JAAFR INTERNATIONAL RESEARCH JOURNAL
JOURNAL OF ADVANCE AND FUTURE RESEARCH
JAAFR.ORG | ISSN : 2984-889X
An International Open Access, Peer-reviewed, Refereed Journal

Children's Privacy Rights in Online Platforms

Sayied Nujahat Jahan
Research Scholar
Maharaj Vinayak Global University, Jaipur
Dr. Mani Kumar Meena
Associate Professor
Jaipur School of Law, Maharaj Vinayak Global University, Jaipur

Abstract

In the current digital economy, the structural basis is to constantly extract data through algorithms, which creates serious privacy risks for minors. Global regulatory systems have traditionally sought to address these risks by relying on a rigid notice-and-consent model, effectively outsourcing data protection to parental mediation. However, this doctrinal analysis argues that reliance on verifiable parental consent is practically obsolete. Rather than offering genuine legal protections, these mechanisms serve as loopholes of procedure enabling tech conglomerates to commercially exploit youth under the cover of legal compliance.

This study critically deconstructs the divergent legislative architectures of the United States (COPPA), the European Union (GDPR) and India (DPDP Act) using a strict comparative legal methodology. The analysis reveals a common stagnation of doctrine in these jurisdictions. The US framework incentivises wilful architectural blindness with its arbitrary "actual knowledge" standard. The EU model collapses under the chaotic Article 8 consent thresholds. The Indian model creates severe constitutional friction, imposing stringent prohibitions, which strip away autonomy and run counter to the "best interests" standard of the UNCRC. Moreover, by assessing the theoretical basis of contextual integrity, this study shows the incompatibility of hyper-commodified environments with minor vulnerabilities.

In a rigorous study of recent regulatory enforcement actions, including the landmark FTC intervention against Epic Games and the historic Irish DPC ruling against TikTok, this research shows that digital platforms systematically weaponise their interfaces. Dark patterns and default-to-public settings are deliberately designed by platforms to violate the user's authorisation. The study concludes that to rescue this crisis, legislatures must decisively abandon the illusion of notice-and-choice. Instead, international frameworks should enact mandatory age appropriate design codes modelled on the UK AADC, which legally obligate platforms to incorporate privacy-by-design as an absolute, non-negotiable structural baseline that protects minors by default.

Keywords: Notice-and-consent, Privacy by design, Verifiable parental consent, Dark patterns, Age-appropriate design codes, Doctrinal legal research.

1. Introduction

1.1 The Doctrinal Problem: Beyond Notice and Consent

The architecture of the modern digital economy is based on the extraction, aggregation and commodification of user data, which places disproportionate vulnerabilities on minor internet users.[1] These inherent privacy risks have been addressed through a strict notice and consent approach in legal regimes in the past. This strategy is based on the assumption that parental consent will be able to overcome the extreme lack of information that digital platforms have compared to consumers.[2] Yet, when challenged in court, this doctrinal structure is becoming more and more unworkable. It rests on a pervasive legal fiction, that is the belief that either children are cognitively able to understand intentionally complex privacy policies, or that parents are technically literate enough to be able to meaningfully intercept the ubiquitous data harvesting.

This legal discourse is fundamentally transformed by the *United Nations Convention on the Rights of the Child* (UNCRC), in particular in the form of *General Comment No. 25*.[3] The Comment calls for the "evolving capacities" of the child to be "structured by the environment of the digital world. It is aware that privacy is not just a right that is granted by a tick box consent, but a fundamental right essential for autonomous development. General Comment No. 25 makes a clear statement that the responsibility for data protection should never be delegated to children and/or guardians. Static, binary consent thresholds do not take into account these changing capacities. The statutory reliance on verifiable parental consent is then merely a formality without any real legal protection when platforms deploy hyper-optimised algorithms. The heart of the doctrinal issue is therefore the considerable discrepancy between the goals of global privacy regimes and the way they are implemented, and the fact that they leave minors vulnerable to commercial exploitation.

1.2 Research Questions

This study engages with this dissonance of the statute and seeks to break it down systematically and move the legal conversation forward through the following analytical questions:

1. How do the strict notice and consent procedures set out in existing international laws and conventions limit the overriding jurisprudential principle of the best interests of the child?
2. How are contemporary regulators responding to the weaponisation of deceptive digital architectures, in particular manipulative *dark patterns*, that are being used to systematically circumvent verifiable parental consent requirements?
3. How do the current legislative approaches need to change from a reactive and consent-driven compliance approach to a mandatory approach to age-appropriate design?

