THE PATERNALISM PARADOX: RETHINKING INDIA'S CONSENT-CENTRIC APPROACH TO CHILDREN'S DATA PROTECTION UNDER THE DPDP ACT, 2023

Vaishali Dilip Parikh*

ABSTRACT

This article subjects the children's data protection architecture erected by Section 9 of the Digital Personal Data Protection Act, 2023, and Rules 10–12 of the Digital Personal Data Protection Rules, 2025, to sustained critical scrutiny. It advances the claim that India's consent-centric regulatory paradigm anchored in mandatory verifiable parental consent and a blanket age-gate at eighteen years fundamentally misidentifies the regulatory target. The genuine peril for children in the digital ecosystem originates not at the point of entry but within platform architectures: in design choices that enable profiling, behavioural manipulation, and data exploitation. Drawing upon the constitutional privacy jurisprudence of Puttaswamy, a comparative survey of the GDPR, COPPA, and the United Kingdom's Age Appropriate Design Code, and the evolving-capacities doctrine articulated by the UN Committee on the Rights of the Child in General Comment No. 25, this article proposes a four-pillar alternative: graduated age thresholds calibrated to developmental capacity, a statutory platform duty of care, outcome-based regulation enforced through audit, and the institutionalisation of digital literacy as public infrastructure.

Keywords: DPDP Act 2023, Children's Data Protection, Verifiable Parental Consent, Age Verification, COPPA.

INTRODUCTION

Imagine a fifteen-year-old girl in the Vidarbha region of eastern Maharashtra. Her widowed mother, an agricultural labourer earning a daily wage, owns a single shared smartphone. The girl wishes to enrol in a free online mathematics course offered by one of India's prominent educational-technology platforms. Under the Digital Personal Data Protection Act, 2023

('DPDP Act' or 'the Act'), the platform must, before processing any of her personal data, obtain 'verifiable consent' from her mother.[1] To trigger that obligation, the platform must first establish that she is below eighteen, the age at which the Act defines a 'child'.[2] It must then identify and authenticate her mother, and secure her informed, recorded consent through 'appropriate technical and organisational measures' prescribed under Rule 10 of the DPDP Rules, 2025.[3] The mother has never used a digital identity platform. Her Aadhaar record contains no machine-readable link to her daughter. The Aadhaar Demographic API returns age data only in decadal bands, unable to distinguish a seventeen-year-old from a twenty-two-year-old.[4] The girl is barred from an educational resource that her urban peers access without impediment.

This vignette is neither speculative nor exceptional. India is home to over 430 million individuals below the age of eighteen, a population exceeding that of the entire European Union.[5] At the beginning of 2025, approximately 806 million people in India were using the internet, with penetration standing at 55.3 per cent.[6] Section 9 of the DPDP Act, enacted on 11 August 2023 and operationalised through the DPDP Rules notified on 13 November 2025,[7] creates what is, on paper, the most stringent children's data protection framework anywhere in the world. It mandates verifiable parental consent for all processing of children's data, imposes unconditional prohibitions on tracking and behavioural advertising directed at minors, and sets the definitional threshold of childhood at eighteen years.[8][9] Penalties for non-compliance can reach two hundred and fifty crore rupees.[10]

This article advances a disruptive contention: India possesses the most protective children's data regime on statute and possibly the least enforceable one in lived reality. The disjunction is not administrative but structural. The global orthodoxy on children's data protection instantiated in the United States' Children's Online Privacy Protection Act,[11] the European

[1] UNICEF Data, 'How Many Children Are There in India?' (2025): 430,108,317 individuals under 18.
[2] Digital Personal Data Protection Act 2023, s 2(f).
[3] Cyril Shroff and Arjun Goswami, 'Children and Consent under the Data Protection Act: A Study in Evolution' (India Corporate Law/Cyril Amarchand Mangaldas, August 2023).
[4] Ashok Hariharan, 'Challenges of Age-Gating: Why Verifiable Parental Consent Has Become a Major Hurdle in India' (ABP News, 22 October 2024).
[5] UNICEF Data, 'How Many Children Are There in India?' (2025): 430,108,317 individuals under 18.
[6] DataReportal, 'Digital 2025: India' (25 February 2025) https://datareportal.com/reports/digital-2025-india accessed 15 June 2026.
[7] Digital Personal Data Protection Rules 2025, GSR 846(E), notified 13 November 2025.
[8] UNICEF Data, 'How Many Children Are There in India?' (2025): 430,108,317 individuals under 18.
[9] Digital Personal Data Protection Act 2023, s 9(3).
[10] Digital Personal Data Protection Act 2023, s 33.
[11] Children's Online Privacy Protection Act 1998 (US), 15 USC §§ 6501–6506; COPPA Rule, 16 CFR pt 312.

Union's General Data Protection Regulation,[12] and now India's DPDP Act has crystallised around what this article terms the 'consent-at-the-gate' paradigm: the conviction that children's data is best safeguarded by controlling who enters the digital space and on whose authority. The paradigm asks: 'Has a parent given permission?' The more penetrating question, this article insists, is: 'Once the child is inside the digital environment, what does the platform do with the data it collects and how does its architecture shape the child's experience?'

A regime that conditions digital access on parental authorisation produces three compounding failures. It excludes children who most urgently require digital resources because their parents lack the literacy, devices, or documentation to furnish verifiable consent. It paradoxically expands data collection because age verification necessitates gathering additional personal information from every user. And it deflects regulatory attention from platform architecture, the actual locus of harm, onto households, which constitute the weakest node in the enforcement chain. The consent-at-the-gate paradigm shields children from the digital world. It does not shield them within it. The distinction is not rhetorical; it is constitutionally and operationally decisive.

