abuse material is a necessary step in protecting the rights of the children whose rights are violated by those images. It is important to consider the needs of those who have been harmed as well as trying to prevent this harm from occurring in the first place.[[9]](#footnote-10)

Paragraph 78 refers to safety by design ‘as an approach to anonymity’. Whilst this is a legitimate interpretation of safety by design, safety by design should be applied beyond privacy, and throughout the general note. Considerations of safety by design for protection from harm, abuse and exploitation should be referenced as per recommendations in this response.

**VII. Violence against children (arts. 19, 24 (3), 28 (2), 34, 37 (a) and 39; OPSC; OPAC)**

Paragraph 85 states that some risks of harm in the digital environment are perpetrated by children themselves. Whilst true to an extent, this phrasing seems to place the blame on children themselves, when often the design features of a site exacerbate or compound these risks. We would recommend rephrasing to reflect the nuance of peer on peer abuse and online harms.

For example:

85. Some risks of harm in the digital environment are perpetrated by children themselves, not necessarily with the child’s full understanding of the harm that can result. This risk of harm can be exacerbated by design features of social media sites and online platforms, and as such, States should consider regulation that follows a duty of care and safety by design approaches to minimise this risk.

For more information, please contact:

Hannah Ruschen, Policy and Public Affairs Officer | [hannah.ruschen@nspcc.org.uk](mailto:hannah.ruschen@nspcc.org.uk)

1. ‘The State of the World’s Children 2017: Children in a Digital World’ (UNICEF, 2017: pg. 1) [↑](#footnote-ref-2)
2. ‘The dark side of the internet for children: online child sexual exploitation in Kenya –A Rapid Assessment Report’ (Terre des Hommes, 2018: pg. 3) [↑](#footnote-ref-3)
3. ‘Global Threat Assessment 2019.’ (WePROTECT Global Alliance, 2019: pg. 7) [↑](#footnote-ref-4)
4. Between 2018 and 2019, ‘Global Threat Assessment 2019.’ (WePROTECT Global Alliance, 2019: pg. 10) [↑](#footnote-ref-5)
5. ‘Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce’ (We Are Social, 2019: pg. 8-63) [↑](#footnote-ref-6)
6. ‘Global Threat Assessment 2019.’ (WePROTECT Global Alliance, 2019: pg. 7) [↑](#footnote-ref-7)
7. ‘State obligations, children’s rights and business’ (UNICEF, 2011: pg. 2) [↑](#footnote-ref-8)
8. ‘Global Threat Assessment 2019.’ (WePROTECT Global Alliance, 2019: pg. 7), National Strategic Assessment (National Crime Agency, 2019: pg. 13) [↑](#footnote-ref-9)
9. “This non-discrimination obligation requires States actively to identify individual children and groups of children the recognition and realization of whose rights may demand special measures.” One of these groups of children is those who have been abused online to produce child sexual abuse material, and need special measures to realise their right to privacy, by removing those images. CRC/GC/2003/5. Pg. 4, Article 2. [↑](#footnote-ref-10)