1.3 Jurisdictional Scope

A comprehensive and cross-border comparative approach is needed to tackle the intricate fragmentation of children's data rights. This research focuses on a tripartite jurisdictional model, with the aim of directly juxtaposing the world's most powerful regulatory architectures. The United States has a historically sectoral, explicitly age-gated approach with COPPA, which is the first model for verifiable parental consent. On the other hand, the European Union offers a

[1] N Helberger and others, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2021) 45 Journal of Consumer Policy.
[2] Sajda Qureshi, 'Why Data Matters for Development? Exploring Data Justice, Micro-Entrepreneurship, Mobile Money and Financial Inclusion' (2020) 26 Information Technology for Development 201.
[3] UN Committee on the Rights of the Child, 'General Comment No 25 (2021) on children's rights in relation to the digital environment' (2 March 2021) UN Doc CRC/C/GC/25

complete and fundamental rights-based framework through the GDPR, which puts the principles of data minimisation and privacy by design at its heart. Last but not least, India is another critical new paradigm with its recently passed *Digital Personal Data Protection Act*.[4] The Indian framework is an absolute statutory prohibition on the behavioural monitoring of minors, whereas the Western models are consent-based. The Indian framework is quite different from the Western models, which are consent-based, in that it has an absolute statutory prohibition on the behavioural monitoring of minors. This study highlights the specific shortcomings of age-of-consent thresholds in these different legal contexts and brings forward legal norms that are scalable and can withstand fast technological change.

1.4 Doctrinal Methodology

This study takes a black-letter doctrinal and comparative legal approach in order to perform this analysis in a strict manner. It avoids the typical weaknesses of empirical and survey research and adopts a strong normative critique.[5] The inquiry is based solely on the critical reading and interpretation of primary legal documents such as the statutes, international treaties, heavy-handed regulatory enforcement and administrative decisions. The research goes beyond a description of the laws by examining high-stakes regulatory actions, like recent federal trade commission fines, and the *European Data Protection Board* guidelines. Instead, it critically examines the interpretation, enforcement and regular evasion of the law by the technology sector in practice. Peer-reviewed legal scholarship and well-known theoretical works by academics on digital privacy provide much context for this primary data, and these are the secondary sources. This process can be used to build a unified and legally robust case for a paradigm shift towards required structural safety in the digital world.

2. Literature Review

2.1 Concept of Digital Privacy

Solove[6] theorises digital privacy as a complex concept that extends beyond data protection and involves surveillance, information processing, dissemination, and invasion. They state that privacy in the digital era should be perceived as a complex of interdependent issues, but not as an individual concept. This view is especially applicable when it comes to children since their personal information is frequently gathered, processed, and distributed without proper protection. The growing popularity of digital platforms has amplified the issue of informational privacy, particularly as kids engage with applications that gather behavioural and personal data.

Nissenbaum[7] presents the theory of contextual integrity, which states that privacy is ensured when information flows in a manner that meets the expectations and contextual norms. With children, such norms are often broken since online platforms can often apply such data to the purpose not clearly visible to young users. This contextual incompleteness generates ethical issues, especially when children cannot understand the consequences of their data-sharing behaviours. Therefore, when considering the issue of digital privacy among children, there is a need to take the perspective of both technological complexity and developmental constraints.

[4] Age Appropriate Design: A Code of Practice for Online Services (Information Commissioner's Office, 2020) (issued under the Data Protection Act 2018, s 123)
[5] Rodolfo Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law (Installment II of II)' (1991) 39 The American Journal of Comparative Law 343.
[6] Daniel J Solove, 'The Digital Person: Technology and Privacy in the Information Age (Full Text of Book)' (Social Science Research Network, 1 October 2004).
[7] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119.

2.2 Children as Vulnerable Internet Users

Livingstone and Third[8] emphasise that children are one of the most vulnerable groups in the online space because of their developing intellectual capacity and limited awareness of the dangers of the Internet. Their analysis highlights that children do not have the critical skills to navigate privacy settings and evaluate possible dangers, which makes them more vulnerable to the exploitation of their data and online victimisation. The architecture of the digital platforms is another factor that contributes to this vulnerability, as it is usually designed to be engaging rather than secure.

According to Loudon, Boyle and Larsson-Lund,[9] vulnerability of children is not merely a factor of their age but also of their socio-technical environments. They indicate that a large number of digital platforms are not child-friendly, exposing them to more privacy risks. Moreover, children are more willing to disclose personal information, which, in many cases, they do not even know about the repercussions of such disclosure in the long term. Such behaviour enhances the chances of privacy violations, theft of identity and manipulation over the internet.

Montgomery et al. (2017) studied the digital marketing strategies based on data collection and profiling of children. They find that the data of children is often utilised to make elaborate consumer profiles, which poses a question of exploitation and manipulation. The article highlights the importance of a higher set of regulations and increased education of children and their parents to reduce these risks.

2.3 Existing Laws and Policies (COPPA, GDPR-K, etc.)

Kosseff (2014) also gives an in-depth insight into the Children's Online Privacy Protection Act (COPPA)[10] and how it has been used in governing the gathering of personal information related to children below the age of 13. He mentions that although COPPA has been effective in providing minimum guarantees, it has been struggling with enforcement and adaptation to emerging technologies. There are numerous ways of going around these regulations through many online platforms, thus constraining their effectiveness.

Voigt and von dem Bussche[11] argue about the *General Data Protection Regulation* (GDPR), especially the aspects concerning the protection of child data. The GDPR imposes more strict conditions of consent and focuses on transparency, responsibility and the right to forget. The regulation identifies children as a vulnerable population and offers extra protection to safeguard their personal data. The authors, however, state that the success of GDPR is heavily reliant on its adoption and the goodwill of an organisation to adhere to it.

