CONSENT, AGE, AND THE BEST INTERESTS OF THE CHILD: EVALUATING SECTION 9 OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT

Dr Ankit Raghuvanshi
Assistant Professor, Department of Law
Harish Chandra PG College, Varanasi

Abstract

India's first statutory framework for children's data protection was constructed by Section 9 of the Digital Personal Data Protection Act 2023 and Rules 10 to 12 of the DPDP Rules 2025. The framework which was built around verifiable parental consent as a standard turns out to be ambitious in design while remaining critically under-specified when it comes to its operation. This paper argues that without providing the definitional clarity or institutional infrastructure necessary for meaningful enforcement, the consent-centric model Parliament has chosen delegates an unworkable technical and legal burden to Data Fiduciaries. It argues that fundamentally, the best interest of the child cannot be protected by centering parental consent; rather , it produces a framework that protects parental authority rather than children. The paper identifies three structural deficits and proposes targeted legislative reforms drawing on comparisons with the GDPR, the UK's Age Appropriate Design Code, and the US Children's Online Privacy Protection Act.

I. INTRODUCTION

In a digital economy, children cannot merely be the incidental users. Rather in most situations they are seen as the intensively monetisable participants . Various forms of data fiduciaries like the Social media platforms, ed-tech intermediaries, online gaming operators, and health applications, collect data with such depth and breadth that even most adults would find it alarming if they understood scale and granularity. The day a child picks up a device, his profiling begins on the internet. This includes logging of data relating to emotional patterns, attention responses and extends to social relationships. This information gets processed, and sold as data for the advertisers which operate in ways which are difficult to comprehend, making it difficult to have oversight both by the parents and the regulators.

Section 9 of the Digital Personal Data Protection Act 2023 was brought into force by the parliament taking into account this issue. In order to process a child's personal data the provision of the act requires Data Fiduciaries to obtain before processing any data, verifiable parental consent further this bars targeted advertising directed at them, prohibits tracking and behavioural monitoring of children. In order to make the mechanism more robust, The DPDP Rules 2025 through Rule 10 add the operational layer as it specifies the verification mechanics, Further Rule 11 extends the framework to persons with disability, and Rule 12 with the Fourth Schedule carves out exemptions for healthcare and educational providers.

The paper tries to raise the question regarding the adequacy of the mechanism . The answer for now is a no. The more detailed answer requires going through the internal working of Section 9 thoroughly, keeping in view the rights of the children and ensuring its compliance with the international commitments. The paper tries to put into focus a twofold question. First, it questions the structure of the verifiable consent, without actually specifying the means of doing it, it provides for a legal obligation. The technical infrastructure which it requires is neither universal nor goes against the values of the constitution. Second, the framework which

bases itself around parental consent instead of focusing meaningfully on the interests of the child fails to identify the problem it aims to solve.

II. THE ARCHITECTURE OF SECTION 9: FOUR LAYERS

A reading of Section 9 of the DPDP Act gives us the understanding that this provision of the Act has been depicted in a dense manner. It moves in multiple realms which extends to data protection law, child rights law, administrative law, and constitutional doctrine. An understanding can be developed when read in layers.

Section 9(1) provides for the core obligation being verifiable consent of the parent or the lawful guardian that needs to be there before the actual processing of the personal data of a child, which Data Fiduciary must obtain. Section 2(f) defines 'Child' as any individual under eighteen years of age. India, rather wisely has chosen eighteen as the age before which, verifiable consent would be needed. This is significantly more protective than the GDPR's Article 8, which sets the default digital consent age at sixteen. It is also considerably higher than COPPA's threshold of thirteen. The decision to use eighteen has received less analytical attention than it deserves. It means that the entire data economy's interaction with minors — from a sixteen-year-old's Zomato account to a seventeen-year-old's Instagram profile — is technically subject to parental consent requirements. Whether that is practically enforceable is a different question, and one the Act does not seriously engage.