This article unfolds as follows. Part II dissects the legislative architecture of Section 9 and Rules 10–12, mapping the obligations, prohibitions, and exemptions that compose India's children's data framework. Part III identifies five structural failures of the consent-at-the-gate paradigm in the Indian setting. Part IV traces comparative trajectories, examining how the United States, the European Union, the United Kingdom, and Australia have navigated children's data protection with particular focus on the UK's Age Appropriate Design Code as an exemplar of the alternative 'safe-by-design' approach.[13] Part V interrogates the constitutional dimensions, drawing on the privacy right articulated in Puttaswamy,[14] the right to education under Article 21A,[15] freedom of expression under Article 19(1)(a),[16] and the UN Committee on the Rights of the Child's evolving-capacities doctrine elaborated in General

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1, art 8.
[13] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.
[14] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[15] Constitution of India, art 21A.
[16] Constitution of India, art 19(1)(a).

Comment No. 25.[17][18] Part VI surveys sectoral dislocations. Part VII proposes a four-pillar alternative. Part VIII concludes.

THE LEGISLATIVE MACHINERY: DECODING SECTION 9 AND RULES 10–12

The children's data protection regime constructed by the DPDP Act rests on three normative pillars: mandatory parental authorisation, a harm-based processing prohibition, and an unconditional surveillance bar. Each is established in Section 9 and operationalised by the Rules. This Part examines the architecture with the analytical precision necessary to expose its structural pressure points.

The Gatekeeping Mandate: Verifiable Parental Consent: Section 9(1) stipulates that a Data Fiduciary shall, before processing 'any' personal data of a child, obtain verifiable consent from the parent or lawful guardian 'in such manner as may be prescribed.'[19] The operative term is 'any'; the obligation encompasses all processing, not merely the collection of sensitive categories. The qualifier 'verifiable' demands authentication exceeding mere self-assertion; a website checkbox reading 'I confirm I am over 18' does not satisfy the statutory threshold.[20] The Explanation to Section 9(1) clarifies that 'consent of the parent' encompasses lawful guardians where applicable.

Rule 10 operationalises this mandate through four illustrative verification pathways.[21] First, the child voluntarily discloses minority status and the fiduciary subsequently verifies the parent's identity. Second, a parent directly opens the user account on the child's behalf. Third, the parent's identity is confirmed through reliable identity details already held by the fiduciary. Fourth, verification proceeds through voluntarily provided identity details or a virtual token issued by a regulated entity, including through the Digital Locker framework.[22] The first two scenarios presuppose that the child will cooperate in triggering the very mechanism designed to circumscribe the child's own digital autonomy, a logical paradox that commentators have

[17] UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25 (2 March 2021).
[18] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, arts 3, 5, 12, 13, 16, 17.
[19] Digital Personal Data Protection Act 2023, s 9(1).
[20] Cyril Shroff and Arjun Goswami, 'Children and Consent under the Data Protection Act: A Study in Evolution' (India Corporate Law/Cyril Amarchand Mangaldas, August 2023).
[21] Digital Personal Data Protection Rules 2025, r 10.
[22] Vikram Jeet Singh, Prashant Mara and Arushi Mukherji, 'The Emerging Contours of "Verifiable Parental Consent" Under India's New Data Privacy Law' (BTG Advaya, July 2025).

identified as structurally incoherent.[23] The fourth scenario is technologically promising but depends on infrastructure that, as IT Minister Ashwini Vaishnaw himself acknowledged, remains a work in progress; he conceded that verifiable parental consent constitutes a 'global problem.'[24]

The Harm Standard Without a Measuring Stick: Section 9(2): Section 9(2) provides that a Data Fiduciary shall not undertake processing of personal data that is 'likely to cause any detrimental effect on the well-being of a child.'[25] This prohibition is distinct from and supplementary to the consent mandate: even where a parent has provided fully verifiable consent, processing that injures the child's well-being remains unlawful. The provision's normative reach is deliberately expansive; it targets addictive interface design, algorithmic amplification of distressing content, profiling that facilitates social exclusion, and manipulative techniques exploiting developmental vulnerabilities. Yet the phrase 'detrimental effect on the well-being' is defined nowhere in the Act, the Rules, or any subordinate instrument.[26] Without sector-specific codes of practice, adjudicatory precedent from the Data Protection Board of India, or formal regulatory guidance, Data Fiduciaries cannot determine ex ante where legitimate processing concludes, and harmful processing commences. The provision functions, at present, as an aspirational declaration rather than an actionable compliance standard.

The Unconditional Surveillance Prohibition: Section 9(3): Section 9(3) imposes a categorical prohibition: no Data Fiduciary may undertake tracking, behavioural monitoring, or targeted advertising directed at children.[27] The prohibition is unconditional and cannot be displaced by parental consent. A children's gaming application cannot profile a minor's usage patterns for advertising purposes. A social media service cannot construct behavioural models of users below eighteen. This constitutes the most aggressive anti-surveillance mandate in global data protection law; neither the GDPR nor COPPA contain an equivalent blanket prohibition on all tracking and behavioural monitoring of individuals under eighteen.[28][29] The provision is normatively compelling, yet it creates an enforcement paradox that Part III

[23] Ashok Hariharan, 'Challenges of Age-Gating: Why Verifiable Parental Consent Has Become a Major Hurdle in India' (ABP News, 22 October 2024).
[24] 'Tech Solutions Can Help Verify Kids' Age: Vaishnaw' Hindustan Times (New Delhi, 7 January 2025).
[25] Digital Personal Data Protection Act 2023, s 9(2).
[26] Prashanth Shivadass, Shri Gayathri and Ananya K, 'Indian Perspective on Protecting Children's Personal Data' (Law.Asia, 3 April 2025).
[27] Digital Personal Data Protection Act 2023, s 9(3).
[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1, art 8.
[29] Children's Online Privacy Protection Act 1998 (US), 15 USC §§ 6501–6506; COPPA Rule, 16 CFR pt 312

elaborates: to enforce the ban on tracking children, platforms must first identify which users are children — and that identification itself requires a form of data-driven surveillance that brings the exercise uncomfortably close to the conduct Section 9(3) prohibits.

