5RIGHTS FOUNDATION

Consultation response: General comment on children's rights in relation to the digital environment

Overview

The general comment, No.25: Children's rights in relation to the digital environment is a welcome guide on legislative, policy and other measures to ensure States' full compliance with obligations under the United Nations Convention on the Rights of the Child (UNCRC) and its Optional Protocols. The general comment is a significant step towards prioritising the safety and security of children by setting out how existing rights apply in the digital environment and the enduring relevance of the UNCRC to a changing digital world. Below, 5Rights Foundation provides overall comments on sections of the draft general comment. Red text indicates suggested edits to phrasing or additions to the general comment.

Comprehensive policy and strategy (section B) *and* civil rights and freedoms (Section VI)

- Paragraph 26 calls for measures focused on protecting children, providing the example of online sexual abuse and exploitation.[1] Examples are valuable, however a broader list that explains a range of risks facing children in the digital environment would be useful here. Suggested rephrasing *'should protect children from harms resulting from content, contact, conduct and commercial risks[2], including online sexual abuse and exploitation. Measures should also provide…'*
- The general comment discusses the need to balance children's freedom of expression with ensuring online safety. While recognising the importance of the inclusion of this in the general comment, the current phrasing in paragraph 55[3] may be interpreted as prioritising children's right to freedom of expression above that of their safety. The general comment should reflect the fundamental premise of children's rights, that they are indivisible and all of equal importance and thus individual rights cannot be privileged over others. This could be resolved by suggested rephrasing to paragraph 57: *'Such controls should balance protection against children's rights, notably their rights to freedom of expression, privacy, and their other rights.[4]'*

---

[1] Paragraph 26: 'measures should protect children, including from online sexual abuse and exploitation, and provide remedy and support for child victims and measures to meet the needs of children in disadvantaged or vulnerable situations, including resource materials translated into relevant minority languages.'

[2] Commercial risks are also referred to as contract risks

[3] Paragraph 55: 'Any restrictions on the operation of any internet-based, electronic or other information dissemination systems, are only permissible to the extent that they are compatible with Article 13'

[4] Mentioning the need to balance children's safety alongside that of their expression and privacy is particularly important given the current phrasing of paragraph 72.

Freedom of thought, conscience and religion (art.14) (section C)

- Paragraph 63 discusses the role of automated systems and the impact these can have on children, with particular reference to education, health, criminal justice and commercial contexts. In addition to the impact of automated systems on children's behaviour and emotions, this paragraph should also refer to the impact that such systems can have on a child's future outcomes. For example, welfare provision that is increasingly reliant on automated systems has been found to 'disadvantage women, older people, people who do not speak English and persons with disabilities.'[5] The general comment should therefore make an additional provision so that States ensure that children's rights to non-discrimination, for example, are recognised and embedded into the design and use of automated systems.

For example:

63. States shall respect the right of the child to freedom of thought, conscience and religion in the digital environment. Automated systems are sometimes used to make inferences about a child's inner state, in education, health, criminal justice or commercial contexts, among others. States shall ensure that automated systems are not used to impact or to influence children's behaviour, emotions or future outcomes. States shall also ensure that automated systems are designed to uphold children's rights, to prevent discrimination and enable equal access to health, education and justice.

Right to privacy (section E)

- Paragraph 69 discusses threats to children's privacy arising from data processing. Naming children and their actions at the beginning of this list of actors may risk interpretation that children themselves are disproportionately responsible for maintaining their own data privacy, when the reality is that an asymmetry of power means children have little control. As part of this, reference should be made to how a failure to provide high privacy settings by design and default undermines children's privacy.

For example:

69. Privacy is vital for children's agency, dignity and safety, and for the exercise of their rights. Threats to children's privacy may arise from data processing by public institutions, businesses and other organizations; as well as from criminal activities such as hacking and identity theft. Threats to children's privacy may arise from their own activities in the digital environment,[6] but such threats are also invited by low privacy settings that make children's personal information public to all online users by design and default. Alongside this, the activities of others pose a threat to children's privacy, for example by parents' sharing online the photos or other information of their children, or by caregivers, other family

[5] Paragraph 60 UN General Assembly, Report of the Special Rapporteur on extreme poverty and human rights, available here. 23rd April 2019.

[6] Children's consultation.

members, peers, educators or strangers.

- Minor rephrasing also suggested to paragraph 70 as follows: 'Children are concerned about their privacy and want to better understand how their data is processed, by whom and how this is used.'
- The current phrasing of paragraph 72[7] uses end to end encryption as an example of privacy-by-design and calls on States to legislate for the adoption of end to end encryption (E2EE). In doing so, the Committee suggests that E2EE results in unmitigated benefits for children, however internationally, there are significant and shared concerns about the implementation of E2EE among those tasked with children's safety.