Ermakova, Fabian, and Baumann discuss the usability of privacy policies and discover that the majority of privacy policies are so complicated that users, in particular, children, are unable to comprehend them.[12] This is a challenge to the idea of informed consent, because users cannot make significant choices about their data. This paper indicates that the simplification and increased accessibility of privacy policies should be considered a key factor in enhancing data protection results.

---

[8] Sonia Livingstone and Amanda Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19 New Media & Society 657.

[9] Fiona M Loudoun, Bryan Boyle and Maria Larsson-Lund, 'Children's Experiences of Play in Digital Spaces: A Scoping Review' (2022) 17 PLOS ONE.

[10] Children's Online Privacy Protection Act 1998, 15 USC §§ 6501–6506 (United States)

[11] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) (Springer International Publishing 2017).

[12] Tatiana Ermakova and others, 'Privacy Policies and Users" Trust: Does Readability Matter?' [2014] Twentieth Americas Conference on Information Systems (AMCIS 2014).

2.4 Gaps in the Current Research

The literature is quite critical of the theoretical weaknesses of notice-and-consent approaches, but there is a gap in the doctrinal literature on comparative structural enforcement of notice-and-consent approaches. The current scholarship often looks at COPPA or GDPR without considering parental mediation as part of the problem, and sees it as a failure to implement. Current scholarship often examines COPPA or GDPR without taking parental mediation into account as a problem, and as a failure to implement. Moreover, there is a clear absence of comparative legal analysis comparing these well-established models of consent with the new models of absolute prohibition (such as the Indian DPDP Act) and proactive structural consent (such as the UK AADC). There is a lack of a satisfactory synthesis in the literature to explain how these conflicting statutory structures manage to balance the substantive data protection and the child's right to decisional autonomy. This study attempts to fill this gap by undertaking a doctrinal cross-jurisdictional analysis of the age thresholds, algorithmic tracking and design obligations that are regulated by specific statutory mechanisms.

3. Comparative Legal Architecture

Children's digital privacy is normatively highly fragmented, marked by a rather fundamental tension between a sense of parental responsibility to protect children and a jurisprudential imperative to respect their autonomy. Legislators are dealing with the sneaky nature of algorithmic data extraction and different legislative frameworks have been developed to regulate this vulnerability. This chapter examines the localised mechanisms implemented in the United States, the European Union and India, and finds their structure to be deficient when it comes to substantive data protection, thus revealing the limitations of parental mediation as a legal substitute for substantive data protection.

3.1 The United States: COPPA and the Constraints of Sectoral Age-Gating

COPPA was passed before the advent of algorithmic surveillance capitalism and laid the groundwork for the notice-and-consent model.[13] The key mechanism of operation of the statute is the requirement for operators of commercial websites that are directed to children under the age of thirteen to seek verifiable parental consent before collecting, using or disclosing personal information about children. A careful doctrinal examination of the statute shows that it is on the surface strong, but has serious weaknesses of its own, stemming from its narrow sectoral focus and impossibly high evidentiary standards.

The fatal defect of COPPA is its "actual knowledge" requirement, as clearly stated in §§ 6502(a)(1).[14] In the case of general audience platforms, liability is only for the operator if he or she has actual and express knowledge that a particular user is under the age of thirteen. This statutory language is a recipe for the encouragement of "wilful blindness". Digital platforms strategically design their user interfaces to not get this definitive knowledge, and they may use age neutral screeners, effectively avoiding any compliance obligations altogether. Moreover, COPPA's binary age-gating system leaves a dangerous legal gap for kids age 13-17, leaving them vulnerable to the predatory data collection practices used for adults.[15] The statute assumes the rarely held belief that a 13-year-old is cognitively sophisticated enough to be able to navigate the hyper-complex data ecosystem on their own. The statute is based on the discredited and arbitrary fiction that turning 13 grants the cognitive sophistication necessary to be able to navigate the hyper-complex data ecosystem independently. As a result, rather than being a complete protection from

[13] Vincent Okonkwo, 'Watching the Watchers: Surveillance Capitalism and Why to Solve It' [2025] SSRN Electronic Journal.
[14] Children's Online Privacy Protection Act 1998, 15 USC §§ 6501–6506 (United States)
[15] Federal Trade Commission, 'Children's Online Privacy Protection Rule ("COPPA")' (Federal Trade Commission, 2025).

exploitation, COPPA often serves as a legal protection for technology giants. It enables platforms to monetise the digital trails of teenagers and to sit safely behind artificial compliance hurdles which can be readily overcome.

3.2 The EU: The Article 8 Paradox and the Promise of Privacy by Design

The GDPR aims to overcome the serious sectoral restrictions of the American approach by providing children's data rights in a broad-based, fundamental rights framework.[16] Recital 38 explicitly states that minors require particular heightened protection for their personal data, due to their limited awareness of the risks and consequences of using the data.[17] However, the enforcement of this protection under Article 8 creates a significant doctrinal paradox which could undermine the effectiveness of the whole concept. Article 8 requires parents' consent for processing of a child's data in connection with information society services, but allows for a reduction in the age limit below sixteen, to no less than thirteen years.[18] This legislative exception has resulted in an uncoordinated landscape of divergent consent ages across Europe, and has badly divided the digital single market. More importantly, Article 8 is a transcontinental version of the systemic problems of the consent paradigm. It assumes that parents are technically literate enough to be able to meaningfully mediate their children's digital engagements, an assumption that is empirically challenged by the intentionally opaque and frictionless nature of current data processing architectures.