The second layer consists of absolute prohibitions. Section 9(2) bars 'any processing likely to cause detrimental effects on a child's well-being' . Section 9(3) prohibits tracking, behavioural monitoring, and targeted advertising directed at children. These prohibitions cannot be overridden by parental consent — a parent cannot authorise a platform to behaviourally track her child. This is a stronger position than the GDPR's, which addresses targeted advertising to children through the ePrivacy framework rather than the data protection regulation itself. It is also, potentially, the most litigated provision in the Act: 'detrimental effect on well-being' is not defined, and determining what processing meets that threshold will require regulatory guidance that the Act does not currently anticipate.

The third layer is the exemption regime. By virtue of Section 9(4) the Central Government is empowered to exempt certain classes of Data Fiduciaries and purposes from both the parental consent obligation and the tracking prohibition. Rule 12 operationalises this through the Fourth Schedule. Part A exempts five categories of fiduciary: clinical establishments, allied healthcare professionals, educational institutions, crèches and child day care centres, and transport providers engaged by educational institutions. Part B however provides for exemption of six purposes, this would include creation of an email account, tracking location in real-time for child safety, this also includes verification processing. A careful look at these exemptions, give us an understanding of their nature being defensible. A combined reading of these points out to the categories of fiduciaries which would have a bearing on the activity of the children. When it comes to the application of these exemptions together, the actual extent of the parental consent standard as envisaged by the provisions gets reduced.

Section 9(5) provides for the fourth layer which deals with the point of age-threshold flexibility. Upon the Central Government being ensured by the Data Fiduciary about the verifiable safety of Children's data, the Central Government by notification provide for an age below eighteen, beyond which that data fiduciary would be exempt from the purview of Sections 9(1) and 9(3). Upon reading this section one could easily argue that this Section would require a greater attention. It even goes a step further by creating platform-specific age thresholds, where a social media platform could allow users above age fifteen and not require verifiable parental consent for such, whereas for another platform such age could still be required to abide by the mandated age of eighteen. The differential treatment of children based on which platform they happen to use raises serious concerns that Part V of this paper addresses directly.

III. THE VERIFIABLE CONSENT STANDARD: RULE 10 AND ITS GAPS

Rule 10 is where the legal obligation meets operational reality, and the gap between the two is considerable. The Rule requires Data Fiduciaries to adopt 'appropriate technical and organisational measures to obtain verifiable parental consent before processing a child's data' Verification must be by reference to one of two mechanisms: 'reliable details of identity and age available with the Data Fiduciary', or details provided through a virtual token mapped to the individual's identity, issued by an authorised entity such as a Digital Locker service provider.

Three structural gaps in this standard demand attention.

The first is the absence of any prescribed verification methodology. 'Appropriate technical and organisational measures' is the standard language of technology-neutral regulation. In the context of verifiable parental consent, it is also operationally empty. A small ed-tech startup with five thousand registered users and a platform with fifty million users face identical legal obligations under Rule 10 but radically different technical capacities. The aim of the rule seems to be to create a sense of formal equality but, in its function it leads to substantive inequality. The approach used by COPPA comes handy as the FTC puts a statutory condition to specify what constitutes 'reasonable methods' for the purpose of verification. This is done with the help of a sliding scale which moves with the amount of sensitivity involved with the data and amount of apparent harm.On the other hand Rule 10 does not offer an equivalent sliding scale, also it does not provide for a regulator guidance for minimum standard. To the point where these conditions do not find a way to the legislation, these obligations would have no effect .

The second gap is the infrastructure problem. Rule 10's virtual token mechanism depends on an ecosystem of 'authorised entities' capable of issuing identity and age tokens. In practice, this points toward DigiLocker and, ultimately, Aadhaar-based authentication. DigiLocker penetration is uneven, particularly in rural India and among lower-income households — precisely the populations whose children are most vulnerable to exploitation in digital markets. More significantly, the Supreme Court's Aadhaar judgment in 2019 struck down Section 57 of the Aadhaar Act as unconstitutional to the extent that 'it permitted private entities to use Aadhaar-based authentication'. A parental consent verification system that in practice requires Aadhaar authentication for its virtual token mechanism may therefore face a direct constitutional challenge. The Rules do not engage with this tension, and the Act provides no alternative.

