CHILDREN'S DATA PRIVACY UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 - ARE INDIAN CHILDREN ADEQUATELY PROTECTED?

K. Anu Priyanka, PhD Scholar, Tamil Nadu Dr. Ambedkar Law University Chennai

ABSTRACT

When a child in Chennai opens DIKSHA to study or a teenager in Mumbai scrolls through Instagram before bed neither of them knows that every click, every pause and every search is being recorded, stored and in many cases sold. India's lawmakers saw this problem and tried to address it through Section 9 of the Digital Personal Data Protection Act 2023.[1] But the provision they produced leaves too much unsaid. Platforms are told to get parental consent but not how to check it is real. They are told not to harm children's well-being but not what harm looks like. They are told not to track children but there is no way to enforce this against platforms sitting outside India. Certain platforms are exempted from these rules through a schedule that nobody has yet published. Others may process children's data without consent if their processing is safe a concept the Rules have not defined. This paper goes through each of these failures, shows through the DIKSHA breach what they cost in practice and sets out the specific changes that would make Section 9[2] worth the paper it is written on.

Keywords: Children's Data Privacy, DPDP Act 2023, Section 9, DIKSHA, Parental Consent, Right to Privacy.

[1]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[2]Section 9, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

I. INTRODUCTION

Every school going child in India today has a digital footprint. A ten year old using DIKSHA for homework, a thirteen year old on YouTube and a sixteen year old on Instagram are all generating personal data every minute they spend online. Platforms use this data in ways that most parents would find alarming if they understood them. A child's viewing history tells a platform exactly which type of content will keep that child watching longest. An eleven year old's search patterns tell an advertiser exactly which products to push. None of this is disclosed in language that a parent or child can meaningfully understand. With approximately 250 million children below eighteen years of age India has one of the largest child user bases in the world and the commercial incentive for platforms to exploit this data is enormous.

The Digital Personal Data Protection Act 2023[3] is India's first attempt at comprehensive data protection law. Section 9 of this Act deals specifically with children. It covers parental consent, harmful processing and behavioural monitoring. On first reading it looks like a serious attempt at protection. On closer reading it turns out that almost every protective provision has a gap where the real protection should be. This paper works through those gaps one by one, uses the DIKSHA breach to show what they mean in practice and makes specific recommendations for what Parliament must do to fix them.

II. SECTION 9 OF THE DPDP ACT 2023: WHAT THE LAW SAYS

Section 9 carries the heading Processing of Personal Data of Children and is divided into five sub-sections each dealing with a different aspect of how platforms must handle children's data. Section 9(1)[4] puts the parental consent requirement at the centre of the framework before processing a child's personal data a Data Fiduciary must obtain verifiable consent from the parent or lawful guardian. How exactly that verification must happen is left to future Rules. The sub-section adds that processing must happen in a manner that protects the rights and best interests of the child a standard that sounds meaningful but is not defined anywhere in the Act.

Section 9(2)[5] prohibits processing that is likely to cause any detrimental effect on the well-

[3]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The Act was passed by Parliament on August 7, 2023 and received Presidential assent on August 11, 2023.
[4]Section 9(1), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023): Before processing any personal data of a child, every Data Fiduciary shall obtain verifiable consent of the parent or the lawful guardian of such child in such manner as may be prescribed.
[5]Section 9(2), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023): No Data Fiduciary shall

being of a child. This goes beyond regulating how data is collected and addresses the impact of processing on the child directly.

Section 9(3)[6] targets the practices that platforms find most profitable tracking children's behaviour, building profiles of their interests and using those profiles to push advertising at them. Prohibiting these practices is the right instinct but the prohibition is only as strong as the enforcement behind it.

Section 9(4)[7] gives the Central Government power to exempt certain Data Fiduciaries from both the parental consent requirement and the prohibition on behavioural monitoring but only those specifically listed in the Fourth Schedule.

Section 9(5)[8] carves out a further exception some Data Fiduciaries may process children's data without parental consent if their processing qualifies as safe under criteria to be set by the Central Government.

Reading Section 9 as a whole gives the impression of a comprehensive protective framework but that impression does not survive contact with the details.