The real innovation of the GDPR, however, is not in the problematic consent requirements of Article 8, but in the structural and proactive requirements of *Article 25: Data Protection by Design and by Default*.[19] Article 25 puts data minimization and privacy-preserving default settings at the heart of the design of data controllers' platforms. Article 25 gives the statute book teeth to fight against unfair interface designs when read together with the overall "fairness" principle of Article 5(1)(a). This structural approach is becoming more prevalent in a progressive regulatory enforcement. Jurisprudence is starting to see that age gates would be a direct violation of the right to access information, while platforms would need to redesign their platforms by default to comply with best interests.

3.3 India: The DPDP Act and the Paternalistic Prohibition

The recently enacted DPDP Act presents a completely different paradigm, which is highly paternalistic, in the global regulatory landscape. The Act's Section 9 is particularly strict on the processing of children's data, and stands in contrast to the more nuanced approaches in Western jurisdictions.[20] Importantly, the DPDP Act introduces a single, absolute age limit of 18, whereafter data processing of any person under that age requires verifiable parental consent. Section 9(1) is very rigid in its application of consent, but the real legal oddball is in Section 9(3), which makes it a strict law to not track, monitor behaviour and target ads at children.[21] On the protection side, it is a clear-cut law against the monetisation of minors through surveillance. It acknowledges that there is an inherent exploitation of vulnerable users in behavioural profiling. However, subjected to rigorous doctrinal scrutiny, this framework creates severe constitutional and developmental friction. The DPDP Act creates significant tension with the jurisprudential principle

[16] Christopher F Mondschein and Cosimo Monda, 'The EU's General Data Protection Regulation (GDPR) in a Research Context' (Pieter Kubben, Michel Dumontier and Andre Dekker eds, PubMed, 2019).
[17] 'Recital 38 - Special Protection of Children's Personal Data' (General Data Protection Regulation (GDPR)).
[18] 'Art. 8 GDPR – Conditions Applicable to Child's Consent in Relation to Information Society Services | General Data Protection Regulation (GDPR)' (General Data Protection Regulation (GDPR), 2019).
[19] GDPR, 'General Data Protection Regulation (GDPR) – Final Text Neatly Arranged' (General Data Protection Regulation (GDPR), 2013).
[20] Dhanush Prabha, 'DPDP Act 2023 Compliance Guide for Indian Businesses In 2026' (IncorpX, 11 April 2026).
[21] Ankshita Rout, 'DPDP Compliance Framework for Companies in India: From Data Mapping to Incident Response'.

of the evolving capacities of the child as set out in the UNCRC, by making the mental capacity of a 17-year-old equal to that of a toddler.[22]

This legislative overreach essentially stymies the digital independence of adolescents. The age of 18 is an arbitrary age for when parents should have the right to consent to all digital interactions, especially when older minors are seeking information on sensitive, fundamental rights that may require absolute privacy from parents, such as information on reproductive health, mental health support, or educational resources. In this way, the Indian model boldly tries to solve the exploitative pitfalls of algorithmic monitoring but ends up creating a chilling impact on the fundamental rights of adolescents. It tries to solve the problem of commercial surveillance by creating a system of "total" parental surveillance. It seeks to solve the problem of commercial surveillance by creating a system of "total" parental surveillance.

3.4 Integrating the Global Friction

A cross-jurisdictional analysis of COPPA, the GDPR and the DPDP Act reveals a stark difference between the statutory architectures in balancing protection against the evolving capacities of the child. These frameworks resort to broken mechanisms to deal with digital vulnerabilities instead of creating a single international standard. This doctrinal fragmentation is reflected in Table 1 across key regulatory parameters.

Table 1: Comparative Legal Architecture of Minor Data Protection Regimes

Regulatory Parameter	United States (COPPA)	European Union (GDPR)	India (DPDP Act)
Age Threshold	Binary: Under 13.	Fragmented: 13 to 16 (varies by Member State).	Absolute: Under 18.
Parental Consent	Mandated ex-ante, contingent on "actual knowledge".	Mandated under Art. 8, relies on valid guardianship verification.	Mandated universally for all minors under Sec. 9(1).
Profiling and Tracking	Regulated only for under-13s, unrestricted for adolescents.	Subject to general data minimisation and Art. 22 restrictions.	Strictly prohibited for all minors under Sec. 9(3).
Default Settings	Not structurally mandated by statute.	Addressed implicitly via Art. 25 (Privacy by Default).	Not structurally mandated by statute.
Design Obligations	Minimal, focuses on privacy policy transparency.	Strong structural mandate (Art. 25: Privacy by Design).	Focuses on strict behavioural prohibitions rather than design.
Child Autonomy	Ignored for adolescents (13-17 treated as adults).	Partially preserved, dependent on state-level age variations.	Severely restricted, assumes static incapacity until age 18.

This comparative matrix demonstrates that none of the existing systems attain an ideal equilibrium. The strict application of the "actual knowledge" standard and an arbitrary age-13 cutoff point leaves older minors completely vulnerable to targeted profiling, with the focus on industry compliance rather than meaningful adolescent protection.

