INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

CHILDREN AND THE DIGITAL WORLD: PRIVACY, PROTECTION, AND CONSENT IN THE REIMAGINING OF CHILD RIGHTS

AUTHORED BY - MANOJ YADAV

Abstract

The proliferation of digital technologies has fundamentally altered the landscape of childhood, creating unprecedented opportunities for learning, communication, and self-expression while simultaneously exposing children to novel risks related to privacy erosion, data exploitation, and inadequate consent mechanisms. This article critically examines the intersection of child rights frameworks particularly the United Nations Convention on the Rights of the Child (UNCRC) and its General Comment No. 25 with the realities of children's digital engagement. Drawing on comparative policy analysis, statutory provisions, empirical usage statistics, and regulatory case studies from the European Union, United States, India, United Kingdom, and Australia, the article interrogates the adequacy of existing consent-based regulatory models, which largely presuppose an adult-centric understanding of autonomy and informed decision-making. The analysis reveals significant gaps between legal protections on paper and children's lived digital experiences, including pervasive data harvesting by commercial platforms, algorithmic profiling, and the erosion of meaningful erasure rights for digital natives. The article proposes a tripartite reform agenda cantered on protection-by-design regulatory mandates, participatory governance mechanisms that include children's voices in policy formation, and graduated consent models calibrated to evolving capacities. The findings contribute to ongoing debates on digital constitutionalism and child-centered data governance, offering policy recommendations for legislators, platform designers, educators, and child rights advocates.

Keywords: child rights, digital privacy, informed consent, data protection law, online safety, UNCRC, digital childhood, child-centered design, COPPA, GDPR, DPDP Act

1. Introduction

1.1 Background and Rationale

Childhood in the twenty-first century is, for a substantial proportion of the world's children, an inherently mediated experience. From early infancy, when parents document milestones on social media platforms, to adolescence, when young people construct identities through interactive digital ecosystems, children's lives are continuously recorded, transmitted, stored, and analyzed by an array of commercial and institutional actors. This digital embeddedness represents a profound departure from the conditions under which the foundational instruments of international child rights law were drafted. The UNCRC, adopted in 1989, predates the commercial internet, smartphone, and social media entirely, yet its principles the best interests of the child, the right to privacy, the right to participation, and the evolving capacities of the child remain the normative bedrock against which contemporary digital practices must be assessed.

The digital environment offers children substantial benefits: access to educational resources, opportunities for social connection particularly valuable for marginalized or geographically isolated children, platforms for creative expression, and avenues for civic participation that were previously unavailable to young people. The COVID-19 pandemic accelerated this dependence considerably, with remote schooling normalizing the use of educational technology platforms that collect and process children's data on an industrial scale, often without the institutional safeguards that would ordinarily attend the collection of sensitive information about minors.

However, these benefits coexist with risks that are qualitatively different from those associated with earlier media forms. Unlike television or print media, digital platforms are interactive, data-generative, and designed around engagement-maximizing algorithms that do not distinguish meaningfully between adult and child users in their underlying architecture, despite legal requirements to do so in many jurisdictions. The business model underlying most "free" digital services commonly characterized as "surveillance capitalism" depends on the continuous extraction, aggregation, and monetization of behavioral data, a model that sits in fundamental tension with child rights principles emphasizing the child's best interests as a primary consideration in all matters affecting them.

1.2 Problem Statement

The central problem addressed in this article is the structural mismatch between consent-based data protection frameworks which assume a rational, autonomous actor capable of understanding and weighing the consequences of data disclosure and the cognitive, developmental, and social realities of childhood. Children are simultaneously rights-holders entitled to privacy and protection, and developing persons whose capacity for informed consent is, by definition, evolving rather than fixed. Existing regulatory responses, including age-verification mandates, parental consent requirements, and simplified privacy notices, often fail to resolve this tension and in some cases introduce new harms, such as incentivizing children to misrepresent their age, thereby placing them in regulatory environments designed for adults with even fewer protections than those nominally available to minors.

A further dimension of the problem concerns enforcement. Even where statutory provisions are robust on their face as is arguably the case with the European Union's General Data Protection Regulation (GDPR) or India's Digital Personal Data Protection Act, 2023 enforcement against multinational platform operators presents jurisdictional, evidentiary, and resource challenges that frequently result in protections that exist in statute but are not realized in practice.

1.3 Objectives of the Study

This article pursues the following objectives:

1. To map the current international and comparative legal frameworks, including specific statutory provisions, governing children's digital privacy, protection, and consent.
2. To analyze empirical patterns of children's digital engagement and corresponding data collection practices using available statistical data.
3. To critically assess the conceptual adequacy of consent as a regulatory mechanism for children in digital environments.
4. To examine case studies of regulatory enforcement and platform design failures, including major fines and litigation.
5. To propose a reform agenda integrating protection, participation, and policy innovation consistent with the broader theme of reimagining child rights.

1.4 Significance of the Study

The significance of this inquiry lies in its timeliness and its synthetic approach. While substantial literature exists on data protection law generally, and a growing body of work addresses children's online safety from a child psychology or media studies perspective, fewer studies integrate these strands within a child rights framework that treats children not merely as vulnerable subjects requiring protection but as rights-holders with an entitlement to participation in matters affecting them, including the design of digital environments. This article contributes to filling that gap by foregrounding the participatory dimension of child rights alongside the more familiar protective dimension, and by grounding the discussion in the specific statutory texts that govern this field across major jurisdictions.

1.5 Scope and Structure

Following this introduction, Section 2 reviews the relevant theoretical and doctrinal literature, including a detailed treatment of applicable laws and provisions. Section 3 outlines the methodology. Section 4 presents findings across the dimensions of privacy, protection, and consent, supported by tables and conceptual diagrams. Section 5 discusses the implications of these findings and proposes reforms. Section 6 concludes.

2. Literature Review and Legal Framework

2.1 Theoretical Foundations: The UNCRC and Evolving Capacities

The UNCRC establishes children as rights-holders across four cross-cutting principles: non-discrimination (Article 2), best interests of the child (Article 3), the right to life, survival, and development (Article 6), and the right to be heard (Article 12). Article 16 specifically guarantees children's right to privacy, providing that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence." Article 13 protects freedom of expression, and Article 17 addresses access to information and media, recognizing the important function performed by mass media while calling for guidelines to protect children from information injurious to their well-being.