III. FIVE CRITICAL GAPS IN SECTION 9

3.1 Section 9(1): Verifiable Consent Without Any Standard

The word verifiable carries the entire weight of Section 9(1)'s protective function. It tells us that consent must be confirmed rather than merely claimed but it tells us nothing about how that confirmation must happen. The manner of verification is left entirely to future Rules and the DPDP Rules 2025[9] which were notified in November 2025 also do not prescribe any

undertake processing of personal data that is likely to cause any detrimental effect on the well-being of a child.

[6]Section 9(3), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023): No Data Fiduciary shall undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

[7]Section 9(4), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The Central Government may, by notification, exempt such classes of Data Fiduciaries as may be specified in the Fourth Schedule from the application of sub-section (1) and (3).

[8]Section 9(5), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). Certain classes of Data Fiduciaries may be permitted to process children's personal data without verifiable parental consent if such processing is considered safe as may be prescribed.

[9]The Digital Personal Data Protection Rules, 2025 were notified by the Ministry of Electronics and Information Technology on November 13, 2025 and published in the Gazette of India on November 14, 2025. The Rules do not prescribe any specific technical standard for verifiable parental consent verification under Section 9(1).

specific technical standard.

This matters enormously in practice. A child who wants to sign up for a platform can simply enter a false date of birth and proceed. A platform that wants to meet the technical requirements of the provision can offer a checkbox asking users to confirm they are parents and accept that as verifiable consent. Without a prescribed standard there is nothing to stop either of these outcomes.

The United States addressed this directly in the Children's Online Privacy Protection Act[10] which lists specific acceptable verification methods signed consent forms, credit card transactions, telephone calls, video conferencing and government ID verification. India's Section 9(1) has no equivalent list. Until the Rules prescribe a clear standard the consent requirement will remain easy to circumvent.

3.2 Section 9(2): A Prohibition With No Definition

Section 9(2)[11] says that processing likely to cause detrimental effect on a child's well-being is prohibited. The protection sounds strong until you ask what detrimental means and discover that the Act does not say. This silence creates real problems. A platform whose algorithm keeps pushing disturbing content to a twelve year old can say the algorithm just responds to what the child clicks and any harm that follows is not the platform's fault. A platform that keeps a fourteen year old awake until two in the morning through addictive design can say parents should be setting screen time limits at home. Without a definition of detrimental effect neither of these arguments can be decisively rejected.

Research on children's digital well-being has documented a consistent pattern of harm recommendation algorithms pushing self-harm content to vulnerable teenagers, advertising systems creating body image problems in young girls and platform designs engineered to maximise engagement at the cost of sleep and academic performance. Each of these outcomes is a detrimental effect on a child's well-being in any reasonable understanding of the phrase. But Section 9(2) does not use a reasonable understanding it uses no understanding at all. The

[10]Children's Online Privacy Protection Act, 1998 (United States of America) as amended in 2013. The Act lists specific acceptable methods for verifiable parental consent including signed consent forms, credit card transactions, telephone calls, video conferencing and government ID verification.
[11]Section 9(2), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The provision does not define what constitutes detrimental effect on the well-being of a child leaving significant ambiguity in enforcement.

Data Protection Board cannot enforce what Parliament has not defined and Parliament has not defined detrimental effect anywhere in the Act and that is a position no enforcement authority should be placed in. The United Kingdom's Age Appropriate Design Code[12] avoided this problem by listing specific categories of harm that platforms must guard against. India's provision needs the same specificity.

3.3 Section 9(3): Strong Rules That Cannot Reach Foreign Platforms

Tracking, behavioural monitoring and targeted advertising are how platforms make money from children and Section 9(3) goes directly after these practices. The provision is welcome but it has an enforcement problem that the Act does not address. Most platforms that Indian children use every day YouTube, Instagram, Snapchat, gaming platforms are headquartered outside India. Section 3 of the DPDP Act[13] gives the law extraterritorial reach when processing is connected to offering goods or services to persons in India. But extraterritorial jurisdiction in the statute does not automatically translate into effective enforcement against platforms sitting in California or Singapore.

India has no data cooperation agreements with the countries where these platforms operate. There is no mechanism for compelling foreign platforms to respond to enforcement actions by the Data Protection Board. The European Union has built enforcement cooperation into its data protection framework over decades. India is starting from scratch and Section 9(3) does not acknowledge this problem at all.