[22] Ibid. 23

However, the GDPR has a stronger basis in fundamental rights in Article 25, but the messy, state-dependent age thresholds in Article 8 make its procedural use difficult and complicate cross-border enforcement and digital autonomy. The Indian DPDP Act establishes the most stringent framework. It effectively neutralises commercial surveillance by banning tracking by statute and requiring consent until the age of 18, but at the same time causes severe constitutional friction. This leads to a legally frozen view of childhood which clashes with the UNCRC's 'evolving capacities' and exchanges adolescent digital autonomy for total paternalistic safety. Ultimately, this comparative audit demonstrates that statutory regimes must move beyond reliance on parental consent as a primary legal safeguard, and toward unified, structural obligations that embed privacy by design throughout the stages of adolescence.

4. Critical Doctrinal Analysis

4.1 The Weaponisation of Digital Architecture

The doctrinal view of privacy assumes a rational, autonomous user of a computer system who is engaging in a transaction with a provider in a vacuum of law, and based on the classical contract law theory of mutual assent. Today, this legal fiction is being systematically undermined by the use of "dark patterns", user interfaces that are designed in an asymmetric way and carefully crafted using behavioural psychology to manipulate the user's behaviour, in order to increase the amount of data that can be gathered by the algorithm.[23] When used on minors, whose cognitive capabilities and executive functions are still in critical development, these manipulative digital architectures are not only an affront to the ethical spirit of privacy regimes, but also fundamentally question the legal validity of consent itself.

In contemporary law, there are four key elements to a valid legal consent: it must be freely given, it must be specific, it must be informed, and it must be completely unambiguous. When a platform is intentionally designed to cause consent fatigue, to make privacy-enhancing options difficult to locate in the menu, or to punish a privacy-seeking choice with a behavioural "confirmshaming", any consent that is given is "coercive".[24] This reality makes the statutory protection afforded by COPPA and GDPR protection essentially meaningless. The key legal issue uncovered here is that existing legal frameworks tend to control the text of privacy policies and not the underlying code of the platform. This doctrinal defect allows technology firms to easily take advantage of the fact that, on the surface, they are legal and on the ground, they are coercive, making parental mediation nearly impossible.

4.2 FTC v. Epic Games and the Inadequacy of Verifiable Parental Consent

In *FTC v. Epic Games*,[25] the landmark 2022 federal enforcement action, the court's jurisprudential indictment of the verifiable parental consent paradigm clearly illustrates how fragile notice-and-choice models can be in the face of complex, hyper-gamified digital architectures. In addition to an administrative penalty of $245 million for using "dark patterns" to trick users into making unwanted in-game payments, the *Federal Trade Commission* (FTC) issued a $275 million penalty specifically for violating the COPPA. Frictionless ecosystems fail to provide adequate parental supervision, and doctrinally, the FTC's complaint showed that this was a fatal flaw. Epic was clearly targeting and filling its game with children, but it blatantly ignored COPPA's strict consent requirements. The platform did this by

[23] Sakshi Agrawal and Sajith Narayanan, 'When Design Deceives: Consumer Reactions to Dark Patterns in Quick Commerce' (2026) 18 Journal of Indian Business Research 37.
[24] Zachary Hankel, 'Trivializing Values With Dark Patterns: An Ethical Analysis of the Use of Dark Patterns by Social Media...' [2024] ResearchGate.
[25] Federal Trade Commission v Epic Games, Inc No 5:22-cv-00518-BO (EDNC 2022)

deliberately creating a "frictionless" interface that automatically selected the most intrusive data collection options available, thereby turning on live, global text and voice communications without parents' knowledge or consent.

The weight accorded to this particular enforcement is legal, doctrinal and enormous. The regulatory body not only punished an inadequate privacy policy, but also actively penalised the use of a digital environment that used default settings to weaponize highly vulnerable users. The platform's default settings placed children in the public broadcasting arena, where they were subjected to documented and severe psychological and privacy harms, without any prior, verifiable consent from parents. But this administrative judgment is a negative one and of historical importance, and also highlights the reactive, structural shortcomings of the US system. The FTC's action is a corrective measure in response to a broken, ex-ante consent model. It is clear that as long as regulators have to prove that technology companies have deliberately and intentionally misled consumers into using their products without consent, not providing for structural safety by law, then technology companies will continue to take small bits of data from the legally ambiguous grey areas of interface design. The case clearly illustrates that COPPA's limited scope on the point of data collection utterly misses the mark on the ongoing, architectural manipulation of the child user during their digital lives.

4.3 Ireland's DPC TikTok Ruling

On the other hand, European administrative law is starting to take a more aggressive stance on using the GDPR to reorient the law from post-breach enforcement to structural requirements. The Irish *Data Protection Commission's* (DPC) September 2023 landmark decision against TikTok for an unprecedented €345 million administrative fine is illustrative of this vital doctrinal shift.[26] The DPC's forensic investigation uncovered the mechanisms that TikTok relied on to ensure compliance with its architecture, from July to December 2020, and found that the platform's user interface violated the fundamental rights of its minor users. More importantly, the judgment explicitly shifts the focus of regulation from the validity of the consent thresholds of Article 8, to the architectural requirements of Article 25.