Executive Discretion as Regulatory Safety Valve: Sections 9(4)–(5): Acknowledging the breadth of its own prescriptions, the Act incorporates executive escape mechanisms. Section 9(4) authorises the Central Government to prescribe categories of Data Fiduciaries or processing purposes for which the consent and tracking-ban requirements shall not apply, subject to prescribed conditions.[30] Section 9(5) takes a further step: where the Government is satisfied that a specific Data Fiduciary processes children's data 'in a manner that is verifiably safe,' it may designate an age above which that particular fiduciary is exempted from the Section 9(1) and 9(3) obligations.[31] This is a remarkable legislative design choice: it permits fiduciary-specific, risk-calibrated derogation, the precise kind of graduated mechanism this article argues should constitute the general regulatory framework rather than a narrow exception. As of mid-2026, however, the Central Government has not exercised this power, and no criteria for assessing 'verifiably safe' processing have been publicly specified.[32]

Narrow Exemptions, Severe Consequences: Rule 11 of the DPDP Rules, read with Part A of the Fourth Schedule, carves out a constrained exemptive perimeter.[33] Exempted classes are limited to clinical establishments, mental health establishments, healthcare professionals, and allied healthcare professionals and only where processing is restricted to health services necessary for the child's protection. Part B identifies exempt purposes, including processing necessary for the safety of, or provision of assistance to, children. Rule 12 extends parallel safeguards for persons with disabilities who have lawful guardians.[34] Critically, this exemptive perimeter does not encompass educational institutions, EdTech platforms, social media services, or gaming companies, the sectors that process children's data at the most formidable scale.[35] India's largest educational-technology platforms serve tens of millions of users below eighteen, yet fall entirely beyond the Fourth Schedule's protective carve-outs. Section 33 of

[30] Digital Personal Data Protection Act 2023, s 9(4)–(5).
[31] Digital Personal Data Protection Act 2023, s 9(4)–(5).
[32] Ministry of Electronics and Information Technology, Press Release on DPDP Rules Notification (Press Information Bureau, 14 November 2025).
[33] Jhalak M Kakkar, Shashank Mohan and Angelina Dash, 'Parental Consent is a Conundrum for Online Child Safety' (TechPolicy.Press, 22 July 2025).
[34] Digital Personal Data Protection Rules 2025, GSR 846(E), notified 13 November 2025.
[35] Jidesh Kumar and Aurelia Menezes, 'Children's Data Under the DPDP Act, 2023 and DPDP Rules, 2025: The New Compliance Frontier' (King Stubb & Kasiva, April 2026).

the Act prescribes monetary sanctions reaching two hundred and fifty crore rupees for violations involving children's data.[36]

FIVE STRUCTURAL FAILURES OF THE CONSENT-AT-THE-GATE PARADIGM

Having mapped the statutory architecture, this Part marshals evidence for five structural deficiencies that render the consent-at-the-gate paradigm unworkable in the Indian digital ecosystem. These failures are not peripheral implementation difficulties that further subordinate legislation might remedy. They are embedded in the conceptual foundations of the model itself.

The Impossibility of Meaningful Consent at Demographic Scale: India harbours roughly 430 million persons who have not yet attained the age of eighteen.[37] At the start of 2025, over 806 million Indians were connected to the internet, with penetration expanding rapidly in semi-urban and rural districts.[38] The consent model postulates that for every digital transaction involving a minor every lesson viewed on an EdTech platform, every social media profile created, every game session initiated, every search query executed a parent or guardian will be identified, authenticated, and will furnish specific, informed, recorded consent. When one considers that an ordinary adolescent may interact with a dozen or more Data Fiduciaries in a single day, each constituting a separate fiduciary under the Act, the logistical implausibility of universal parental consent becomes apparent.

The consequence is what privacy scholars describe as 'consent fatigue': a phenomenon in which the sheer volume of consent requests erodes the deliberative quality of each consent act, reducing what ought to be an exercise in informational self-determination to a reflexive, unreflective click.[39] Kakkar, Mohan, and Dash have argued compellingly that equating parental proxy consent with genuine child protection conflates a procedural formality with a substantive safeguard.[40] At the population scale at which India operates, this conflation is not merely

[36] Digital Personal Data Protection Act 2023, s 33.
[37] UNICEF Data, 'How Many Children Are There in India?' (2025): 430,108,317 individuals under 18.
[38] DataReportal, 'Digital 2025: India' (25 February 2025) https://datareportal.com/reports/digital-2025-india accessed 15 June 2026.
[39] Jhalak M Kakkar, Shashank Mohan and Angelina Dash, 'Parental Consent is a Conundrum for Online Child Safety' (TechPolicy.Press, 22 July 2025).
[40] Jhalak M Kakkar, Shashank Mohan and Angelina Dash, 'Parental Consent is a Conundrum for Online Child Safety' (TechPolicy.Press, 22 July 2025).

imperfect; it is systemically misleading, creating a veneer of compliance that masks the absence of meaningful protection.

The Privacy-Defeating Paradox of Age Verification: To enforce the parental consent requirement, a Data Fiduciary must first determine whether a given user falls below the age of eighteen. Since the platform cannot know this in advance, compliance effectively mandates that every user, adult and minor alike, submit to some form of age verification. As Ahuja and Rawat have framed the dilemma: 'Age Checks or Privacy Wrecks?'[41] Hard verification mechanisms government-issued document checks, biometric scans, Aadhaar-based demographic queries require the platform to collect and process precisely the categories of sensitive personal data that the Act purports to shield. Facial age-estimation technologies are both intrusive and disproportionately unreliable for younger cohorts and non-Western populations. Soft methods, principally self-declaration, are trivially circumvented. France's data protection authority has squarely acknowledged this paradox: more effective age-verification tools contravene data-minimisation principles, while less intrusive methods lack the precision to be meaningful.[42] The DPDP Act thus generates a regulatory environment in which safeguarding children's privacy demands the expanded collection of personal data from everyone a structural contradiction that undermines the Act's foundational objective.