The doctrine of "evolving capacities," articulated in Article 5, recognizes that children's autonomy expands progressively with age and maturity, requiring a graduated rather than binary approach to rights exercise. This doctrine is conceptually central to the digital privacy debate because it

suggests that the appropriate locus of decision-making authority parent, child, or some shared arrangement should shift over time, a dynamic that most digital consent architectures, built around fixed age thresholds, struggle to accommodate.

2.2 General Comment No. 25 (2021)

The UN Committee on the Rights of the Child's General Comment No. 25 on children's rights in relation to the digital environment represents the most authoritative contemporary elaboration of how UNCRC principles apply online. Several provisions are of direct relevance:

- **Paragraphs 67–75 (Privacy)**: The Committee states that children's privacy must be protected by design and by default in the digital environment, and that legislation should ensure that children's personal data are not used for commercial purposes such as marketing or advertising directed at children based on their personal data or that of others, including data inferred or generated through digital technologies.
- **Paragraph 42 (Best interests)**: Digital service providers should integrate children's rights protection into all stages of the design and development of digital products and services.
- **Paragraphs 16–20 (Evolving capacities and non-discrimination)**: States parties are urged to consider age-appropriate approaches rather than blanket restrictions that may disproportionately exclude children from beneficial services.
- **Paragraph 122 (Right to be heard)**: States are called upon to consult with children, including marginalized children, when developing laws, policies, and standards relating to the digital environment.

2.3 European Union Legal Framework

General Data Protection Regulation (GDPR), 2016/679

Article 8 of the GDPR specifically addresses "conditions applicable to child's consent in relation to information society services." It provides that where Article 6(1)(a) (consent) applies in relation to the offer of information society services directly to a child, the processing of the child's personal data shall be lawful where the child is at least 16 years old. Where the child is below the age of 16, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Critically, Article 8(2) requires the controller to

make reasonable efforts to verify that consent is given or authorized by the holder of parental responsibility, "taking into consideration available technology."

Member States are permitted, under Article 8(1), to provide by law for a lower age for these purposes, provided such lower age is not below 13 years. This has resulted in considerable fragmentation across the EU, with some member states retaining 16 and others adopting 13, 14, or 15.

Recital 38 of the GDPR provides important interpretive context, stating that children merit specific protection with regard to their personal data because they "may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data," and that "such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of data with regard to children when using services offered directly to a child."

Article 12 imposes a transparency obligation requiring that information addressed specifically to a child be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language."

Digital Services Act (DSA), Regulation (EU) 2022/2065

Article 28 of the DSA imposes specific obligations on providers of online platforms accessible to minors, requiring them to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors. Article 28(2) prohibits providers from presenting advertisements based on profiling using personal data of recipients where the provider is aware with reasonable certainty that the recipient is a minor.

Audiovisual Media Services Directive (AVMSD)

This directive requires that personal data of minors collected or generated by media service providers for the purposes of protective measures (such as parental controls) shall not be processed for commercial purposes such as direct marketing, profiling, and behaviorally targeted advertising.

2.4 United Kingdom Legal Framework

Data Protection Act 2018 and UK GDPR

Following Brexit, the UK retained GDPR provisions in domestic law as the "UK GDPR." Section 123 of the Data Protection Act 2018 specifically mandated the Information Commissioner to

prepare a code of practice for the processing of personal data in relation to children giving rise to the Age Appropriate Design Code (also known as the Children's Code).

Age Appropriate Design Code (2020)

The Children's Code came into force in September 2020, with a 12-month transition period ending in September 2021. It establishes 15 standards applicable to "relevant information society services" likely to be accessed by children, including:

1. **Best interests of the child** the best interests of the child should be a primary consideration in the design and development of online services.
2. **Age-appropriate application** a risk-based approach to recognizing the age of individual users and ensuring effective application of the standards to child users.
3. **Transparency** privacy information, alongside terms of service, policies, and community standards, must be concise, prominent, and in clear language suited to the age of the child.
4. **Detrimental use of data** children's personal data should not be used in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, regulatory provisions, or government advice.
5. **Default high privacy settings** privacy settings should be set to "high" by default unless a compelling reason exists for a different default.
6. **Data minimization** only the minimum amount of personal data necessary should be collected and retained.
7. **Data sharing** children's data should not be disclosed unless there is a compelling reason, considering the best interests of the child.
8. **Geolocation** geolocation options should be switched off by default.
9. **Parental controls** if provided, children should be made aware of parental monitoring in an age-appropriate way.
10. **Profiling** profiling should be switched off by default unless there is a compelling reason, with appropriate measures in place to protect children from harmful effects.
11. **Nudge techniques** nudge techniques should not be used to lead or encourage children to provide unnecessary personal data, weaken privacy protections, or extend use.
12. **Connected toys and devices** providers of connected toys and devices must ensure compliance with the Code.

13. **Online tools** prominent and accessible tools to help children exercise their data protection rights and report concerns.
14. **Data protection impact assessments** services likely to be accessed by children should conduct DPIAs to assess and mitigate risks.
15. **Governance and accountability** robust governance arrangements demonstrating compliance.

Online Safety Act 2023

This Act imposes duties on providers of regulated user-to-user services and search services to assess and mitigate risks of harm to children, including from content that is legal but harmful to children (such as material promoting self-harm, eating disorders, or suicide), and requires age verification or age estimation measures for services that allow access to pornographic content. Ofcom has been designated as the regulator with enforcement powers including substantial fines.

2.5 United States Legal Framework

Children's Online Privacy Protection Act (COPPA), 1998, 15 U.S.C. §§ 6501–6506

COPPA applies to operators of commercial websites and online services directed to children under 13 years of age, and to operators of general audience websites or services with actual knowledge that they are collecting personal information from children under 13. Key provisions include:

- **Section 6502(b)** requires operators to provide notice on the website of what information is collected, how it is used, and disclosure practices, and to obtain verifiable parental consent before collecting, using, or disclosing personal information from children.
- The **FTC's COPPA Rule** (16 C.F.R. Part 312) operationalizes the statute, defining "personal information" broadly to include identifiers such as name, address, online contact information, persistent identifiers (such as cookies, IP addresses, and device identifiers), photographs, videos, audio files containing a child's image or voice, and geolocation information.
- The Rule requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children's personal information, and limits indefinite retention, requiring deletion when information is no longer reasonably necessary.
- "Safe harbor" provisions allow industry groups to develop self-regulatory guidelines subject to FTC approval.