The DPC concluded that the company deliberately had "public by default" policies for its users aged 13 to 17. The architecture of the platform allowed for the global public visibility of the minor's creation as soon as it was made, and for it to be algorithmically engaged, a process that the minor had to actively undertake by navigating through complex and counter-intuitive menus in order to retroactively "private" his or her digital footprint. The DPC's doctrinal assessment of this particular interface design was that this was a severe, systemic violation of Article 25 (Data Protection by Design and by Default).[27] TikTok intentionally engineered the cognitive hurdles of sharing information publicly into a barrier while making them the cognitive hurdles of securing the information into a barrier. TikTok's design systematically turned default biases that are adverse to adolescent vulnerabilities into weapons. Moreover, the DPC's decision highlighted the inherent flaw of the parental mediation approach in its comprehensive analysis of TikTok's "Family Pairing" tool, which revealed its problematic nature. In addition, the decision by the DPC deconstructed the problematic nature of the parental mediation approach, as seen in TikTok's "Family Pairing" tool. This enabled adult users to gain access to a minor's account and change sensitive privacy settings without the platform implementing strong and cryptographically secure protocols for verifying the adult's real legal guardianship. This architectural gap directly challenged the GDPR's protection goals, and it's not difficult to see that the out-of-house consent model is very easy to algorithmically subvert and manipulate by bad actors.

[26] Inquiry into TikTok Technology Limited (Irish Data Protection Commission, Decision IN-21-9-1, 1 September 2023)
[27] GDPR, 'General Data Protection Regulation (GDPR) – Final Text Neatly Arranged' (General Data Protection Regulation (GDPR), 2013.

In the end, the DPC decision strengthens the overall fairness principle in Article 5(1)(a), and provides a good ground for a strong legal precedent that digital architectures that give preference to the speed of data extraction over user safety are in principle unlawful, irrespective of how comprehensive the privacy policies can be found in the T&C.[28] This is a significant shift in jurisprudence, from more of a "process" mentality to a "structure" mentality, in that it moves from a focus on "procedural" to "absolute" architectural integrity. The production of these highly aggressive enforcement measures highlights a doctrine-based fact, that is, the consent paradigm is totally irrelevant. The only way to achieve real statutory protection is to stop pretending that it is enough to give notice and choose, and to go back to the principle of "privacy by design", where digital architectures must protect minor vulnerabilities by default, by design, and structurally.

5. Normative Law Reform

5.1 Outside the Protection-Autonomy Binary

The fundamental flaw that undermines contemporary privacy law is the false legislative dichotomy it preserves, the erroneous assumption that safeguarding vulnerable users must come at the cost of severely restricting their digital agency. The statutory requirements of the DPDP Act, and COPPA's binary age-gating, are just two examples of how legislation tends to view child privacy as a zero-sum game between absolute protection and unmediated access. This is not effective in operationalising the UNCRC's mandate. These policies, which are much more reliant on parental permission as the main entry point to the digital world, may unwittingly lead to a view of digital safety as complete parental control.

Thus, in an effort to overcome this doctrinal inertia, legal reform must re-conceive privacy not simply as a defensive shield against data extraction, but as an indispensable prerequisite for autonomous intellectual and social development. This paradigm shift is underpinned by a landmark constitutional jurisprudence established in *Justice K.S. Puttaswamy v. Union of India (2017)*.[29] The Indian Supreme Court has conclusively recognised privacy as an inalienable fundamental right, intrinsically connected to human dignity and decisional autonomy, in *Puttaswamy*. When extended to the digital ecosystem of minors, the *Puttaswamy* doctrine makes it clear that privacy is neither a transactional commodity to be bargained through consent nor a fundamental right that must be structurally guaranteed. The law, therefore, should not compel the child to traverse exploitative architectures to safeguard their dignity. Instead, the law should require platforms to design their environments to promote that dignity by default and by default.

5.2 The UK Age Appropriate Design Code

The most viable doctrinal roadmap to implement this paradigm shift is the *United Kingdom's Age Appropriate Design Code* (UK AADC).[30] Unlike the structurally deficient notice-and-choice models, the UK AADC breaks from the superficiality of consent by converting the "best interests of the child" standard into binding, enforceable architectural mandates. It is based on a novel legal premise. 15. Where a digital service is likely to be accessed by children, the underlying code of that service should actively identify and reduce risks to the fundamental rights of children.

The UK AADC's ban on weaponising interface design effectively rectifies the systemic failures identified in the FTC and DPC enforcement actions. It requires that settings be "high privacy" by default, and prohibits the use of nudge

[28] Damian Clifford, 'The Data Protection Fairness Principle and the GDPR' (Oxford Public International Law, 2022).
[29] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1
[30] ICO, 'Age Appropriate Design: A Code of Practice for Online Services' (ico.org.uk, 19 May 2023).

techniques or dark patterns to entice minors to lower their own privacy protections. It also directly addresses the perilous algorithmic tracking systems fuelling the surveillance economy that must be subject to automatic opt-out of geolocation and profiling, unless there is a compelling and strictly necessary functional reason to be enabled. The UK AADC is doctrinally about making compliance with architecture the focus of regulation, rather than penalties for breaches. The Code calls for structural safeguards, such as *Data Protection Impact Assessments* (DPIAs) that will require platforms to anticipate and minimise risks before introducing child-directed services. It also clearly states that default settings should be set to 'high privacy' and that 'nudge techniques' or 'manipulative designs' to weaken privacy settings should not be used to encourage minors to do so. The AADC places these design obligations on the 'best interests' principle, which means that it is legally binding and must be considered and taken into account in the software development lifecycle, helping to reduce the imbalance of power between platforms and vulnerable users.

