

KEY TAKEAWAYS FROM THE ROUNDTABLE DISCUSSION ON FROM ACCESS TO ACCOUNTABILITY: RETHINKING CHILD SAFETY IN THE DIGITAL AGE

Closed-Door Roundtable | Chatham House Rules

Organised by: Broadband India Forum

Location: New Delhi

Date: 16 June 2026, Tuesday

Context and Background

Broadband India Forum organised a closed-door roundtable discussion titled **“From Access to Accountability: Rethinking Child Safety in the Digital Age”** in New Delhi. The discussion was held under **Chatham House Rules** and brought together a diverse group of stakeholders for a focused exchange on child safety in the digital environment. The roundtable was very well attended, with close to 20 speakers and around 40 participants in the room.

The roundtable was convened at a time when children’s digital participation has become central to how they learn, communicate, access opportunities, and engage with the world. While digital access can support education, inclusion, and social mobility, it also raises growing concerns around children’s safety, well-being, and exposure to online harms. Against this backdrop, BIF organised the roundtable to move the conversation towards a more balanced discussion on accountability, safety-by-design, and shared responsibility. The discussion focused on how India can develop effective, proportionate, and evidence-based approach that protect the children while preserving the benefits of meaningful digital participation.

KEY TAKEAWAYS

The key takeaways from the Roundtable discussion are as follows:

Ongoing Policy-Making Process

1. NCPCR is in the process of developing guidelines on children’s use of social media, following consultations with industry, civil society organisations and other relevant stakeholders. This indicates a move towards a more structured framework for age-appropriate access, awareness-building and coordinated stakeholder action.
2. Open and meaningful stakeholder consultations should precede the finalisation of child online safety guidelines or regulatory frameworks. Wider consultation with industry, civil society, educators, parents and children would help build trust, reduce gaps between government and platforms and improve the legitimacy and practical relevance of proposed interventions.

Evidence on Children’s Lived Experiences

3. Children’s internet access in India has expanded rapidly due to affordable smart devices, widespread telecom connectivity and low-cost data (i.e., The discussion noted that 1 GB of data costs approximately ₹9 in India, compared to nearly ₹120–130 in some developed markets).
4. India’s current evidence base on online harms to children remains constrained by limited data availability, uneven quality of studies and restricted access to platform-held data. This makes it difficult to assess the precise scale, severity and nature of risks faced by children online.
5. Official crime statistics may capture only a limited part of the actual scale of online harms affecting children, as many incidents remain unreported or incorrectly reported. This makes it

difficult to rely solely on formal crime data, particularly where technology-facilitated elements of abuse, exploitation, fraud, grooming or harassment are not adequately captured.

6. Child sexual abuse and exploitative material remain among the most serious areas of concern. A global study across 54 countries and around 5,400 respondents found that nearly 54%¹ had faced some form of sexual abuse while growing up, underscoring the need for stronger prevention, detection and response mechanisms.
7. Child online safety interventions should be informed by children's lived online experiences, rather than moving directly to an adult-defined harms-based framing. Children's voices should be included in policy discussions, and such participation must reflect India's diversity, including children from rural areas and different socio-economic backgrounds whose understanding of data, algorithms, AI and online risks may vary significantly.
8. The span of online safety frameworks need to address a variety of age groups focusing on younger children as well as adolescents. Around 15% of active internet users are estimated to fall within the 5–11 age group, with many children accessing digital services through personal, parental or shared devices.

Understanding the Impact of Digital Harms

9. Algorithmic recommender systems were identified as a major risk area. Children engaging with certain content may continue receiving similar or more harmful material, including hate speech, discriminatory narratives, harmful body-image content and other inappropriate content.
10. Children's exposure to online harms can result in a wide spectrum of mental health and behavioural concerns, ranging from depression, anxiety and post-traumatic stress to poor self-esteem, self-blame, avoidance of digital platforms or compulsive checking of harmful online comments. Since only a small proportion of affected children reach clinical support systems, interventions must not be limited to severe cases alone and should address varying levels of distress across schools, families and community settings.
11. A meaningful taxonomy of digital harms affecting children should move beyond rigid offence-based categories. Many online harms overlap and may involve multiple elements, including grooming, identity theft, spyware, fraud, hacking, financial exploitation or circulation of abusive material. A more practical framework would categorise harms based on what is being regulated, including content-related harms, conduct-related harms, contact-related harms, design-related risks and algorithmic accountability.

Learnings from across the Globe for India

12. International experience indicates that age-gating and restriction-based approaches, while well-intentioned, are insufficient as standalone child safety measures.
13. The discussion noted that early evidence from jurisdictions such as Australia and the United Kingdom shows that children may bypass restrictions through VPNs, false age declarations or alternative accounts. Such measures may also have unintended consequences, including loss of

¹ Space2Grow, *Digital Safety of Children: Creating Safe Online Spaces* (2023): https://b58a3240-b788-4b8e-b1ed-39f5ca507ffa.filesusr.com/ugd/d2759d_ca7984fe036945188217ac55a516c1bc.pdf

access to important social networks and support communities, or migration to less regulated and less visible platforms.²

14. The discussion further noted that while blanket social media bans may appear to be an immediate and politically appealing response, they are unlikely to serve as effective evidence-based measures for ensuring child online safety.