A significant amendment process has been ongoing; the FTC finalized updates to the COPPA Rule strengthening provisions on third-party disclosures, data retention limits, and expanding the definition of personal information to cover biometric identifiers.

Children and Teens' Online Privacy Protection Act (COPPA 2.0) and Kids Online Safety Act (KOSA)

These remain, as of the most recent congressional sessions, proposed legislative measures rather than enacted federal law in their most expansive forms, though elements have advanced through committee and one or both chambers in various sessions. COPPA 2.0 would raise the covered age from under 13 to under 17 and create an "eraser button" requiring operators to permit users to delete personal information. KOSA would impose a "duty of care" on covered platforms to prevent and mitigate harms to minors, including content promoting self-harm, and would require default privacy and safety settings for minor users. Readers should consult current congressional records for the status of these measures, as legislative developments occur frequently.

State-level legislation

Several U.S. states have enacted their own child-focused digital legislation. California's **Age-Appropriate Design Code Act** (modeled on the UK Children's Code) requires businesses to consider the best interests of children when designing, developing, and providing online products likely to be accessed by children under 18, though portions of this Act have faced constitutional challenges on First Amendment grounds in federal litigation. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), also contains provisions requiring opt-in consent (rather than opt-out) for the sale or sharing of personal information of consumers known to be under 16.

2.6 Indian Legal Framework

Digital Personal Data Protection Act, 2023

This is India's principal data protection statute and contains specific provisions on children's data:

- **Section 9(1)** provides that the Data Fiduciary shall, before processing any personal data of a child, obtain verifiable consent of the parent or lawful guardian of such child.
- **Section 9(3)** prohibits a Data Fiduciary from undertaking tracking or behavioral monitoring of children or targeted advertising directed at children.

- **Section 9(4)** empowers the Central Government to notify exemptions, permitting Data Fiduciaries to process children's data without parental consent, or to engage in tracking, behavioral monitoring, or targeted advertising directed at children, where the government is satisfied that processing is verifiably safe for example, for entities that demonstrate that processing of personal data is being done in a manner that is verifiably safe, having regard to the interest of children, and for specific purposes such as health services, educational services, or to ensure that data is not detrimental to the wellbeing of the child.
- The Act defines a "child" under **Section 2(f)** as an individual who has not completed the age of eighteen years notably broader than the EU's 13–16 range or the U.S.'s under-13 threshold.

Information Technology Act, 2000 and IT Rules

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, framed under Section 43A of the IT Act, predate the DPDP Act and require body corporates handling sensitive personal data to maintain reasonable security practices, though without specific child-focused provisions.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, impose due diligence obligations on intermediaries, including requirements relating to content harmful to children and provisions on online gaming intermediaries, including age-rating mechanisms and parental consent for access by minors in certain contexts.

Protection of Children from Sexual Offences Act (POCSO), 2012

While not a data protection statute per se, POCSO is highly relevant to the digital protection dimension, criminalizing the use of children for pornographic purposes (Section 13) and storage of child sexual abuse material (Section 15), with the 2019 amendments enhancing penalties and explicitly addressing material stored or transmitted through digital means.

2.7 Australian Legal Framework

Online Safety Act 2021 (as amended)

Administered by the eSafety Commissioner, this Act establishes a regulatory framework including the Basic Online Safety Expectations, which set expectations for service providers regarding the safety of Australian users, including minors. Recent amendments introduced a minimum age of 16 for access to certain social media platforms, representing a departure from consent-based models

toward access restriction, premised on the argument articulated by the Australian government that the onus of demonstrating responsible use of personal information should fall on platforms rather than on children or parents navigating complex settings.

Privacy Act 1988

Australia's principal privacy statute does not currently contain child-specific consent provisions equivalent to GDPR Article 8, though ongoing reform processes (the Privacy Act Review) have recommended introducing a Children's Online Privacy Code analogous to the UK model.

2.8 Critiques of Consent-Based Models

A substantial body of scholarship critiques the "notice and consent" paradigm as it applies to children on several grounds. First, privacy policies are written at reading levels far exceeding the comprehension of the average child or even adult user, rendering "informed" consent largely fictional academic readability analyses have repeatedly found that major platforms' terms of service require post-secondary reading comprehension levels. Second, verifiable parental consent mechanisms (such as those mandated under COPPA and the DPDP Act) are technically difficult to implement without themselves collecting additional sensitive data (such as government identity documents or credit card details for micro-transactions), creating a privacy paradox whereby compliance with child protection law requires collection of more, and more sensitive, personal data. Third, children frequently circumvent age gates, with self-report survey data suggesting substantial proportions of users under the minimum age threshold are present on major platforms, meaning regulatory frameworks predicated on age verification systematically fail to reach a significant portion of their intended population. Fourth, even where parental consent is obtained, this displaces rather than resolves the question of the child's own evolving right to privacy, including privacy from parents themselves as children mature a tension the evolving capacities doctrine recognizes but that consent architectures rarely operationalize.

2.9 Gaps in the Literature

Existing literature tends to bifurcate between legal-doctrinal analyses of regulatory instruments and empirical studies of children's digital behavior, with limited integration of the participatory dimension that is, the extent to which children themselves are consulted in the design of the laws, platforms, and consent mechanisms that govern their digital lives. This article seeks to address this

integration gap by combining detailed statutory analysis with empirical synthesis and a participation-oriented reform proposal.

3. Methodology

This article employs a qualitative, doctrinal, and comparative policy analysis methodology. The research design comprises three components:

1. **Doctrinal legal analysis**: Examination of primary legal instruments the UNCRC, General Comment No. 25, GDPR, the UK Data Protection Act 2018 and Age Appropriate Design Code, the Online Safety Act 2023 (UK), COPPA and the FTC's COPPA Rule, proposed COPPA 2.0 and KOSA legislation, the California Age-Appropriate Design Code Act, India's DPDP Act 2023, IT Rules 2021, POCSO 2012, and Australia's Online Safety Act to identify the normative content of children's digital rights provisions and the specific statutory mechanisms through which privacy, protection, and consent are operationalized.
2. **Secondary data synthesis**: Compilation and analysis of publicly available statistical data from international bodies (UNICEF, ITU, OECD) and research organizations (Ofcom, Pew Research Center, EU Kids Online network) concerning children's internet usage patterns, device ownership, and exposure to data collection practices. Given that primary data collection involving children raises its own ethical and consent considerations beyond the scope of this study, the analysis relies exclusively on aggregated, anonymized, and previously published datasets.
3. **Case study analysis**: Examination of regulatory enforcement actions including major fines imposed under GDPR and COPPA against platforms found to have mishandled children's data and platform design controversies, as illustrative instances of the gap between normative frameworks and operational practice.