5.3 Recommendations for Statutory Global Regimes

In order to secure comprehensive, transnational protection, global legislatures must reject piecemeal amendments and pursue aggressive, normative statutory reforms modelled on the structural safety paradigm. First, jurisdictions must universally eliminate the "actual knowledge" standard that currently hampers enforcement regimes. This statutory loophole must be replaced with a rigorous precautionary principle that applies a strict liability standard to platforms whose user demographics objectively indicate a high likelihood of adolescent engagement, regardless of whether the platform uses superficial age-neutral screeners. "Wilful blindness" in architecture can no longer be a defence in law.

Second, statutory architectures must require rigorous, independent algorithmic impact assessments before any child-directed feature is rolled out. Platforms should be legally required to proactively model and mitigate the psychological and privacy harms of algorithmic recommendations, infinite scrolling, and gamified engagement loops. If these assessments are not carried out and adhered to, punitive administrative fines must be imposed automatically that threaten the core revenue models of non-compliant entities, rather than simply being an acceptable cost of business.

While the DPDP Act's protective intent demands the strict prohibition of behavioural profiling of minors, this prohibition must never be weaponised to digitally exile adolescents or impose absolute parental surveillance on them. Legal structures should clearly guarantee that the deactivation of data monetisation mechanisms does not result in a deterioration of core platform functionalities. The legal separation of service provision from data extraction allows global regimes to finally dismantle the surveillance capitalism machinery aimed at youth. This is done in a manner whereby the digital environment structurally acknowledges youth's considerable vulnerability as well as their basic, changing autonomy.

6. Conclusion

The dominant architecture of children's digital privacy is profoundly broken and essentially hamstrung by a rigid commitment to legal structures that are ill-suited to the realities of modern technology. Through the systematic deconstruction of global statutory paradigms, this doctrinal analysis gives definitive answers to the questions that have been posed at the beginning of this research. The analysis has shown that the traditional notice-and-consent model does not only fail to protect minors but also actively enables their commercial exploitation.

6.1 The Fallacy of Consent and the Best Interests Test

The analysis, in response to the first core research question, confirms that rigid notice-and-consent mechanisms are inherently in violation of the jurisprudential principle of the "best interests of the child". The consent thresholds in the

GDPR and frameworks such as COPPA are based on a seriously flawed legal fiction that parents can adequately mediate hyper-gamified, frictionless data environments. Moreover, the DPDP Act vividly exemplifies that efforts to mitigate this vulnerability via absolute bans on behavioural tracking unwittingly result in a restrictive, zero-sum paradigm. By mandating parental observation until age eighteen, these paternalistic regimes destroy the digital autonomy promised by the UNCRC, substituting safety for a total loss of legal independent agency.

6.2 The Judicial Reality of Algorithmic Exploitation

Regarding the second question, it is evident from the current regulatory enforcement that a shallow compliance with procedural aspects is deadly insufficient. Key administrative actions, including the FTC's aggressive action against *Epic Games* and the landmark Irish DPC ruling against TikTok, illuminate how technology conglomerates systematically weaponise digital architecture to evade verifiable parental consent mandates. The deliberate use of dark patterns and public-by-default settings completely undermines the legal legitimacy of user authorisation. This new jurisprudence establishes an important, firm precedent: not even a thorough, legally watertight privacy policy can save a platform that deliberately designs its interface to take advantage of minors' cognitive vulnerabilities. The focus of regulation is therefore permanently shifting from the text of terms-of-service agreements to the underlying algorithmic code of the platform itself.

6.3 Structural Safety Requirement

This study ultimately argues that the global privacy crisis requires a radical, normative legislative turn. The law needs to shift from reactive, consent-based compliance to mandatory, proactive implementation of age-appropriate design codes to answer the final research question. The UK AADC is a prime example of this necessary doctrinal evolution, which effectively shifts the legal burden of proof away from vulnerable users and squarely onto the technology conglomerates. The world's jurisdictions must close the 20th-century "actual knowledge" loopholes and instead adopt a strict liability standard mandating privacy-by-design as an absolute non-negotiable baseline.

To put it simply, superficial tick-box authorisations will shift regulatory responsibility to parents and will not deliver real digital privacy for minors. The extraction of smooth data in hyper-commodified milieus, as the foundational theoretical frameworks on contextual integrity postulate, is a fundamental violation of the contextual norms expected by vulnerable users. Statutory frameworks need to protect the right to decisional autonomy and legally require digital platforms to internalise the true costs of child protection. The law can only ensure the digital ecosystem finally respects the deep vulnerability and developing capacities of its youngest users if it abandons the fiction of consent and enforces architectural integrity from the bottom up.