The Digital Literacy Inversion: The consent-at-the-gate model rests upon an unstated premise: that the parent furnishing consent possesses superior digital competence relative to the child and can evaluate the implications of data processing on the child's behalf. In India, this premise is demonstrably false for a large proportion of the population. The 2022 Oxfam India Inequality Report established that only 38 per cent of Indian households meet basic digital literacy standards.[43] In numerous families, it is the children who are the first digital adopters, introducing their parents and grandparents to smartphones, applications, and internet platforms.[44][45] In such households, the consent model demands that the less digitally informed party authorise data processing on behalf of the more digitally informed party. Rather than

[41] Kinjal Ahuja and Ashish Rawat, 'Age Checks or Privacy Wrecks? Decoding Rule 10 of DPDP Draft Rules, 2025' (NUALS Law Journal, August 2025).
[42] Jhalak M Kakkar, Shashank Mohan and Angelina Dash, 'Parental Consent is a Conundrum for Online Child Safety' (TechPolicy.Press, 22 July 2025).
[43] Oxfam India, India Inequality Report 2022: Digital Divide (Oxfam India 2022).
[44] Aparajita Bharti, Nikhil Iyer, Rhydhi Gupta and Sidharth Deb, 'Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023' (The Quantum Hub, 2024).
[45] Jhalak M Kakkar, Shashank Mohan and Angelina Dash, 'Parental Consent is a Conundrum for Online Child Safety' (TechPolicy.Press, 22 July 2025).

enhancing protection, this inverted hierarchy generates a legal fiction: the formal satisfaction of a statutory requirement that, in substance, provides no meaningful safeguard against the data practices the child actually encounters.

The Shared-Device Conundrum: India's digital landscape is characterised by a phenomenon largely absent from the regulatory imagination of Western jurisdictions: widespread device-sharing within households. Industry estimates suggest that approximately forty per cent of Indian internet-user households share a single smartphone among multiple family members, with the proportion climbing substantially in rural areas.[4647] The DPDP Act's age-verification and consent architecture presupposes that each user possesses a distinct device, a distinct digital identity, and a distinct user account. On a shared device, per-user age-gating is technically unachievable without creating individualised user profiles, which itself requires collecting personal data from each potential user, including minors, before any consent mechanism can be initiated. The regulatory framework thus confronts a circular dependency: it cannot determine whether consent is required without first collecting the very data that cannot be collected without consent.

The Circumvention Inevitability: The most practically devastating critique of the consent-at-the-gate model concerns its trivial circumventability. Two of Rule 10's four illustrative scenarios assume that the child will voluntarily disclose their minority status.[48] A teenager who has been denied access to a social media platform or a gaming application because the consent requirement has not been satisfied has every incentive to misrepresent their age. Self-declaration is the age-gating mechanism most frequently deployed by platforms globally, and it is the mechanism most effortlessly defeated. An Aadhaar PDF document can be digitally altered in a matter of minutes, a fact known to any technically capable adolescent.[49]

Even where platforms attempt harder verification, the underlying infrastructure does not currently support it at the requisite granularity. The Aadhaar Demographic API returns age information only in decadal bands, rendering it incapable of distinguishing a seventeen-year-

[46] Ashok Hariharan, 'Challenges of Age-Gating: Why Verifiable Parental Consent Has Become a Major Hurdle in India' (ABP News, 22 October 2024).
[47] Aparajita Bharti, Nikhil Iyer, Rhydhi Gupta and Sidharth Deb, 'Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023' (The Quantum Hub, 2024).
[48] Nikhil Pahwa, 'What's Missing With Parental Consent For Children In India's Data Protection Rules' (MediaNama, November 2025).
[49] Nikhil Pahwa, 'What's Missing With Parental Consent For Children In India's Data Protection Rules' (MediaNama, November 2025).

old from a twenty-three-year-old with the precision that Section 9 demands.[50] Indian identity documents do not generally incorporate parent-child relational data, meaning that even after a minor's age is confirmed, there exists no automated pathway to identify or contact the parent for consent.[23] As Singh and Mukherji have noted, neither the Act nor the Rules prescribe any specific age-gating method, a technology-agnostic posture that, in the absence of viable technology, is functionally indistinguishable from a posture of non-enforcement.[51]

COMPARATIVE TRAJECTORIES: FROM GATEKEEPING TO ENVIRONMENT DESIGN

India's DPDP Act did not emerge in isolation. It belongs to a family of regulatory responses to a shared challenge: how to protect minors in a digital environment engineered primarily for adult economic transactions. This Part examines four comparator jurisdictions and argues that India has embraced the maximalist iteration of a paradigm from which its comparators are progressively distancing themselves.

The United States: COPPA and Its Evolution: The Children's Online Privacy Protection Act, enacted in 1998 and first effective in 2000, is the longest-standing children's data protection statute in any major jurisdiction.[52] COPPA defines a 'child' as an individual under the age of thirteen, markedly lower than India's threshold of eighteen. It applies to operators of websites and online services 'directed to children' or possessing 'actual knowledge' of collecting personal information from children below thirteen, requiring verifiable parental consent before collection, use, or disclosure.[53]

The Federal Trade Commission's January 2025 amendments to the COPPA Rule, the first substantive update since 2013, mark a significant paradigmatic evolution.[54] The amended Rule, effective from June 2025, requires operators to obtain separate opt-in parental consent for disclosing children's personal information to third parties for targeted advertising; imposes explicit data-retention limits; expands the definition of personal information to include