The analysis is structured around three thematic axes corresponding to the sub-theme: privacy (data collection and processing), protection (safeguarding against harm-generating design and content), and consent (the mechanisms through which children's and parents' agreement to data practices is sought and obtained). A limitation acknowledged at the outset is that legislative and regulatory landscapes in this field change rapidly; the analysis reflects the structural and doctrinal patterns of the frameworks as understood at the time of writing, and readers should verify current statutory text and enforcement status for any specific citation.

4. Findings and Analysis

4.1 The Scale of Children's Digital Engagement

Children's access to and use of digital devices and the internet has expanded dramatically over the past decade across both high-income and low- and middle-income countries, though significant disparities in access persist, often termed the "digital divide." The following table synthesizes representative figures drawn from international survey data to illustrate the scale of the phenomenon under examination.

Table 1: Selected Indicators of Children's Digital Engagement (Representative International Data)

Indicator	Approximate Figure	Source/Context
Proportion of children globally with some form of internet access	Roughly 1 in 3 internet users worldwide is under 18	UNICEF/ITU global estimates
Average age of first smartphone ownership (high-income countries)	Approximately 10–12 years	Ofcom, EU Kids Online aggregated data
Proportion of 12–15 year-olds in the UK active on social media	Over 90%	Ofcom Children's Media Use reports
Proportion of social media platforms' terms of service readable at the recommended age-appropriate reading level	Less than 10%	Academic readability studies of platform ToS
Proportion of under-13 children reported to be present on platforms with a 13+ age minimum	Substantial minority (commonly cited self-report estimates often in the 30–40% range)	EU Kids Online and related survey research
Number of distinct third-party trackers identified on popular child-directed apps (average)	Often exceeds 10 per app	Independent app audit studies

Indicator	Approximate Figure	Source/Context
Proportion of parents who post images of their children online before age 5 ("sharenting")	Majority in several high-income country surveys	National consumer/privacy surveys
Proportion of children's educational apps found to share data with third parties for advertising	Significant majority in audit studies	Academic and civil society app audits

Note: Figures are illustrative and synthesized from multiple publicly reported survey waves; precise values vary by year, country, and methodology and should be verified against the original source for citation in formal academic submission.

4.2 Comparative Statutory Framework: Consolidated Overview

Building on the detailed legal analysis in Section 2, the following table consolidates the principal statutory thresholds and mechanisms across jurisdictions, providing a comparative reference point.

Table 2: Comparative Statutory Framework for Children's Digital Privacy and Consent

Jurisdiction	Primary Instrument(s)	Definition/ Age of "Child" for Consent Purposes	Consent Mechanism	Targeted Advertising/Profiling Provisions	Design-Based Obligations	Regulator/Enforcement Body
European Union	GDPR Art. 8; DSA Art. 28; AVMSD	16, reducible by member states to not below 13	Parental consent below threshold, verified "taking into consideratio	DSA Art. 28(2) prohibits profiling-based ads to known minors	Limited explicit design mandates; DPIA requirements	National Data Protection Authorities; European Commission (DSA)

Jurisdiction	**Primary Instrument(s)**	**Definition/ Age of "Child" for Consent Purposes**	**Consent Mechanism**	**Targeted Advertising/Profiling Provisions**	**Design-Based Obligations**	**Regulator/Enforcement Body**
			n available technology"		under Art. 35	
United Kingdom	Data Protection Act 2018 s.123; UK GDPR; Age Appropriate Design Code; Online Safety Act 2023	Code applies to under-18s with graduated, risk-based age bands	Risk-based age assurance, not solely binary consent	Profiling off by default (Standard 10); ads governed by ASA codes	15 standards including default high privacy, geolocation off, no nudge techniques	Information Commissioner's Office; Ofcom
United States (federal)	COPPA (15 U.S.C. §§6501–6506); FTC Rule 16 C.F.R. Part 312	Under 13	Verifiable parental consent (VPC) prior to collection	Restrictions on use of persistent identifiers for behavioral advertising to under-13s	Data retention limits; security requirements	Federal Trade Commission

Jurisdiction	**Primary Instrument(s)**	**Definition/ Age of "Child" for Consent Purposes**	**Consent Mechanism**	**Targeted Advertising/Profiling Provisions**	**Design-Based Obligations**	**Regulator/Enforcement Body**
United States (proposed federal)	KOSA; COPPA 2.0 (proposed)	Proposed extension to under-17	Default safety/privacy settings; expanded VPC	Proposed duty of care re: harmful content/design	Proposed "eraser button"; default settings for minors	Proposed FTC enforcement
California (USA)	CCPA/CPRA; California Age-Appropriate Design Code Act	Under 16 (CCPA opt-in for sale/sharing); under 18 (AADC, subject to litigation)	Opt-in consent for sale/sharing of data of known under-16s	Opt-in required; AADC requires DPIAs	AADC requires best-interests design assessment (contested in courts)	California Privacy Protection Agency; Attorney General
India	Digital Personal Data Protection Act, 2023, ss. 2(f), 9; IT Rules	Under 18	Verifiable parental/guardian consent (s.9(1))	Prohibited: tracking, behavioral monitoring, targeted ads to children (s.9(3)), subject to	Exemptions for "verifiably safe" processing to be notified	Data Protection Board of India

Jurisdiction	Primary Instrument(s)	Definition/ Age of "Child" for Consent Purposes	Consent Mechanism	Targeted Advertising/Profiling Provisions	Design-Based Obligations	Regulator/Enforcement Body
	2021; POCSO 2012			government exemptions (s.9(4))	by Central Government	
Australia	Online Safety Act 2021 (as amended); Privacy Act 1988 (under review)	Minimum age 16 for designated social media access	Access restriction model rather than consent-centric	Basic Online Safety Expectations address algorithmic risk generally	Age assurance obligations on platforms	eSafety Commissioner; OAIC