  The UK Home Office recently warned that encryption threatens public safety: "*1) By severely undermining a company's own ability to identify and respond to violations of their terms of service. This includes responding to the most serious illegal content and activity on its platform, including child sexual exploitation and abuse, violent crime, terrorist propaganda and attack planning; and 2) By precluding the ability of law enforcement agencies to access content in limited circumstances where necessary and proportionate to investigate serious crimes and protect national security, where there is lawful authority to do so.*"[8]

  The Australian E-Safety Commissioner also warns; *"Encryption can assist in serious harms by hiding or exacerbating criminal activities, including online child sexual abuse. Technologies that detect illegal material by proactively scanning, monitoring and filtering user content currently do not work on systems that use E2EE. Because of this, E2EE can facilitate the production, exchange and proliferation of child sexual abuse material, perpetuating the abuse of victims and exposing survivors to ongoing trauma."*[9]

  A recent communication from the European Commission explains that: *"The introduction of end-to-end encryption, while beneficial in ensuring privacy and security of communications, also facilitates the access to secure channels for perpetrators where they can hide their actions from law enforcement, such as trading images and videos. The use of encryption technology for criminal purposes therefore needs to be immediately addressed through possible solutions which could allow companies to detect and report child sexual abuse in end-to-end encrypted electronic communications. Any solution would need to ensure both the privacy of electronic communications and the protection of children from sexual abuse and sexual exploitation, as well as*

[7] Paragraph 72: 'States should encourage the adoption of privacy-by-design, such as end to end encryption, in services that impact on children.'

[8] Home Office, UK Government: International Statement: End-to End Encryption and Public Safety. Published 11th October 2020

[9] E-Safety Commissioner, Australian Government: End-to- End Encryption Trends and Challenges- Position Statement. Updated 11th May 2020

the protection of the privacy of the children depicted in the child sexual abuse material."[10]

- The current phrasing of paragraph 72 of the general comment fails to acknowledge the safety concerns raised by the introduction of end to end encryption, for example the impact this could have on the efficacy of tools used to detect child sexual abuse imagery. The inclusion of this example either requires a caveat that explains *'such as end to end encryption, only if evidence is provided that the functionality of existing detection and safety technologies can be met by new technologies.'* Ideally, this example would be changed altogether to an aspect of design that does not jeopardise the safety of children. A suitable example would be default settings that ensure high levels of privacy.

For example:

72. States shall take legislative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Such legislation should include strong safeguards, independent oversight and access to remedy and routine provision of privacy-by-design, such as high privacy default settings, in all online services that impact on children. States should regularly review such legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. States should ensure that consent to process a child's data is informed and freely given by the child or, depending on the child's age and maturity, by the parent or caregiver, and obtained prior to the processing.

- Paragraph 78 of the general comment explains that children use online avatars or names that protect their identity to aid with privacy online, however this section also goes on to say that anonymity should be considered within safety-by-design so that *'anonymous practices are not routinely used to hide harmful or illegal behaviour'* and suggests *'Safety-by-design might include encouraging platforms to forbid such behaviours in their published terms and block users who fail to uphold their standards.'* Currently this section seems to undermine the practices that children adopt to ensure privacy by proposing platforms prohibit these. A change to the structure of this paragraph or rephrasing could aid with balancing children's practices with the need for safety-by-design via other means including effective content moderation, age verification and upholding published terms.

For example:

78. Many children use online avatars or names that protect their identity, and such practices can be important to protect children's privacy. States should take a safety-by-design approach to anonymity, to ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, for example bullying or hate speech. Safety by design and privacy by design prioritise child safety and or privacy as a starting point for the development, design, production and

[10] European Commission: Brussels, 24.7.2020, COM(2020) 607 final. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions.

distribution of all new online services. This involves the assessment and mitigation of content, contact, conduct and commercial risks that may threaten the child's safety or privacy. This means that online services are designed according to children's rights. Protecting a child's privacy in the digital environment may be vital in circumstances when the parents or caregivers themselves pose a threat to the child's safety or, for example, when they are in conflict over the child's care (e.g. custody or access). Such cases may require interventions such as family counselling or other online services to safeguard the child's right to privacy.

Dissemination of information. awareness-raising and training (section G)

- In paragraph 33, the general comment calls on States to provide educational programs for children, parents and caregivers, as well as the general public and policy makers, to enhance knowledge of children's rights and develop digital literacy skills. Additionally, this paragraph should call on States to ensure that children have access to a variety of information in the digital environment.