7. Bibliography

7.1 Primary Sources

Table of Cases

Federal Trade Commission v Epic Games, Inc No 5:22-cv-00518-BO (EDNC 2022)

Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1

Table of Legislation and Statutory Instruments

Age Appropriate Design: A Code of Practice for Online Services (Information Commissioner's Office, 2020) (issued under the Data Protection Act 2018, s 123)

Children's Online Privacy Protection Act 1998, 15 USC §§ 6501–6506 (United States)

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

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Table of Administrative and Regulatory Decisions

Inquiry into TikTok Technology Limited (Irish Data Protection Commission, Decision IN-21-9-1, 1 September 2023)

Table of International Instruments

UN Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3

UN Committee on the Rights of the Child, 'General Comment No 25 (2021) on children's rights in relation to the digital environment' (2 March 2021) UN Doc CRC/C/GC/25

7.2 Secondary Sources

Journal Articles

Agrawal S and Narayanan S, 'When Design Deceives: Consumer Reactions to Dark Patterns in Quick Commerce' (2026) 18 Journal of Indian Business Research 37 <https://doi.org/10.1108/jibr-05-2025-0188> accessed 2 September 2026

Dhanush Prabha, 'DPDP Act 2023 Compliance Guide for Indian Businesses In 2026' (*IncorpX*, 11 April 2026) <https://www.incorpx.io/guide/dpdp-act-2023-compliance-guide-businesses> accessed 2 September 2026

Ermakova T and others, 'Privacy Policies and Users" Trust: Does Readability Matter?' [2014] Twentieth Americas Conference on Information Systems (AMCIS 2014) <https://www.researchgate.net/publication/262563357_Privacy_Policies_and_Users> accessed 2 September 2026

Federal Trade Commission, 'Children's Online Privacy Protection Rule ("COPPA")' (*Federal Trade Commission*, 2025) <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> accessed 2 September 2026

Hankel Z, 'Trivializing Values With Dark Patterns: An Ethical Analysis of the Use of Dark Patterns by Social Media...' [2024] ResearchGate <https://doi.org/10.13140/RG.2.2.29170.31689> accessed 2 September 2026

Helberger N and others, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2021) 45 Journal of Consumer Policy <https://doi.org/10.1007/s10603-021-09500-5>

Livingstone S and Third A, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19 New Media & Society 657 <https://doi.org/10.1177/1461444816686318> accessed 2 September 2026

Loudoun FM, Boyle B and Larsson-Lund M, 'Children's Experiences of Play in Digital Spaces: A Scoping Review' (2022) 17 PLOS ONE <https://doi.org/10.1371/journal.pone.0272630> accessed 2 September 2026

Mondschein CF and Monda C, 'The EU's General Data Protection Regulation (GDPR) in a Research Context' (Pieter Kubben, Michel Dumontier and Andre Dekker eds, *PubMed*, 2019) <https://www.ncbi.nlm.nih.gov/books/NBK543521/> accessed 2 September 2026

Nissenbaum H, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119 <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/> accessed 2 September 2026

Okonkwo V, 'Watching the Watchers: Surveillance Capitalism and Why to Solve It' [2025] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.5836102> accessed 2 September 2026

Qureshi S, 'Why Data Matters for Development? Exploring Data Justice, Micro-Entrepreneurship, Mobile Money and Financial Inclusion' (2020) 26 Information Technology for Development 201 <https://doi.org/10.1080/02681102.2020.1736820>

Rout A, 'DPDP Compliance Framework for Companies in India: From Data Mapping to Incident Response' <https://doi.org/10.2139/ssrn.7056638> accessed 2 September 2026

Sacco R, 'Legal Formants: A Dynamic Approach to Comparative Law (Installment II of II)' (1991) 39 The American Journal of Comparative Law 343 <https://doi.org/10.2307/840784>

Solove DJ, 'The Digital Person: Technology and Privacy in the Information Age (Full Text of Book)' (*Social Science Research Network*, 1 October 2004) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899131> accessed 2 September 2026

Voigt P and Bussche A von, *The EU General Data Protection Regulation (GDPR)* (Springer International Publishing 2017)

Websites

Art. 8 GDPR – Conditions Applicable to Child's Consent in Relation to Information Society Services | General Data Protection Regulation (GDPR) (*General Data Protection Regulation (GDPR)*, 2019) <https://gdpr-info.eu/art-8-gdpr/> accessed 2 September 2026

Clifford D, 'The Data Protection Fairness Principle and the GDPR' (*Oxford Public International Law*, 2022) <https://opil.ouplaw.com/display/10.1093/law-oeeul/law-oeeul-e137?p=emailAogE8H2IivqW6&d=/10.1093/law-oeeul/law-oeeul-e137&print> accessed 2 September 2026

GDPR, 'General Data Protection Regulation (GDPR) – Final Text Neatly Arranged' (*General Data Protection Regulation (GDPR)*, 2013) <https://gdpr-info.eu/art-25-gdpr/> accessed 2 September 2026

ICO, 'Age Appropriate Design: A Code of Practice for Online Services' (*ico.org.uk*, 19 May 2023) <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 2 September 2026

Recital 38 - Special Protection of Children's Personal Data (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/recitals/no-38/> accessed 2 September 2026