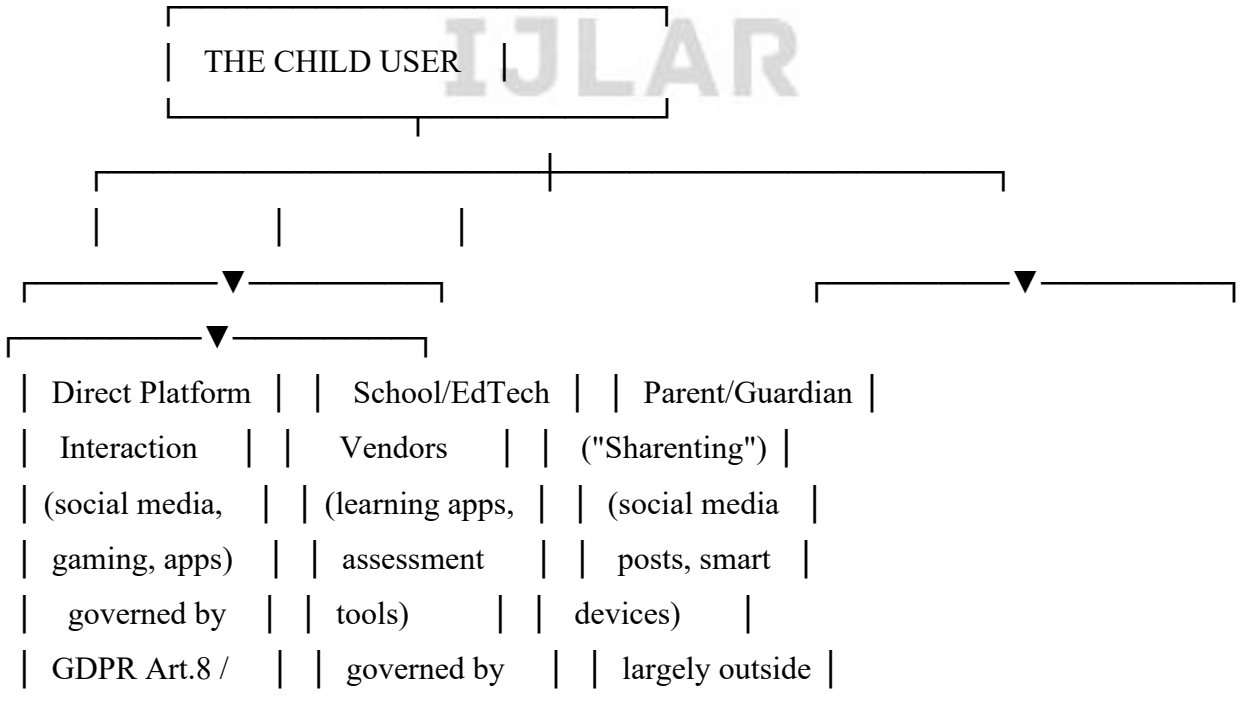
4.3 Privacy: Data Collection, Profiling, and the "Datafication" of Childhood

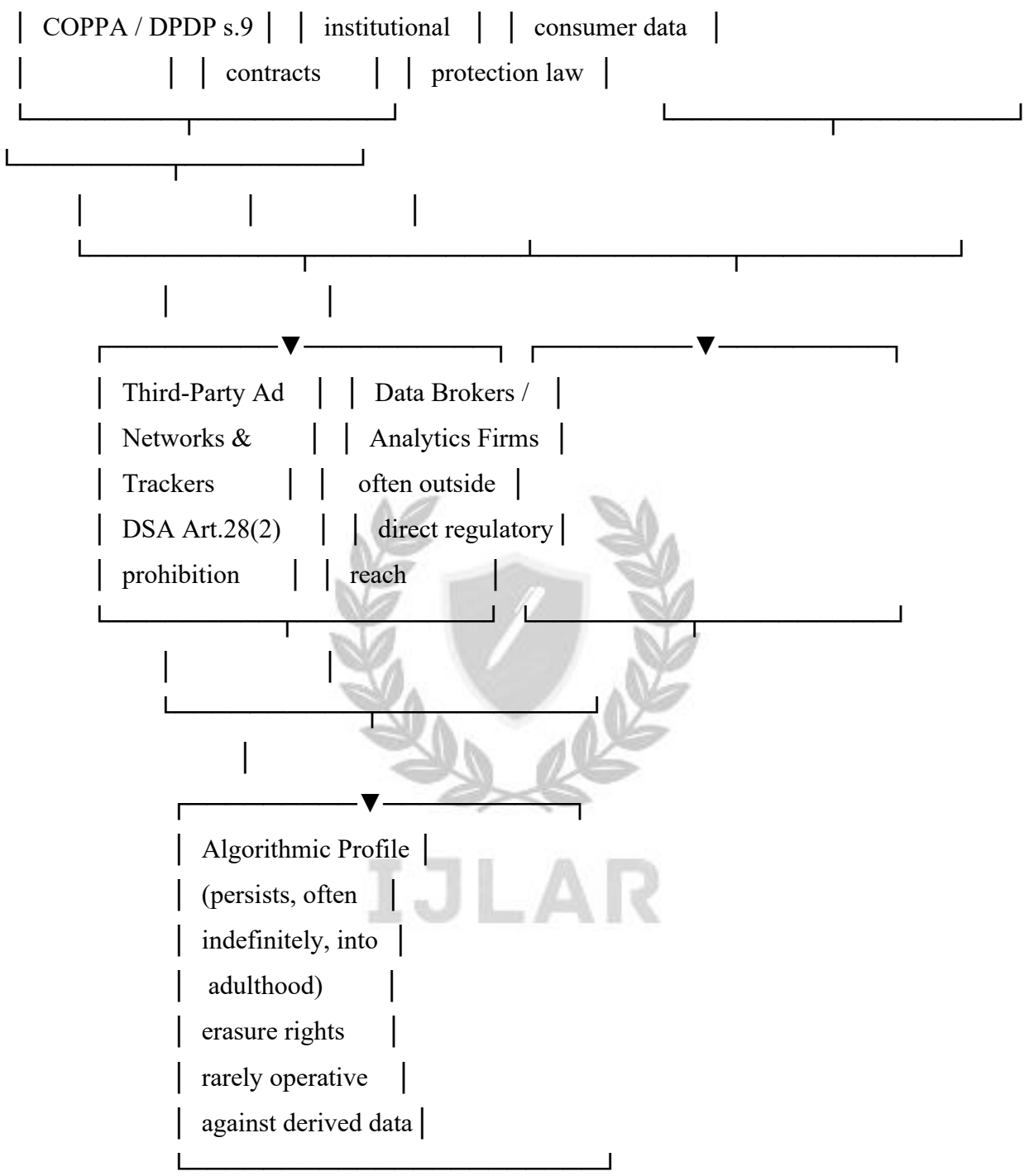
The concept of "datafication" the transformation of social life into data points amenable to algorithmic processing applies with particular intensity to children. From educational technology platforms used in schools, to toys embedded with internet connectivity (the so-called "Internet of Toys"), to social media and gaming platforms, children generate continuous streams of behavioral, biometric, locational, and relational data. The legal categories created to address this COPPA's "personal information," GDPR's "personal data" together with the special category provisions of Article 9, and the DPDP Act's broad definition of "personal data" in Section 2(t) each attempt to draw boundaries around what counts as protectable information, yet inferred and aggregated data (a profile constructed from many individually innocuous data points) often falls into definitional gray areas.