For example:

33. States should disseminate information and conduct awareness raising campaigns on the rights of the child in the digital environment. States should facilitate educational programs for children, parents and caregivers, as well as the general public and policy makers, to enhance their knowledge of children's rights and develop their digital literacy and skills. This should include how children can benefit from digital services, how to minimize risks and how to recognize a child victim of online harm and respond appropriately. Alongside educational programs, States should ensure that children are able to access a plurality of information including news media and information from trusted sources in the digital environment.

- Paragraph 34 notes that professionals working for and with children require training that includes how the digital environment impacts the rights of the child. It is good to see explicit reference to the technology industry here, however the general comment could also refer specifically to those who design automated systems that are used in the settings discussed here.

For example:

34. Professionals working for and with children in all settings, including in health and mental health facilities, in social work, alternative care institutions, law enforcement, the justice system as a whole, and the business sector including the technology industry and those who design automated systems for these settings, should receive training that includes how the digital environment impacts the rights of the child in the multiple contexts, the ways in which children access and use technologies, and the impact automated systems may have on the future outcomes of a child. States should ensure that pre-service and in-service training relating to the digital environment is provided for educators working in nurseries, schools and other learning settings.

The business sector (section I)

- This section of the general comment should make explicit reference to the obligation on businesses to not only ensure their online services are not *'misused'* but also to ensure safety-by-design and privacy-by-design. Suggested addition to paragraph includes: *'States have obligations to ensure that the business sector meets its responsibilities for children's rights in relation to the digital environment by assessing how online services impact on children's rights, by ensuring safety and privacy by design, and by taking all necessary measures including adoption of legislation and regulations, and the development, monitoring and enforcement of policy.'* These additions are also consistent with the content of paragraph 39.
- Paragraph 38 of this section of the general comment would be strengthened by reiterating the call for child rights impact assessments made elsewhere in the document. This can be achieved via the following addition to this paragraph: *'States should take appropriate steps to prevent, monitor, and investigate child rights violations by businesses in the digital environment. For example, ensuring that as part of a child rights impact assessment, businesses are transparent about the steps they have taken to ensure safety and privacy in their design of online services.'*

Violence against children (section VII)

- Paragraph 87 refers explicitly to the responsibility of business enterprises to protect children. It would be good to ensure this responsibility is more consistent throughout the general comment, and this could be referred to as safety by design. This is particularly important given that the *'risks of harm'* outlined in paragraph 85, (for example *'the promotion of self-harming behaviours such as cutting, suicidal behaviour or eating disorders'*) are very often delivered as a result of businesses data processing and automated recommendation that serve up inappropriate or harmful content.

For example:

85. Forms of digitally mediated violence and sexual exploitation may be perpetrated within the child's circle of trust, for instance by family and friends or, for adolescents, by intimate partners. 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. These may include cyberbullying, harassment, violence, and sharing of sexualized images of children ("sexting"), and the promotion as a result of data processing of self-harming behaviours such as cutting, suicidal behaviour or eating disorders. Where children have carried out or instigated such actions, States should pursue preventive, safeguarding and restorative justice approaches whenever possible.[11]

87. States should ensure that business enterprises assess and mitigate the risks associated with the design of online services and implement safety-by-

[11] CRC/C/GC/24, para. 101.

design. In addition, business enterprises including all online services should meet their responsibility to effectively protect children from all forms of violence including cyber-bullying, cyber-grooming, sexual exploitation and abuse in the digital environment. Although businesses may not be directly involved in such harmful acts, they can be complicit in these violations of children's right to freedom from violence. States should develop regulatory approaches to encourage and enforce the ways businesses meet these responsibilities, taking all reasonable and proportionate technical and procedural steps to combat criminal and harmful behaviour directed at children in relation to the digital environment.[12]

Family environment and alternative care (section VIII)

- Paragraphs 89-95 emphasise the importance of empowering parents and those with caring responsibilities to understand the harms of the digital environment and suggest States should provide guidance on how best to support children. The final paragraph refers to the fact that some risks are enabled via the design and use of digital technologies. Following this, the general comment says: '*States should ensure that parents and caregivers are fully conversant with the risks and aware of strategies to support and protect children*' despite the fact that parents and caregivers have little control over the design of service. Restructuring the order of this paragraph so that parents' and caregivers' need for awareness and strategies is mentioned first, before then going on to explain that parents' role sits within a broader range of stakeholders, not least designers of online products and services.

For example:

95. Measures taken to enhance digital access should be balanced against the need to protect children in cases where parents or other family members, or caregivers, whether physically present or distant, may place them at risk. States should ensure that parents and caregivers are fully conversant with the risks and aware of strategies to support and protect children. Alongside this, States should ensure that the role of parents and caregivers is part of a wider societal response as such risks may be enabled through the design and use of digital technologies, for example by unintentionally revealing the location of the child to a potential abuser.