[50] Ashok Hariharan, 'Challenges of Age-Gating: Why Verifiable Parental Consent Has Become a Major Hurdle in India' (ABP News, 22 October 2024).
[51] Vikram Jeet Singh and Arushi Mukherji, '4 Learnings on Age-Gating from India's Draft DPDP Rules, 2025' (BTG Advaya, January 2025).
[52] Children's Online Privacy Protection Act 1998 (US), 15 USC §§ 6501–6506; COPPA Rule, 16 CFR pt 312.
[53] Children's Online Privacy Protection Act 1998 (US), 15 USC §§ 6501–6506; COPPA Rule, 16 CFR pt 312.
[54] Federal Trade Commission, 'FTC Finalises Changes to Children's Privacy Rule Limiting Companies' Ability to Monetise Kids' Data' (16 January 2025) https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data accessed 15 June 2026.

biometric identifiers; and increases transparency requirements for Safe Harbour programmes.[55] The pending COPPA 2.0 legislation would extend protections to teenagers and introduce a direct ban on targeted advertising directed at minors.[56] The direction of travel is instructive: even the United States, which pioneered the consent-based, gate-keeping model, is now supplementing consent with substantive restrictions on what platforms may do with data.

The European Union: GDPR Article 8: Article 8 of the General Data Protection Regulation provides that where processing of a child's personal data is based on consent, the processing shall be lawful only if consent is given or authorised by the holder of parental responsibility and the child is below sixteen.[57] Member States may lower this threshold to as low as thirteen, a flexibility widely exercised. The GDPR does not impose a blanket ban on tracking or behavioural monitoring of children, nor does it prescribe a specific age-verification mechanism; controllers must instead make 'reasonable efforts' to verify parental consent.[58][59] The GDPR's approach is thus more calibrated than the DPDP Act's: a lower default threshold, a recalibration mechanism, and a proportionality-based verification standard. It softens the consent-at-the-gate paradigm rather than replacing it.

The United Kingdom: The Age-Appropriate Design Code: The United Kingdom's Age-Appropriate Design Code ('AADC' or 'Children's Code'), issued by the Information Commissioner's Office in 2020 and fully enforceable since September 2021, represents what this article contends is the paradigm shift that India should emulate.[60] Unlike COPPA, the GDPR, and the DPDP Act, the AADC does not ask parents to consent; it asks platforms to design services that are safe for children by default. The Code comprises fifteen standards that online services 'likely to be accessed by children' (defined as individuals under eighteen) must follow, including: the best interests of the child as a primary design consideration; mandatory

[55] Federal Trade Commission, 'FTC Finalises Changes to Children's Privacy Rule Limiting Companies' Ability to Monetise Kids' Data' (16 January 2025) <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data> accessed 15 June 2026.
[56] Shreya Arun and Aravind Ganapathy, 'Verifiable Parental Consent and Age Verification: A Comparative Analysis of India's Draft DPDP Rules and COPPA' (NUJS IP & Technology Laws Society, March 2025).
[57] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1, art 8.
[58] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1, art 8.
[59] Anirudh Krishna, 'Navigating Child Personal Data Protection: A Comparative Analysis of the Indian DPDP Regime and the GDPR' (TLH Law Insights, March 2025).
[60] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.

data protection impact assessments; high privacy settings by default; geolocation disabled by default; prohibitions on nudge techniques encouraging children to provide personal data; and minimised data collection.[61]

The AADC's conceptual innovation lies in its regulatory target. Rather than governing the relationship between parent and child (who consents on whose behalf), it governs the relationship between platform and child (how the platform architects its service). The burden of protection shifts from the family to the corporation. Since the Code came into full enforcement, major platforms including YouTube, Instagram, and TikTok have implemented substantive service changes for UK users: disabling autoplay for child users, restricting direct messaging to minors, switching off targeted advertising, and enabling default high-privacy settings. These changes were driven not by parental consent mechanisms but by a regulatory framework that placed accountability on the platform, precisely the direction this article argues India should pursue.

Australia and the Duty-of-Care Trajectory: Australia's regulatory trajectory reinforces the global shift toward platform accountability. The Online Safety Act 2021, administered by the eSafety Commissioner, imposes obligations on online service providers to take reasonable steps to minimise the risk of harm to Australians, with specific provisions for the protection of children. The Australian approach increasingly looks beyond consent toward systemic platform accountability, a movement aligned more with the UK's environment-based model than with the US-originated consent paradigm. The Australian experience confirms that the global direction is unmistakable: from parent-as-gatekeeper to platform-as-duty-bearer.

India's Maximalist Embrace: A comparative synopsis reveals a striking pattern. COPPA sets the age at thirteen, requires verifiable parental consent, and applies an 'actual knowledge' standard for general-audience sites.[62] The GDPR sets a default age of sixteen (subject to member-state reduction to thirteen), requires parental consent with 'reasonable efforts' to verify, and offers six lawful bases for processing.[63] The UK AADC targets services likely to be accessed by under-eighteens but does so through fifteen design standards imposed on

[61] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1, art 8.
[62] Children's Online Privacy Protection Act 1998 (US), 15 USC §§ 6501–6506; COPPA Rule, 16 CFR pt 312.
[63] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1, art 8.

platforms rather than consent obligations on parents.[64] India's DPDP Act sets the age at eighteen (the highest globally), mandates verifiable parental consent for all processing (the most demanding standard globally), imposes a blanket ban on tracking, behavioural monitoring, and targeted advertising (the broadest prohibition globally), and prescribes penalties of up to ₹250 crore (among the severest globally).[65][66][67] India has adopted the most aggressive version of the consent-at-the-gate paradigm at the precise historical moment when the jurisdictions that pioneered the paradigm are moving beyond it.[68][69]

CONSTITUTIONAL DIMENSIONS: PRIVACY, EDUCATION, EXPRESSION, AND AUTONOMY

The critique advanced in Parts III and IV is reinforced by a constitutional analysis that reveals potential tensions between Section 9 and several fundamental rights guaranteed under Part III of the Constitution of India, as well as India's obligations under international child rights law.