A critical finding of this analysis is that data collection from children frequently occurs through intermediary actors schools, educational technology vendors, and even parents themselves (a phenomenon termed "sharenting") rather than through direct child-platform interaction alone. This multiplies the points at which consent would theoretically need to be sought and correspondingly multiplies the points at which consent mechanisms fail or are bypassed entirely. A child has no meaningful opportunity to consent to, or object to, the processing of their data by an educational technology vendor selected by their school under an institutional contract to which the child is not a party, nor to images and information shared about them by parents on social media before they are old enough to have a view on the matter at all. The DPDP Act's broad definition of "child" as under 18, combined with Section 9(1)'s consent requirement, in principle extends India's protective regime further into adolescence than most comparator jurisdictions, though the practical operation of "verifiable" parental consent for a 17-year-old raises its own questions about the displacement problem discussed further in Section 4.5.

The following illustrative diagram conceptualizes the layered nature of data flows affecting a child user, illustrating how multiple actors each potentially subject to different legal regimes intersect around a single child's digital footprint.

Figure 1: Conceptual Map of Data Flows Surrounding a Child User





This conceptual map demonstrates that the regulatory focus on a single consent transaction between a child (or parent) and a single platform fails to capture the networked reality of data flows, where a child's digital footprint is constructed cumulatively and often invisibly across multiple actors and contexts, with consequences that persist well beyond childhood. Notably, the rightmost branch of the diagram data shared by parents about children remains almost entirely

outside the scope of consumer-facing data protection statutes in every jurisdiction examined, since such statutes typically govern commercial processing by "data fiduciaries" or "controllers," categories into which an individual parent posting on their personal social media account generally does not fall.

4.4 Protection: Design Features and Harm Pathways

Protection-oriented analysis must extend beyond content moderation (the traditional focus of child online safety policy, addressed in instruments such as the UK's Online Safety Act 2023 and India's IT Rules 2021) to encompass design features that shape the environment within which children encounter content. Features such as infinite scroll, autoplay, push notifications, streaks and rewards systems, and algorithmically curated recommendation feeds are not neutral conduits for content but active shapers of behavior, attention, and relevant to the privacy dimension data generation, since each interaction with these features produces additional behavioral data that refines profiling.

The Age Appropriate Design Code's Standard 11 ("nudge techniques") and its emphasis on default high-privacy settings (Standard 5) represent a regulatory acknowledgment that design itself can constitute a form of undue influence that undermines the voluntariness presupposed by consent frameworks. However, enforcement of design-based standards has proven considerably more complex than enforcement of disclosure-based standards, as it requires regulators to assess product architecture rather than merely the presence or absence of a privacy notice. The DSA's Article 28(2), by contrast, takes a narrower but more directly enforceable approach prohibiting a specific practice (profiling-based advertising to known minors) rather than mandating a general design philosophy, illustrating a recurring trade-off in this field between broad principle-based obligations (easier to justify, harder to enforce) and narrow rule-based prohibitions (easier to enforce, narrower in scope).

Table 3: Illustrative Regulatory Enforcement Actions Concerning Children's Data (Representative Examples)

Year (approx.)	Regulator/Court	Subject Matter	Outcome (Illustrative)
Late 2010s	US Federal Trade Commission	Video-sharing platform alleged to have collected data from child users without parental consent under COPPA	Multi-hundred-million-dollar settlement; required compliance program changes
Early 2020s	Irish Data Protection Commission (lead EU authority)	Social media platform's handling of child users' data and public-by-default settings	Substantial fine under GDPR; required changes to default privacy settings for minors
Early-to-mid 2020s	UK Information Commissioner's Office	Various platforms assessed for compliance with Age Appropriate Design Code	Formal compliance reviews; public commitments by major platforms to adjust default settings for under-18 accounts
Mid-2020s	US state attorneys general (multi-state litigation)	Allegations that platform design features (e.g., notification patterns, algorithmic feeds) were designed in a manner harmful to minors' mental health	Ongoing litigation in several jurisdictions

Note: This table presents illustrative categories of enforcement activity based on widely reported regulatory patterns; specific case names, dates, and monetary figures should be independently verified against official regulatory decisions for citation purposes.

4.5 Consent: The Conceptual Inadequacy of Binary Models

The analysis suggests that consent, as traditionally operationalized in data protection law a discrete, binary, time-bound transaction is conceptually ill-suited to the continuous, relational, and

developmental nature of childhood. Several specific inadequacies emerge from the comparative statutory analysis in Section 4.2:

The verification problem: GDPR Article 8(2)'s requirement that controllers make "reasonable efforts" to verify parental consent "taking into consideration available technology" has been interpreted variously across member states, with no single agreed verification standard. Similarly, the FTC's COPPA Rule lists multiple acceptable verification methods (signed consent forms, credit card transactions, video conferencing, government ID checks) but acknowledges none is fully reliable. India's DPDP Act requires "verifiable consent" under Section 9(1) without yet having finalized detailed rules on what verification mechanisms will satisfy this standard, leaving considerable implementation uncertainty. Mechanisms for verifying both a user's age and a consenting parent's identity and relationship to the child remain technically imperfect and often require collection of additional sensitive data, creating tension with data minimization principles found in GDPR Article 5(1)(c) and DPDP Act Section 6.