- Paragraph 92 currently says *'prioritise positive parenting over prohibition or control'* however an example would help to clarify what *'positive parenting'* means.

Education, leisure and cultural activities (section XI)

- Paragraph 113 explains that digital literacy curricula should 'promote awareness of the risks of children's exposure to potentially harmful content, contact and conduct, including cyberbullying and other forms of violence, and coping strategies to reduce harm and build children's resilience.' Suggest including commercial in this listing as

[12] CRC/C/GC/16, para. 60.

this would be consistent with other references throughout the general comments to economic risks including 'surreptitious advertising or highly persuasive or even gambling like design features'[13] and 'economic exploitation'[14].

Protection from economic, sexual and other forms of exploitation (section XII)

- Given the importance of robust age verification for stemming children's exposure to a host of risks in the digital environment, the following point which currently appears within paragraph 122 could be made more prominent if this appeared as a separate paragraph.

For example:

122. By creating and sharing content, children may be economic actors in the digital environment. The Committee notes that where children are involved in the production and distribution of content, this may constitute potential for their economic and possibly other forms of exploitation. States should review relevant laws and policies to ensure that children are protected against economic and other forms of exploitation and that their rights with regard to work in the digital environment and related opportunities for remuneration are protected. States should also inform parents and children about protections that apply, and ensure that appropriate enforcement mechanisms are in place.[15]

123. States should legislate to ensure that children are protected from harmful goods (such as weapons or drugs) or services (such as gambling). Robust age verification systems should be used to prevent children accessing products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements.

General remarks:

- It is understood that the purpose of the general comment is not to say *how* to implement the practical measures recommended throughout the general comment, for example; '*specialized training for law enforcement'* (para. 48), *'child rights impact assessments'* (para.38), or *'guidance for parents and caregivers'* (para.93). However, States may benefit from a separate document which includes a list of the practical measures referred to throughout the text. Such a list would form a useful checklist for States to reference when, for example, trying to identify the necessary steps to upholding children's rights in the digital environment.

[13] See paragraph 119

[14] See paragraph 121

[15] CRC/C/GC/16, para. 37.

- Throughout, the general comment should indicate what is meant by *'age appropriate'*[16] where this is mentioned in relation to specific practices, such as in the case of commercial advertising and marketing.[17]
- The general comment consistently refers to the need for States to support the provision and creation of *'child-friendly services'*.[18] To aid clarity, a definition[19] of this could be provided in the glossary that explains that services should be *'child-friendly'*, regardless of whether the digital environment is child-directed or a digital environment with users of all ages. The Committee might also consider replacing *child-friendly* with the term *age-appropriate*, as this concept incorporates age, age range and childhood development stages.

For example:

18. Children report that the digital environment affords them crucial opportunities for their voice to be heard.[20] The use of digital technologies can enhance children's right to be heard in matters that affect them and help to realize children's participation at local, national and international levels.[21] States should offer training and support to children, and provide access to child-friendly platforms, in order to let them express their views and become effective advocates for their rights. Here and throughout the general comment, 'child-friendly' refers to digital environments that uphold children's rights including that of their safety via the provision of age appropriate services, regardless of whether the digital environment is child-directed or a digital environment with users of all ages. While States are encouraged to utilise the digital environment to consult with children on relevant legislative and policy developments, they should ensure that children's participation does not result in undue monitoring or data processing that violates their right to privacy. States should also ensure that consultative processes are inclusive of children who lack access to technology.

About 5Rights Foundation

The digital world was never imagined as an environment in which childhood would take place. It was invented by adults, for adults and designed with the idea that all users are equal. But if all users are treated equally, then children and young people are treated as adult.

[16] Suggested addition to glossary: **Age appropriate:** The practice of determining whether an online service or digital environment is appropriate for the age or age range of the anticipated user, recognising children's evolving developmental capacity and the rights and protections to which they are entitled up to the age of 18.

[17] See paragraph 41

[18] See, for example, paragraph 52

[19] Suggested addition to glossary, 'child-friendly' services: The practice of stating that an online service is appropriate for use by children whether or not the digital environment is child-directed or a digital environment with users of all ages.

[20] Children's consultation.

[21] CRC/C/GC/14, paras. 89-91.

5Rights Foundation exists to make systemic changes to the digital world to ensure it caters for young people, by design and default. We advocate for enforceable regulation and international agreements that allow children and young people to thrive online. We develop technical standards and protocols to help businesses redesign their digital services with children and young people in mind. We publish and lead across our four priority areas: Design of Service, Child Online Protection, Children and Young People's Rights, and Data Literacy.

For more information please contact:
Victoria Jaynes, Policy Officer | Victoria@5rightsfoundation.com