Safety-by-Design and Platform Accountability

15. Age-appropriate design was discussed, including default stricter settings for younger users, limits on who can contact children, time-use reminders, protections against unsolicited nude imagery, easier reporting mechanisms and content experiences aligned with age suitability. The discussion highlighted that safety-by-design must translate into concrete product-level choices rather than remain a broad policy principle.
16. Safety-by-design was identified during the discussion as a central principle for child online safety. It was brought out that several platforms already have useful safety features, parental controls and well-being tools in place. However, the discussion emphasised that such safeguards should continue to be embedded at the design and development stage, rather than relying only on post-facto moderation, complaints or retrofitted safety features.³
17. Third-party audits of platforms were identified as an important accountability tool to assess whether platforms can meaningfully identify, mitigate and respond to child safety risks, rather than relying only on internal assurances or self-certification.
18. **Platform-level interventions were recognised as useful but insufficient as a standalone solution for child online safety. The discussion cautioned against treating platforms as a single-point fix, particularly given children's ability to bypass technical controls.**
19. **The discussion also noted that while several platforms have introduced parental controls, safety features and well-being tools, there is limited publicly available information on how widely these safeguards are adopted or used. Greater transparency on the uptake and effectiveness of such tools would help assess whether they are translating into meaningful protection for children.**
20. **Telecom service providers were identified as important actors in the broader child online safety ecosystem, given their position in the digital value chain through which children access the internet. Their role includes working with the government to block identified CSAM-related content and court-directed URLs at the network level, as well as supporting awareness-building through dedicated online resources that explain risks such**

² CCAOI, *The Global Landscape of Age Assurance: Emerging Regulatory Approaches to Child Online Safety and Social Media Governance* (2026):
<https://drive.google.com/file/d/1tDHvLvA80LTpgUBfkon714oLwNCMUcFR/view>

³ Some examples of platform safety resources and parental-control toolkits, including child-safety, teen well-being, intimate-image abuse prevention, sextortion prevention and parental-control resources.
<https://blog.google/intl/en-in/products/platforms/new-ways-to-support-teens-and-families-on-youtube/>
<https://blog.google/intl/en-in/products/platforms/new-ways-were-supporting-health-and-well-being-in-india/>
<https://blog.google/intl/en-in/products/platforms/new-mental-health-wellbeing-tools-built-just-for-teens/>
<https://blog.google/intl/en-in/products/platforms/youtube-and-industry-leaders-announce-the-youth-digital-wellbeing-initiative/>
<https://about.fb.com/news/2024/04/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse/>
<https://www.meta.com/en-gb/safety/topics/bullying-harassment/>
<https://help.netflix.com/en/node/264>

as phishing, cyberbullying and unsafe internet use in simple terms for children and young users.

Age Assurance and Privacy-Preserving Consent

21. Age assurance and verifiable parental consent should be implemented in a privacy-preserving and proportionate manner. The discussion cautioned against identity-linked or Aadhaar-based approaches that could undermine anonymity, increase surveillance risks and effectively require age-gating of all internet users, including adults.
22. The discussion highlighted the practical difficulty of age assurance in India, particularly due to age misrepresentation, shared devices and the limitations of automated age-estimation tools. While AI-based signals may assist in identifying likely age mismatches, such systems are not foolproof and must account for contextual differences, privacy concerns and the risk of inaccurate classification.
23. Age assurance should not evolve in a fragmented or platform-specific manner. Inconsistent implementation across services may create loopholes and weaken the effectiveness of child safety safeguards.

Awareness, Schools and Parental Engagement

24. **Awareness-building was identified as an immediate priority, as existing safety tools, guardrails and guidance materials remain insufficiently known or understood by parents, teachers, children and communities. Public awareness on child online safety should be treated with the same seriousness as awareness campaigns on digital scams and cyber fraud.**
25. Digital safety, online well-being and responsible technology use need to be integrated more meaningfully into school curricula and public education systems. While platform-led and civil society-led awareness initiatives are useful, India-scale impact requires institutional integration through schools and formal learning systems.
26. **Schools and teachers were highlighted as critical actors in the child safety ecosystem, not only as counsellors or technical experts, but as first-line identifiers of distress, harmful online behaviour and emerging mental health concerns. It was also highlighted that it has to be an inter disciplinary effort at schools with all teachers being involved in awareness programmes.**
27. Greater effort is needed to build understanding even among parents about online risks, reporting pathways and responsible digital participation.

Need for a whole-of Government & Society approach

28. **The discussion emphasised that India does not necessarily need more laws to address child online safety, as existing legal frameworks already provide a basis for action.**
29. **To avoid regulatory overlaps and duplicative frameworks in child online safety, the discussion emphasised the need for a clear allocation of institutional roles within a whole-of-government and society approach. While multiple authorities may have legitimate mandates in this space, effective governance would require identifying the lead decision-making authority, clarifying the contribution of other stakeholders, and creating clear coordination markers so that regulation remains coherent for citizens, children, platforms and enforcement agencies.**

30. **Co-regulation and self-regulation were emphasised as necessary, given the dynamic nature of technology and the limitations of state action alone. Responsibility needs to be shared across platforms, civil society, technical experts, parents, schools and the state.**
31. **A balanced child online safety framework could draw on the DPDP model through parental consent, age verification, algorithmic accountability, restrictions on targeted advertising to children, safety-by-design and stronger platform responsibility. Such a framework should remain child-centric, systemic and rights-aware, combining proportionate age assurance, safer and less addictive design features, privacy-preserving verification tools, digital literacy and well-being support, while recognising that several online harms are extensions or amplifications of offline social harms such as misogyny, patriarchy and body-image pressures.**