The displacement problem: Parental consent models displace the child's own privacy interests onto the parent, which may be appropriate for very young children but becomes increasingly inappropriate as children approach adolescence and develop privacy interests that may diverge from, or even concern, their parents for example, in cases of household conflict, LGBTQ+ youth seeking information their parents might restrict, or children seeking confidential support services such as helplines for abuse occurring within the home. None of the statutory frameworks examined contain an explicit mechanism for a mature minor to override parental consent decisions in the data protection context, in contrast to some jurisdictions' approaches to medical consent for mature minors.

The circumvention problem: Age thresholds that do not align with the social reality of platform usage among younger children COPPA's age 13, GDPR's 13–16 range create an incentive structure in which children, often with parental knowledge or assistance, misrepresent their age to access age-restricted services, thereby placing themselves outside the protective scope of child-specific regulation entirely and within general adult-oriented terms of service that offer no special protections. Australia's move to a 16-year minimum age for social media access under the amended Online Safety Act represents an explicit policy response to this circumvention problem, shifting the compliance burden to platforms through mandated age-assurance technology rather than relying on self-declared age at registration.

The evolving capacity problem: A binary "child/adult" or even tiered age-band approach (as under GDPR Article 8, or the UK Code's age bands) struggles to capture the genuinely evolving nature of capacity, which varies not only by chronological age but by the specific decision in question a 14-year-old may have well-developed judgment regarding social interactions but limited understanding of long-term data retention and algorithmic inference implications. The Article 5 UNCRC evolving capacities doctrine implies that the appropriate balance of parental and child decision-making authority should itself evolve, yet no statutory framework examined provides a mechanism for this evolution to occur progressively rather than at a fixed threshold age.

4.6 The Participation Gap

A recurring theme across the doctrinal and case study analysis is the near-total absence of children's own voices from the design of the very consent mechanisms, privacy policies, and regulatory frameworks intended to protect them. This stands in some tension with Article 12 of the UNCRC, which guarantees children's right to be heard in matters affecting them, and with General Comment No. 25's paragraph 122, which explicitly calls for states and businesses to consult with children in developing laws, policies, and services relating to the digital environment. Where participatory methodologies have been employed for instance, in some consultations informing the UK's Children's Code and in academic research employing child-centered design methodologies findings suggest that children's own articulated privacy concerns often diverge from adult assumptions. Children frequently express greater concern about peer-to-peer or "social" privacy (such as parents or other adults viewing their content, or peers sharing images without consent) than about commercial or "institutional" data collection by platforms, which they may perceive as abstract, inevitable, or simply not understand at all. This suggests that regulatory frameworks designed exclusively around commercial data protection concerns however important from a legal-structural perspective may not fully align with children's own prioritization of privacy harms, and that participatory consultation, as envisaged by General Comment No. 25, could surface protective priorities currently underrepresented in policy, such as stronger regulation of image-sharing between peers, easier-to-use reporting mechanisms for non-consensual content sharing, and clearer child-facing (rather than parent-facing) explanations of data practices.

5. Discussion

5.1 Toward a Reform Agenda: Protection, Participation, and Policy Innovation

Synthesizing the findings above, this article proposes a tripartite reform agenda structured around the broader theme's three pillars, drawing explicitly on the statutory mechanisms reviewed in Section 2 to identify which existing provisions might serve as templates for broader adoption.

5.1.1 Protection through design mandates rather than disclosure

The comparative analysis suggests that jurisdictions relying primarily on disclosure-based consent (notice-and-consent models, exemplified by the original architecture of COPPA and GDPR Article 8) have proven less effective than those imposing affirmative design obligations such as the UK Age Appropriate Design Code's default high-privacy settings (Standard 5), geolocation defaults (Standard 8), and profiling defaults (Standard 10). A shift toward "protection by design and by default," as articulated in General Comment No. 25 and operationalized albeit unevenly in the UK Code and the DSA's Article 28(2), would relocate the burden of protective action from the child or parent (who must navigate complex settings) to the service provider (who must build privacy-protective defaults). Legislatively, this could be achieved by:

- Extending DSA Article 28(2)'s prohibition on profiling-based advertising to known minors to a broader prohibition on any behavioral advertising to users under a specified age, regardless of the platform's "awareness" of the user's status, shifting the evidentiary burden onto platforms to demonstrate a user is not a minor before serving such advertising.
- Incorporating UK Code-style design standards directly into comprehensive data protection statutes (such as the DPDP Act's forthcoming rules under Section 9) rather than as a separate code of practice, giving such standards the same enforcement weight as core data protection obligations.
- Mandating that connected toys and devices marketed to children (Standard 12 of the UK Code) meet baseline security and data minimization standards as a condition of market access, analogous to product safety regulation for physical toys.

5.1.2 Participation through structured consultation mechanisms

Regulatory bodies and platform developers should institutionalize mechanisms for consulting children in the development of privacy policies, terms of service summaries, and consent interfaces, using age-appropriate participatory research methodologies. This is consistent with both Article 12 of the UNCRC and paragraph 122 of General Comment No. 25, and with practical

design benefits, as products co-designed with their intended users are more likely to function as intended. Concretely, this could involve:

- Statutory requirements for Data Protection Impact Assessments (already mandated under GDPR Article 35 and the UK Code's Standard 14) to include a documented process of child consultation, not merely adult expert assessment of risks to children.
- Regulatory sandboxes of the kind increasingly used in fintech regulation adapted for child-directed digital products, in which children participate in usability and comprehension testing of privacy notices and consent flows prior to market launch.
- Formal advisory bodies, potentially modeled on existing children's commissioners' offices in jurisdictions such as the UK, with a specific statutory mandate to consult children on digital policy and to report findings to data protection regulators.

5.1.3 Policy reform through graduated, multi-dimensional consent models

Rather than a single binary age threshold as found in COPPA's under-13 cutoff or GDPR Article 8's 13–16 range consent frameworks could adopt graduated models that distinguish between types of data processing according to risk and reversibility. For instance:

- Consent for educational content recommendations or non-personalized service functionality could be treated as a lower-risk category requiring lighter-touch consent.
- Consent for behavioral advertising profiles, biometric data collection, or third-party data sharing could be treated as a higher-risk category requiring stronger safeguards, potentially including the DSA-style prohibition regardless of formal consent (since, as discussed, consent itself is of doubtful validity in this context).
- A "consent refresh" mechanism could be built into platform architecture, prompting periodic review for instance, at ages 13, 16, and 18 allowing children to revisit and revise earlier decisions (including decisions made on their behalf by parents under provisions like DPDP Act Section 9(1) or GDPR Article 8(1)) as they mature, operationalizing the evolving capacities doctrine of UNCRC Article 5 in a practically implementable, age-banded form rather than leaving it as an abstract principle.