The third gap concerns Rule 11 and persons with disability. Rule 11 extends the verifiable consent framework to individuals with disability who have a lawful guardian, requiring Data Fiduciaries to verify that the guardian is appointed by a court, a designated authority, or a local level committee under the Rights of Persons with Disabilities Act 2016 or the National Trust Act 1999. This is a more specific and more demanding standard than Rule 10's adult-identity check — and the information required to make it (court orders, designation certificates) is not typically in the possession of a Data Fiduciary. The provision is well-intentioned but practically aspirational. Under the RPWD Act, any guardian who is not carrying their appointment order during the creation of the account of the family member, there is no specific guidance on how it should be carried on.

IV. COMPARATIVE ANALYSIS: THREE MODELS

The challenge with regard to protection of personal data of children is not something which only India is dealing with, while the international experience could be instructive for India not because it provides a more experienced outlook, but also it provides for a ready set of assumptions to work with while dealing with such an issue. Also such assumptions have been tested through multiple legal regimes. Irrespective the challenges placed before India are more nuanced mostly because of the diversity that we encounter in India.

The age for providing consent under GDPR has been set to Sixteen, while the different regimes under it have even mandated thirteen years as well . This however is not applicable for all data processing, rather it finds its application in 'information society services' which includes online platforms and digital services. The standard provided by the European Data Protection Board based on the risk based assessment instead of a single prescribed method requires the GDPR to put in a 'reasonable effort' for the verification of age and

ensuring parental consent. This comes with the flexibility of Rule 10 but has its own challenges which in absence of the prescribed methods, force the larger platforms for self declaration which when it comes to its application, appears to be no declaration at all. The GDPR's parental consent framework has been widely criticised for this reason.

The UK's Age Appropriate Design Code (the Children's Code), introduced under Section 123 of the Data Protection Act 2018, takes a fundamentally different approach. Insted of requiring parental consent before the processing, it requires Data Fiduciaries to design their services to protect children by default. The Code specifies fifteen standards: data minimisation, geolocation off by default, no nudge techniques, high privacy as default, and others. This privacy-by-design model places the burden on the platform, not on parents whose technical literacy may be no match for the platforms their children use. It also reflects a more honest assessment of where the power actually lies in the relationship between a child, her parents, and a platform with billions in engineering resources. The UK Code is not without its own difficulties — age assurance technology remains imperfect and the compliance burden on smaller services has been criticised — but its underlying logic is sounder than the consent model.

COPPA applies to children under thirteen and 'requires verifiable parental consent before collecting personal data'. What distinguishes COPPA from Rule 10 is the FTC's practice of issuing detailed operational guidance on acceptable verification methods, updated as technology changes. Platforms know what they must do. The FTC enforces: Meta has been fined, TikTok has been fined, and YouTube settled for $170 million. The deterrent is credible because the standard is clear and the enforcement body has the will and the resources to act. India's DPDP Rules provide neither the clarity nor the institutional context for equivalent enforcement.

What unifies the UK Code and, to a degree, COPPA's enforcement practice is a willingness to ask a question the DPDP Act does not ask: what would actually lead up to ensuring the best interests of this child? In an attempt to answer the same, the UN Committee on the Rights of the Child, in its General Comment No 25, has stated that ensuring the best interest of the child must be the primary consideration in the digital environment, and that data protection frameworks should be designed accordingly. The UNCRC's Article 3(1) standard is not aspirational guidance — it is a treaty obligation that India accepted when it ratified the Convention in 1992. Section 9 of the DPDP Act does not talk about the best interest of the Child. The Srikrishna Committee's 2018 report had recommended it. Its absence from the final Act is not an oversight. It is a choice, and it is the wrong one.

V. THE CONSTITUTIONAL DIMENSION

Two constitutional arguments run through this paper and deserve explicit statement.