The Rights to Education and Expression: Article 21A of the Constitution guarantees the right to free and compulsory education for children between six and fourteen years, and the broader right to education has been recognised as implicit in the right to life and personal liberty under Article 21, extending protective reach to adolescents accessing secondary and higher-secondary education.[70] Article 19(1)(a) guarantees the freedom of speech and expression, which the Supreme Court has interpreted to encompass the right to receive information and ideas online.[71] A blanket consent requirement that prevents adolescents from accessing educational platforms, informational resources, and expressive fora without parental authorisation creates a de facto barrier to the exercise of these fundamental rights, not imposed by the platform, but imposed by the regulatory architecture itself. The barrier is not

[64] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.
[65] UNICEF Data, 'How Many Children Are There in India?' (2025): 430,108,317 individuals under 18.
[66] Digital Personal Data Protection Act 2023, s 9(3).
[67] Digital Personal Data Protection Act 2023, s 33.
[68] Devansh Pratap Singh and Habib Ur Rehman, 'Children's Data Protection Under the DPDP Act: Adequacy, Gaps, and Global Perspectives' (2025) 6(2) International Journal of Advanced Legal Research.
[69] Jidesh Kumar and Aurelia Menezes, 'Children's Data Under the DPDP Act, 2023 and DPDP Rules, 2025: The New Compliance Frontier' (King Stubb & Kasiva, April 2026).
[70] Constitution of India, art 21A.
[71] Constitution of India, art 19(1)(a).

hypothetical: it operates precisely against the children in digitally disadvantaged households whom Article 21A most solicitously aims to protect.

The UNCRC and the Evolving Capacities Doctrine: India ratified the United Nations Convention on the Rights of the Child in 1992. The UNCRC recognises a constellation of rights bearing directly on children's data protection: the right to be heard (Article 12); freedom of expression (Article 13); freedom from arbitrary interference with privacy (Article 16); and access to information (Article 17). Crucially, Article 5 of the UNCRC enshrines the 'evolving capacities' doctrine: the recognition that children progressively acquire competencies, understanding, and agency as they mature, and that parental direction must evolve correspondingly.[72]

The UN Committee on the Rights of the Child has elaborated this doctrine in two General Comments of direct relevance. General Comment No. 20 (2016), on the implementation of children's rights during adolescence, calls upon States to recognise adolescents as active rights-holders with increasing autonomy.[73] General Comment No. 25 (2021), on children's rights in the digital environment, applies the evolving-capacities principle explicitly: 'States parties should respect the evolving capacities of the child as an enabling principle' with 'particular significance in the digital environment, where children can engage more independently from supervision by parents and caregivers.'[74] India's uniform eighteen-year threshold ignores this graduated approach entirely, treating a six-year-old and a seventeen-year-old as identically incapable of exercising informational autonomy.[75]

Puttaswamy and the Privacy Rights of Adolescents: The Supreme Court's nine-judge bench decision in Justice K.S. Puttaswamy (Retd) v Union of India unanimously held that the right to privacy is a fundamental right protected under Article 21, forming part of the freedoms guaranteed by Part III.[76] Justice Chandrachud's lead opinion located privacy in the triad of liberty, dignity, and autonomy without limiting its applicability to adults. The privacy right

[72] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, arts 3, 5, 12, 13, 16, 17.
[73] IMARC Group, India EdTech Market Report 2025.
[74] UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25 (2 March 2021).
[75] Cyril Shroff and Arjun Goswami, 'Children and Consent under the Data Protection Act: A Study in Evolution' (India Corporate Law/Cyril Amarchand Mangaldas, August 2023). Cyril Shroff and Arjun Goswami, 'Children and Consent under the Data Protection Act: A Study in Evolution' (India Corporate Law/Cyril Amarchand Mangaldas, August 2023).
[76] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

recognised in Puttaswamy is that of every individual, including minors. This has a consequence the DPDP Act's framers appear not to have fully considered: the Act's consent model collapses the child's privacy into the parent's decision, presupposing that parental interests are coterminous with the children. But adolescents possess privacy interests vis-à-vis their parents' interests in sexual health information, mental health resources, identity exploration, and political expression that they may legitimately wish to shield from parental knowledge. A regime that requires parental consent for all processing effectively grants parents a surveillance prerogative over their adolescent children's digital lives, converting a data-protection statute into a parental-control mechanism.

The Vagueness Challenge: Section 9(2) and Article 14: The prohibition on processing likely to cause 'detrimental effect on the well-being of a child' in Section 9(2) is constitutionally vulnerable on vagueness grounds.[77] The Supreme Court's arbitrariness jurisprudence under Article 14 requires that statutory standards be sufficiently precise to guide both regulated entities and adjudicatory bodies.[78] The phrase 'detrimental effect on the well-being' is a term of extraordinary breadth. Without legislative definition, regulatory guidance, or judicial precedent, it could encompass everything from addictive design patterns to educational gamification, from social media algorithms to online advertising. A standard that can mean anything risks meaning nothing or, worse, meaning whatever the executive determines it should mean on a case-by-case basis, generating precisely the kind of arbitrariness Article 14 prohibits.

SECTORAL DISLOCATIONS: EDTECH, DARK PATTERNS, AND ONLINE COMMUNITIES

The theoretical concerns articulated in Parts III through V acquire urgent practical significance when applied to the three sectors most affected by Section 9: educational technology, dark-pattern enforcement, and social media and gaming platforms.

EdTech: The $7.5 Billion Market at Regulatory Risk: India's educational-technology sector was valued at approximately USD 7.5 billion in 2024, with an expected compound annual

[77] Digital Personal Data Protection Act 2023, s 9(2).
[78] Constitution of India, art 14.

growth rate of 27.65 per cent, projected to reach USD 29 billion by 2030.[7980] The sector is characterised by platforms serving millions of users between the ages of ten and seventeen, including BYJU'S, Unacademy, PhysicsWallah, Vedantu, and a growing ecosystem of vernacular-language learning platforms.[81] For these platforms, Section 9 poses an existential compliance challenge. Verifiable parental consent for every student interaction — every lesson accessed, every test attempted, every progress report generated imposes friction that could fragment the user experience and drive students to unregulated platforms operating from jurisdictions beyond the Act's reach.