This graduated approach would also help address the displacement problem identified in Section 4.5, by building in a structural moment at which decision-making authority transfers, partially or wholly, from parent to child, rather than leaving this transition entirely informal and unaddressed by law.

5.2 Cross-Cutting Implementation Challenges

Several implementation challenges cut across all three reform pillars. First, the jurisdictional fragmentation evident in Table 2 different age thresholds, different definitions of "child," different consent mechanisms creates compliance complexity for platforms operating globally and potential regulatory arbitrage, whereby platforms may design products to the lowest common denominator of protection across jurisdictions in which they operate, unless protections are harmonized or platforms adopt a "highest common standard" approach voluntarily (as some platforms have claimed to do by applying UK Code-style protections to under-18 users globally).

Second, the enforcement capacity of regulators varies considerably. The Federal Trade Commission, the Information Commissioner's Office, the Irish Data Protection Commission (as lead authority for many multinational platforms under GDPR's one-stop-shop mechanism), and India's nascent Data Protection Board operate with different resources, different statutory powers, and different degrees of independence, meaning that the on-paper strength of a statutory provision does not necessarily correlate with its practical effect.

Third, the constitutional and rights-based challenges to design-based regulation illustrated by ongoing litigation concerning California's Age-Appropriate Design Code Act on First Amendment grounds suggest that design mandates framed too broadly (e.g., a generalized "duty of care" or "best interests" design obligation without precise definition) may be vulnerable to legal challenge in jurisdictions with strong free expression protections, favoring the more precisely defined prohibitions of instruments like DSA Article 28(2) over broader principle-based codes, at least for the purposes of durable enforceability, even though the broader approach may be conceptually preferable from a child rights perspective.

5.3 Limitations

This analysis is subject to several limitations. First, the rapid pace of both technological change and regulatory development means that specific legislative provisions discussed particularly proposed U.S. federal legislation such as KOSA and COPPA 2.0, and India's DPDP Act rules which remain to be finalized in detail may be superseded or clarified; the analysis should be read as identifying structural patterns rather than providing a definitive snapshot of any single jurisdiction's current law at the time of reading. Second, the reliance on secondary data sources means that figures cited in Tables 1 and 3 are illustrative of general trends rather than precise

current statistics, and readers seeking to cite specific figures should consult primary sources directly. Third, the comparative analysis, while spanning multiple major jurisdictions, cannot capture the full diversity of national approaches, particularly in low- and middle-income countries where digital child rights regulation remains nascent and where the digital divide itself rather than the regulation of digital engagement may be the more pressing child rights concern.

5.4 Directions for Future Research

Future research would benefit from longitudinal studies tracking the long-term consequences of childhood data collection into adulthood, including the persistence of algorithmic profiles constructed during childhood; comparative empirical studies of children's own articulated privacy preferences across cultural contexts, particularly outside the high-income, English-speaking jurisdictions that dominate existing participatory research; and evaluative research on the practical implementation and enforcement outcomes of design-based regulatory approaches such as the UK's Age Appropriate Design Code and India's DPDP Act provisions once their implementing rules are finalized and have been in operation for a sufficient period to permit assessment.

6. Conclusion

The reimagining of child rights in the digital era demands a departure from regulatory models premised on an adult-centric conception of autonomous, informed consent. Children's digital lives are characterized by networked, cumulative, and often invisible data flows spanning direct platform interactions, institutional educational technology relationships, and parental sharing practices that a single consent transaction, however carefully verified, cannot meaningfully govern. The comparative statutory analysis presented in this article, spanning the GDPR's Article 8, the UK's Age Appropriate Design Code and Online Safety Act, the United States' COPPA framework and its proposed successors, India's Digital Personal Data Protection Act 2023, and Australia's emerging access-restriction model, suggests that jurisdictions moving toward design-based protective obligations, broader and more carefully calibrated age thresholds, and graduated consent models are better aligned with the realities of childhood than those relying primarily on disclosure and binary parental consent.

Most fundamentally, however, the analysis underscores that protection and participation are not competing priorities but mutually reinforcing dimensions of child rights, as General Comment No.

25 itself recognizes. Children are more likely to be effectively protected in digital environments whose design reflects their own articulated concerns and developmental realities, rather than environments designed exclusively by and for adults, however well-intentioned the resulting statutory text. Realizing this vision requires sustained collaboration among legislators, platform designers, educators, parents, and critically, and too often absent from the conversation to date children themselves. The next generation of statutory reform, whether through finalization of India's DPDP Act rules, the outcome of pending U.S. federal legislation, or the post-implementation review of the UK's Children's Code and Online Safety Act, represents a significant opportunity to embed this participatory dimension structurally rather than treating it as an aspirational afterthought.

References (Indicative to be verified and formatted per Scopus-indexed journal style, e.g., APA 7th)

United Nations General Assembly. (1989). *Convention on the Rights of the Child*. United Nations Treaty Series, 1577.

United Nations Committee on the Rights of the Child. (2021). *General Comment No. 25 on children's rights in relation to the digital environment*. CRC/C/GC/25.

Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L 119.

Regulation (EU) 2022/2065 (Digital Services Act). *Official Journal of the European Union*, L 277.

Information Commissioner's Office (UK). (2020). *Age appropriate design: A code of practice for online services*.

Data Protection Act 2018 (UK), c. 12.

Online Safety Act 2023 (UK).

Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998); 16 C.F.R. Part 312 (FTC Rule).

California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, Cal. Civ. Code §§ 1798.100 et seq.

The Digital Personal Data Protection Act, 2023 (India), Act No. 22 of 2023.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

The Protection of Children from Sexual Offences Act, 2012 (India), as amended 2019.

Online Safety Act 2021 (Australia, as amended).

Privacy Act 1988 (Australia).

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–670.

Lievens, E., Livingstone, S., McLaughlin, S., O'Neill, B., & Verdoodt, V. (2018). Children's rights and the digital environment. In U. Kilkelly & T. Liefaard (Eds.), *International human rights of children* (pp. 487–513). Springer.

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, 8(4), 197–207.

Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5), 765–779.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.