Parental Consent is a Conundrum for Online Child Safety

www.techpolicy.press/parental-consent-is-a-conundrum-for-online-child-safety/

July 22, 2025

Perspective

Jhalak M. Kakkar, Shashank Mohan, Angelina Dash / Jul 22, 2025

Shutterstock

India's data privacy law, the Digital Personal Data Protection Act (DPDP Act), seeks to protect children's data and shield them from data-linked online harms. However, two years after its enactment, this law remains unimplemented as the government has yet to finalize the accompanying rules. As a step forward, the Ministry of Electronics and Information Technology (MeitY) concluded a round of public consultation on the Draft DPDP Rules (Draft Rules) in March this year, but has not published the final rules.

Children increasingly rely on digital services for daily activities like learning, entertainment, and gaming. While the internet is a powerful tool, it also exposes them to risks and harms, including addiction, body image issues, toxic masculinity, and online grooming, which can have debilitating impacts. In response, many global regulators have focused on measures to age-gate the internet through age verification and parental consent. But these mechanisms can limit children's autonomy and self-development, and dilute their rights of free expression and access to information, rights recognized under the United Nations Convention on the Rights of the Child (1989).

In this context, we critically examine India's approach to children's data protection by analyzing the implications of age-gating and highlighting the limitations of age verification and parental consent mechanisms, particularly in the Indian context. We also identify pathways towards a safer internet for children in a manner that respects their autonomy.

Children's data protection under the DPDP Act

The DPDP Act defines children as individuals under 18 years of age, and specifies that their data can only be processed with the consent of parents or guardians (section 9(1)). The Act also prohibits data processing that has detrimental effects on the well-being of children (section 9(2)), and bans tracking, behavioral monitoring, and the use of targeted ads on children (section 9(3)). The government can create exceptions to parental consent requirements for certain types and purposes of data processing (section 9(4,5)). The draft rules for the DPDP seek to provide more details on how digital businesses should obtain verifiable parental consent; however, serious concerns remain about the effectiveness and implications of age verification and parental consent requirements under the Act..

Age verification and its limitations

Online age verification raises several issues, particularly around privacy. As France's National Commission on Informatics and Liberty (CNIL) has found, more effective mechanisms contravene data protection principles while less intrusive methods are less accurate. Age-gating mechanisms are also frequently bypassed, with children misrepresenting their age and presenting themselves as adults. A study from India also found that parents are often aware of such misrepresentation and have even assisted their children in registering on social media platforms.

The requirement of parental consent also rests on the flawed assumption that parents possess the maturity, experience, and technical knowledge to make decisions in their child's best interest. For example, generational disconnects may leave parents unaware of online harms that occur on or outside of popular social media services, such as exposure to sexual content and grooming through popular games like Roblox and Minecraft.

Despite these well-documented shortcomings, the DPDP Act relies heavily on age verification and parental consent. Furthermore, the Draft Rules, too, contain critical weaknesses in enabling the law's core principles.

Implementing verifiable parental consent

To effectively implement verifiable parental consent, the law needs to clearly define how to – (i) identify when a user is a child and verify their age, (ii) establish parental relations for obtaining consent, and (iii) operationalize identity verification while maintaining privacy and autonomy. We examine what the Draft Rules provide for at each of these three stages, highlighting specific concerns and challenges.

1. Identification and age verification of children

Children can easily lie about their age to use a digital service or convince a sibling or relative to help them gain access. The Draft Rules do not address this reality. A primary source of ambiguity lies in whether the rules operate on the presumption of minority, that is, are all users considered children until they prove otherwise, or is the opposite assumed? Both alternatives present significant concerns.

The first scenario would require all users of digital services in India to verify their identity, raising a significant concern about age verification: the collection of excessive and unintended data. This is particularly concerning with the use of hard identifiers like government IDs or financial details, which involve sensitive personal data, including biometric information (as in the case of Aadhaar). The Draft Rules also fail to account for the common practices in Indian households of sharing devices within a family.

While there is little indication that the Indian government intends to tie internet access to identity verification in this manner, it should clearly and formally reject this pathway to remove ambiguity.

The second and more likely scenario, relying solely on self-declaration of age, doesn't change the status quo. In this case, an over-reliance on age verification and parental consent may allow digital businesses to shift the responsibility for children's privacy onto parents. This, in turn, could disincentivize businesses from implementing design interventions and technological safeguards to protect children's data and online safety.