The Fourth Schedule exemptions under Rule 11 do not cover EdTech platforms; they are limited to clinical establishments, mental health establishments, healthcare professionals, and allied healthcare professionals.[82] An educational platform that serves millions of minors falls outside these narrow exemptions unless the Central Government exercises its Section 9(5) discretion to declare such platforms 'verifiably safe.'[83] The regulatory irony is acute: India's National Education Policy 2020 aggressively promotes digital education, online learning platforms, and technology-enabled pedagogical innovation, while the DPDP Act simultaneously erects barriers to the very digital access that NEP 2020 seeks to expand.

Dark Patterns and the Enforcement Gap: The intersection of children's data protection and deceptive design was brought into sharp relief in June 2026, when the Central Consumer Protection Authority penalised PhysicsWallah, one of India's largest EdTech platforms, with a user base comprising predominantly students, including minors, for deploying dark patterns.[84] The CCPA found that PhysicsWallah had automatically added a ₹10 donation at checkout without explicit user consent, used emotionally charged messages about children's education to discourage removal of the donation, and required users to share personal information to access courses advertised as 'free.'[85] The penalty was ₹5 lakh, a sum so trivial relative to the platform's revenue that it functions as a cost of doing business rather than a deterrent.

[79] Shaheed Sukhdev College of Business Studies (University of Delhi), Ed-Tech Industry Report (2025), showing India EdTech market valued at USD 7.5 billion (2024).
[80] IMARC Group, India EdTech Market Report 2025.
[81] GlobalData, 'EdTech in India' (February 2025).
[82] Digital Personal Data Protection Rules 2025, r 11, read with Fourth Schedule.
[83] Jidesh Kumar and Aurelia Menezes, 'Children's Data Under the DPDP Act, 2023 and DPDP Rules, 2025: The New Compliance Frontier' (King Stubb & Kasiva, April 2026).
[84] 'Consumer Protection Authority Penalises PhysicsWallah, McAfee for Misleading Consumers' Financial Express (3 June 2026).
[85] 'Consumer Protection Authority Penalises PhysicsWallah, McAfee for Misleading Consumers' Financial Express (3 June 2026).

This enforcement action illustrates both the problem and the regulatory gap. The dark patterns were identified and penalised under the Guidelines for Prevention and Regulation of Dark Patterns, 2023, issued under the Consumer Protection Act, 2019.[86] They were not addressed under the DPDP Act, which, as of mid-2026, has not yet reached full enforcement of its substantive provisions. When the DPDP Act's Section 9 obligations come into full force in May 2027, the regulatory overlap between dark-patterns regulation (which targets platform design) and children's data protection (which targets consent) will create a fragmented enforcement landscape. A well-designed regulatory framework would address platform design and data processing through a unified accountability model, an outcome the four-pillar alternative proposed in Part VII would achieve.

Social Media and Gaming: The Blanket-Ban Dilemma: India's social media platforms serve hundreds of millions of users, a significant proportion of whom are under eighteen. Section 9(3)'s blanket ban on tracking, behavioural monitoring, and targeted advertising directed at children would, if enforced, require these platforms to fundamentally reconfigure their business models for Indian users.[87] But enforcement requires identification of minor users, which returns the analysis to the age-verification paradox. More troublingly, the prohibition may prevent safety-oriented monitoring such as detecting cyberbullying, self-harm indicators, or grooming behaviour that relies on precisely the kind of data analysis Section 9(3) prohibits.[88] The mobile gaming sector, involving real-time data processing, in-app purchases, and behavioural profiling, faces analogous challenges: a consent-per-session model is technically unworkable for gaming environments designed around continuous, immersive engagement.[89] The Fourth Schedule exemptions provide essential but narrowly drawn relief that does not comprehensively address the commercial digital ecosystem in which the vast majority of children's digital interactions occur.

THE ALTERNATIVE: A FOUR-PILLAR FRAMEWORK

This article does not argue that children's data should be unprotected. It argues that the protection should be redesigned. This Part proposes a four-pillar 'Safe Digital Environment'

[86] Guidelines for Prevention and Regulation of Dark Patterns 2023, notified 30 November 2023 under s 18 of the Consumer Protection Act 2019.
[87] Digital Personal Data Protection Act 2023, s 9(3).
[88] Jhalak M Kakkar, Shashank Mohan and Angelina Dash, 'Parental Consent is a Conundrum for Online Child Safety' (TechPolicy.Press, 22 July 2025).
[89] Jidesh Kumar and Aurelia Menezes, 'Children's Data Under the DPDP Act, 2023 and DPDP Rules, 2025: The New Compliance Frontier' (King Stubb & Kasiva, April 2026).

model that draws upon the UK's Age-Appropriate Design Code, the UNCRC's evolving-capacities doctrine, and the emerging international consensus on platform accountability.

Pillar One: Graduated Age Thresholds: The blanket eighteen-year threshold should be replaced with a graduated system that recognises developmental differences between a six-year-old and a seventeen-year-old. For children aged zero to twelve, full verifiable parental consent should be retained, consistent with the COPPA standard and near-universal international practice.[90] For adolescents aged thirteen to fifteen, simplified consent mechanisms, for example, parental authorisation of categories of platforms rather than individual transactions, should be combined with mandatory platform safeguards (default high-privacy settings, no behavioural advertising, no profiling). For young adults aged sixteen to seventeen, self-consent should be permitted, subject to enhanced transparency obligations on the Data Fiduciary: clear, age-appropriate privacy notices; granular control over data sharing; and the right to request deletion of data processed during minority.

