KYC for children's age verification — will this be a misguided missile in child protection

September 3, 2024

By Anand Bhushan G V September 4, 2024, 10:27:29 AM IST (Updated)

The National Commission for Protection of Child Rights (NCPCR) has recently proposed to the Ministry of Electronics and Information Technology (MeitY) that a KYC-based system be mandated for verifying children's age under the Digital Personal Data Protection (DPDP) Act.

Share Market Live

View All
Top GainersTop LosersMost Active Price ShockersVolume Shockers

Company	Value	Change	%Change
Asian Paints	3,273.70	₹35.45	1.09
Bajaj Finance	7,317.15	₹72.25	1.00
JSW Steel	932.80	₹7.35	0.79

Company	Value	Change	%Change
Divis Labs	5,137.80	₹16.90	0.33
LTIMindtree	6,165.40	₹16.10	0.26

While the intent to safeguard children in the digital realm is laudable, the method proposed—relying on KYC for age verification—is akin to aiming a missile at one target and striking another, potentially causing unintended collateral damage in the realm of privacy and practicality.

The Privacy Paradox

The irony of the NCPCR's proposal is stark. If this proposal were adopted, the DPDP Act, designed to protect personal data, would paradoxically lead to the mass collection of what otherwise may have been classified as sensitive information from minors.

This approach contradicts the principle of data minimisation, which is foundational to contemporary data protection laws and advocates for the collection of only essential data. Implementing KYC would necessitate gathering extensive personal details from children, thereby creating a large pool of likely sensitive data that could become a prime target for security breaches and misuse.

Questioning Effectiveness

The practical effectiveness of using KYC for age verification is highly dubious. Many children do not possess official documents, and those who do might not have access to them. Furthermore, the system can be easily bypassed; either through the use of an adult's documents or by falsifying data. This method does not ensure the accuracy of the age entered, nor does it protect against other online risks such as exposure to inappropriate content, cyberbullying, or online predation.

A False Sense of Security

There is a significant risk that relying on KYC-based age verification could instill a false sense of security among parents, guardians, and policymakers. Believing that such a system can adequately shield children from the myriad dangers of the internet might lead to complacency. This misplaced trust could divert attention and resources from more effective measures that address a broader spectrum of online safety issues.

Targeting the Wrong Mark

The real issue at hand is ensuring a holistic safe online environment for children. The focus should be on the multifaceted nature of online risks and not just on the binary metric of age. By concentrating on age verification, the NCPCR is not actually solving the core issue of child safety.

Alternative Approaches

A more effective approach would involve a combination of education, robust parental controls, and the development of inherently safer online platforms. Educating children about the risks associated with online activities and teaching them responsible digital behavior is crucial. This empowerment helps them navigate online spaces safely and make informed decisions.

Additionally, technology companies should be encouraged to design products with built-in safety features that do not rely on invasive data collection. Innovations in privacy-preserving technologies and artificial intelligence can help in creating environments that are safe for children without infringing on their privacy.

Conclusion

The NCPCR's proposal to mandate KYC-based age verification under the DPDP Act, while well-intentioned, is a misguided approach to child safety. It not only undermines privacy but also offers questionable effectiveness and diverts attention from more comprehensive safety measures.

As stakeholders in the realms of digital governance and child protection, it is our responsibility to advocate for solutions that respect children's privacy and provide genuine safety. We must aim for a balanced approach that addresses the complexities of online risks, ensuring a secure and nurturing digital environment for all children.

—The author, GV Anand Bhushan, is a Fulbright Scholar and Visiting Professor at Jindal Global Law School. The views expressed are personal.
First Published: Sept 3, 2024 2:50 PM IST

Tags

FeaturesNCPCRZoomed Out