2. Establishing parental relationship and obtaining parental consent

A critical fault line for enabling parental consent lies in establishing the parental relationship, which is also a goal mentioned in the explanatory note published alongside the Draft Rules. The rules simply state that parents must provide reliable proof they are adults. However, there is no guidance on how services are to verify that the adult in question holds a legitimate parental relationship. Can a sibling or relative provide 'parental' consent for children? The absence of clarity here is problematic.

Moreover, both age verification and verification of parental relationship also risk excluding children, whose parents lack government-issued identification.

Another crucial step in the process is obtaining free, specific, and informed consent from parents. Yet, the Draft Rules appear to assume a narrow, digitally literate user base, where parents are well-versed in the relevant laws and policies, and don't rely on their children to navigate digital spaces.

However, a 2022 report found that only 38% of Indian households are digitally literate. In many cases, children and young adults are the first in the family to access popular internet services, and parental consent and supervision are often absent. It is often

children who introduce their parents and elders to digital platforms. In such scenarios, how meaningful can parental or adult consent truly be?

Conversely, the Draft Rules also fail to consider situations in which parental supervision may cross over into surveillance, particularly in the context of gender and other intersectional factors. For instance, research underscores there is a gender-based gap in access to digital services, with girls having less access, thus age verification mechanisms may reinforce and exacerbate this divide.

3. Operational challenges in rule implementation

Rule 10(1) of the Draft Rules introduces another layer of implementation uncertainty. It places an obligation on businesses to adopt "appropriate technical and organisational measures" to collect verifiable parental consent, leaving much ambiguity for them. In an earlier draft of the DPDP Act called the Personal Data Protection Bill, 2019, clause 16(3) outlined certain factors to be considered when specifying the manner of age verification. This included the volume of personal data processed, the proportion of such personal data likely pertaining to children, and the possibility of harm arising to children from such processing of personal data.

However, no such guidance has been articulated under the DPDP Act or the Draft Rules. How will a business determine what qualifies as "appropriate" when implementing age verification and consent mechanisms? Particularly if parental identity is to be established using government IDs, how can principles of purpose limitation and data minimisation be ensured?

Limited guidance in this regard may lead to fragmented implementation, diffused responsibility, and compliance reduced to a box-ticking exercise, ultimately offering little meaningful protection. In contrast, the UK offers clear guidance on implementing age assurance methods in line with data protection principles, requiring fairness, transparency, accountability, and accuracy.

Rule 10(1)(b) attempts to provide direction by introducing a mechanism centred around the use of virtual tokens to establish identity and age, which will be linked to digital lockers. However, without adequate and uniform safeguards, the use of age verification systems raises concerns, owing to vulnerabilities arising from data breaches. For example, India's DigiLocker, which serves as a digital locker for identity verification, was found to put the personal data of users at risk due to a bug in the app. Given such issues, the Draft Rules should have clearly specified the entities "entrusted" with issuing these tokens, and the criteria by which such decisions are made.

Without this, the scope of what is considered "appropriate" is left entirely to the discretion of private entities working with commercial interests. Other jurisdictions, such as the EU,Australia, and New Zealand, have engaged with these considerations by developing legal and accreditation frameworks that define privacy and cybersecurity standards for digital identity systems.

Conclusion

While the statutory requirements of age verification and parental consent themselves are contestable, the Draft Rules represent an opportunity to address some of the concerns outlined in this article. Unfortunately, the current version does not go far enough.

The government should promote parental engagement, encouraging a balance between support, autonomy, and awareness of digital harms. Children, too, must be empowered to navigate the internet safely. However, this cannot mean shifting the entire burden onto child users and their parents. Instead, policies and legal frameworks should embed safeguards like privacy by design and safety by design, not only in age verification systems, but in the design of digital services themselves. This is where regulation has a key role in enabling safer online spaces for children.

As discourse around children's data protection evolves, we need to think more broadly about online safety beyond data protection alone. Child safety measures should be integrated either through amendments to existing laws like the Information Technology Act, 2000, or through new legislation.

The internet is a vital space for children and young adults to learn, explore, and express themselves. As they increasingly interact with AI tools like Meta's Llama and Google's Gemini, now both readily available in India via WhatsApp and the web, new laws and policies must enable the promise of the internet for children while safeguarding their best interests, reflecting both emerging technologies and India's unique demography.