This graduated approach mirrors the UNCRC's evolving-capacities doctrine[91] and aligns with the GDPR's flexible age-threshold mechanism.[92] It also parallels the approach taken by India's own legal system in other domains: the Indian Penal Code recognises varying degrees of criminal responsibility at different ages; the Indian Contract Act treats minors' contracts as voidable rather than void in certain circumstances; and the Juvenile Justice Act provides for graduated interventions based on age. There is no principled reason why data protection law should treat all minors as a monolithic category when no other major branch of Indian law does so.[93]

Pillar Two: Platform Duty of Care: The regulatory burden should shift from parents to platforms. India should impose a statutory duty of care on all Data Fiduciaries whose services are likely to be accessed by children, requiring them to take reasonable steps to design and operate their services in a manner that protects the well-being, privacy, and developmental interests of minor users.[94] This duty should be operationalised through mandatory Child Data

[90] Children's Online Privacy Protection Act 1998 (US), 15 USC §§ 6501–6506; COPPA Rule, 16 CFR pt 312.
[91] UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25 (2 March 2021).
[92] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1, art 8.
[93] Cyril Shroff and Arjun Goswami, 'Children and Consent under the Data Protection Act: A Study in Evolution' (India Corporate Law/Cyril Amarchand Mangaldas, August 2023).
[94] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-

Protection Impact Assessments modelled on the DPIA requirement under the UK's Age Appropriate Design Code[95] conducted before the launch of any service or feature likely to be accessed by children.

The duty of care should further mandate: default high-privacy settings for all users identified or reasonably suspected to be minors; prohibition on dark patterns, nudge techniques, and persuasive design features that exploit developmental vulnerabilities; data minimisation by design; and restriction on data sharing with third parties for commercial purposes. The UK experience demonstrates that this approach is operationally feasible. Since the Children's Code came into full effect in September 2021, the ICO has conducted multiple engagements with major technology companies, resulting in measurable changes to default settings, data collection practices, and algorithmic recommendation systems.[96]

Pillar Three: Outcome-Based Regulation: The third pillar replaces process-based consent requirements with outcome-based regulatory mandates. Instead of prescribing how consent must be obtained a process that, as Part III demonstrated, is structurally unworkable at Indian scale the framework should prescribe what outcomes must be achieved: no profiling of minors for commercial advertising purposes; no retention of children's personal data beyond the immediate session or transaction; no sharing of children's data with third-party advertisers or data brokers; and no algorithmic amplification of content deemed harmful to child well-being. Compliance should be verified through periodic audits conducted by the Data Protection Board or accredited independent auditors, not through the collection and documentation of individual consent records.[97] This approach is enforceable at scale, technology-neutral, and places the compliance burden on the entity best positioned to bear it the platform rather than on the family least equipped to navigate it.

information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.

[95] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.

[96] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.

[97] Guidelines for Prevention and Regulation of Dark Patterns 2023, notified 30 November 2023 under s 18 of the Consumer Protection Act 2019.

Pillar Four: Digital Literacy as Public Infrastructure: The fourth pillar addresses the root cause rather than the symptom. The consent model fails in part because the population it relies upon lacks the digital literacy to engage meaningfully with data processing decisions. Rather than designing around this deficiency through ever-more-complex consent architectures, India should invest in eliminating it. Digital safety education should be integrated into the school curriculum under the National Education Policy 2020, with age-appropriate modules beginning at the primary level. Parental digital literacy programmes should be funded through corporate social responsibility obligations under the Companies Act, 2013, creating a direct nexus between the corporations profiting from data processing and the communities whose data they process. Most critically, India should establish an independent Children's Digital Safety Commissioner, a statutory office, separate from the Data Protection Board of India, with a mandate to advocate for children's digital rights, research emerging harms, issue guidance to platforms and parents, and represent children's interests in regulatory proceedings.[98]

CONCLUSION

This article has argued that the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025, in their treatment of children's personal data, rest on a paradigm that is simultaneously well-intentioned and fundamentally misconceived. Section 9's consent-centric, gate-based framework treats the digital world as a dangerous place from which children must be excluded unless a parent opens the door. The alternative paradigm proposed here treats the digital world as a shared environment that must be made safe for all its inhabitants, including the youngest. The shift from gate-based to environment-based protection is not merely a regulatory preference; it is demanded by empirical evidence, by comparative analysis, and by constitutional principle. Puttaswamy's recognition of informational autonomy extends to adolescents, and the UNCRC's evolving-capacities doctrine requires that children's increasing agency be reflected in the regulatory framework rather than denied by it.[99][100]

The legislative opening for this transformation already exists within the DPDP Act itself. Section 9(5) empowers the Central Government to notify that a Data Fiduciary whose

[98] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.
[99] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[100] UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25 (2 March 2021).

processing of children's data is done in a manner that is 'verifiably safe' may be exempted from the consent and tracking prohibitions above a specified age.[101] This provision is the hinge on which a graduated, design-based regime can be constructed. The Government should exercise this power not as an ad hoc exemption for favoured entities but as the foundation of a systematic framework that rewards platforms for investing in child-safe design rather than punishing parents for failing to navigate consent architectures.[102]

The Data Protection Board of India, as it begins its enforcement operations in the period leading to the May 2027 full compliance deadline,[103] should prioritise platform accountability over parental burden. Its first enforcement actions should target not the family that failed to produce a verifiable consent record, but the platform that continued to profile, monetise, and amplify content directed at children without regard to their well-being. If the Board establishes this priority from its inception, it will signal that India's data protection regime understands where the real threat to children lies: not at the gate, but inside the walls. The challenge is not to protect children from the digital world. It is to protect them within it.

[101] Digital Personal Data Protection Act 2023, s 9(4)–(5).
[102] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (2 September 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 15 June 2026.
[103] UN Committee on the Rights of the Child, General Comment No 20 (2016) on the implementation of the rights of the child during adolescence, CRC/C/GC/20 (6 December 2016).