The first concerns the child's own right to privacy. Puttaswamy recognised 'privacy as a fundamental right of every individual under Article 21'. A child is an individual. The question then is whether Section 9's framework protects the child's privacy or whether it substitutes parental authority for platform authority. Section 9(2)'s prohibition on processing likely to cause detrimental effect on a child's well-being gestures toward a child-centric standard, but the Act provides no definition of 'detrimental effect' and no mechanism for the child's own interests to be represented in the parental consent transaction. A parent can, under the Act as written, provide consent to processing that serves the parent's interests or the platform's interests without any inquiry into whether it serves the child's. The Supreme Court in Bachpan Bachao Andolan recognised children as a specially vulnerable class requiring heightened constitutional protection. Section 9 acknowledges this vulnerability at a formal level. It does not address it as a structural one.

The second constitutional problem is Section 9(5)'s age-threshold flexibility. Allowing the Central Government to notify platform-specific age thresholds below eighteen means that two children of the same age can be in entirely different legal positions based solely on which platform they use — one protected by the full parental consent standard, another exempt from it by executive notification. This differential treatment is not based on any characteristic of the children themselves. It is based on the Central Government's assessment of whether a particular fiduciary has made its processing 'verifiably safe.' That assessment is made without Parliamentary oversight, without a defined standard of safety, and without any requirement of proportionality. Article 14's guarantee of 'equal protection requires that differential treatment be based on an intelligible

differentia and bear a rational nexus to the legislative objective,. A fiduciary-specific age threshold determined by executive satisfaction with unspecified safety standards is hard to defend against that test.

There is also a third, less obvious constitutional dimension. India ratified the UNCRC in 1992. Under Article 253 of the Constitution, Parliament has the power to legislate for the purpose of implementing international treaties. The UNCRC's Article 3(1) best interests standard is a binding treaty obligation. When Parliament legislates in the area of children's rights, as it has done in Section 9, the question arises whether that legislation can be challenged for failing to give effect to a treaty obligation India has accepted. The matter is not settled, and this paper does not suggest the challenge would succeed. But the absence of any best interests standard in Section 9 creates a tension between the Act and India's international legal commitments that the Government should not be comfortable leaving unresolved.

VI. REFORM PROPOSALS AND CONCLUSION

The application of three reforms would substantially overhaul the framework, without requiring significant reconstruction.

Rule 10 needs to prescribe a tiered verification methodology. Large platforms — those above a threshold of registered users or processing volume to be set by the Data Protection Board — should be required to use biometric or DigiLocker-based verification, or an equivalent standard that the Board specifies. Smaller Data Fiduciaries should face a lighter standard, calibrated to their technical capacity and the sensitivity of the data they process. The current 'appropriate measures' formulation delegates the standard-setting function to individual fiduciaries, each of whom has an obvious commercial incentive to set it as low as possible. That is not regulation. It is the appearance of regulation.

Section 9 should be amended to incorporate a 'best interests of the child' standard alongside the parental consent requirement. The standard should be drawn from Article 3 of the UNCRC and should operate as a constraint on parental consent: consent given by a parent cannot authorise processing that is not in the best interests of the child. This is not a novel concept — it is already implicit in Section 9(2)'s prohibition on processing that causes detrimental effects on well-being. What is missing is an explicit statement that the child's interests are the primary analytical frame, and an institutional mechanism — potentially through the Data Protection Board's guidance function — for making that frame operational.

Section 9(5)'s age-threshold flexibility should be made subject to Parliamentary approval rather than executive notification alone. The ability to lower the effective age of consent for a class of children through a Government notification is a substantial derogation from a protective legislative standard. It should require the same democratic deliberation that enacted the standard in the first place. This reform is consistent with the general principle that executive powers to derogate from fundamental rights require legislative authorisation, not merely legislative delegation.

The DPDP Act 2023 does something important: it recognises, for the first time in Indian law, that children's personal data deserves specific statutory protection. That recognition is not nothing. But the framework Parliament has built around it — consent-centric, operationally under-specified, constitutionally unmoored from the best interests standard, and practically dependent on digital infrastructure that does not yet reach every Indian child — is less than the recognition demands.

The standard India needs is not simply one that protects parental authority over children's data. It is one that asks, at every decision point, what protection this particular child actually needs in this particular digital environment. That question is harder to answer than 'did the parent click yes?' It is also the right question.