3.4 Section 9(4): Exemptions From an Unpublished Schedule

Section 9(4) allows the Central Government to exempt certain Data Fiduciaries from the parental consent requirement and from the prohibition on behavioural monitoring and targeted advertising. These exemptions are to be listed in the Fourth Schedule to the Act.[14]

[12]Information Commissioner's Office, Age Appropriate Design Code (United Kingdom, 2021) available at https://ico.org.uk (last visited May 14, 2026). The Code specifies fifteen design standards that platforms must meet to protect children including high privacy settings as default and prohibition on nudge techniques.
[13]Section 3, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The Act applies to processing of digital personal data within India and also to processing outside India if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.
[14]Section 9(4) read with the Fourth Schedule, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The Fourth Schedule which lists the classes of Data Fiduciaries exempt from Section 9(1) and Section 9(3) requirements has not been published as of the date of writing.

The Fourth Schedule has not been published. It was not published with the Act in August 2023. It was not included in the DPDP Rules 2025 notified in November 2025. The continued non-publication means that nobody not parents, not platforms, not civil society and not the Data Protection Board knows which platforms are exempt from the most important children's data protection provisions in Indian law.

This gap goes to the heart of the provision. Platforms that should be getting parental consent can point to the missing schedule and claim they might be exempt. Platforms that are genuinely exempt cannot point to anything at all. Both situations are the direct result of the Central Government's failure to publish the Fourth Schedule and that failure must be corrected urgently.

3.5 Section 9(5): Safe Processing as an Empty Exception

Section 9(5) adds another layer of complexity by carving out an exception to parental consent for Data Fiduciaries whose processing is classified as safe. Safe processing is to be defined by the Central Government through Rules. The DPDP Rules 2025 do not define it.[15]

The result is that Section 9(5) currently reads as permission for certain platforms to process children's data without parental consent but nobody knows which platforms or what conditions apply. This gap goes to the heart of the provision. An exception to parental consent that comes with no definition of its own scope is not really an exception at all it is an invitation to platforms to argue that whatever they do qualifies as safe. The Rules must close this gap before Section 9(5) can function as intended.

IV. THE DIKSHA DATA BREACH: WHAT HAPPENS WHEN GAPS ARE LEFT UNADDRESSED

DIKSHA was launched by the Government of India in 2017 as the national digital platform for school education. By 2022 it had over 150 million registered users the majority of whom were school children. In 2022 and 2023 it was reported that DIKSHA had exposed the personal data of approximately six lakh students including names, ages, school details and usage patterns. More seriously it was reported that DIKSHA had passed children's data to third party

[15]Section 9(5), The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The Digital Personal Data Protection Rules, 2025 do not define safe processing for the purposes of this sub-section.

advertisers without informing children or their parents.[16]

The DIKSHA breach illustrates every gap in Section 9 at the same time. The platform did not obtain verifiable parental consent before collecting children's data illustrating the gap in Section 9(1). Sharing children's data with advertisers caused detrimental effects on their well-being illustrating the gap in Section 9(2). The platform engaged in behavioural monitoring of children illustrating the gap in Section 9(3). As a government platform DIKSHA may have claimed exemption under the yet unpublished Fourth Schedule illustrating the gap in Section 9(4). And there was no definition of safe processing to constrain how it handled children's data illustrating the gap in Section 9(5).

The DIKSHA breach also raises serious constitutional concerns. The Supreme Court of India recognised in Justice K.S. Puttaswamy v. Union of India 2017[17] that the right to privacy is a fundamental right under Article 21 of the Constitution. Children have the same right to privacy as adults and in many ways require stronger protection because they are unable to fully understand or consent to the processing of their personal data.When a government platform passes children's personal data to advertisers without telling their parents it strikes at the very core of what Article 21 protects.

The DIKSHA breach also raises questions under Article 14 of the Constitution[18] which guarantees the right to equality and prohibits arbitrary action by the State. State action that disadvantages citizens without any published legal basis is exactly what Article 14 exists to prevent and DIKSHA's conduct falls squarely within that description. The absence of a clear legal framework under Section 9 enabled this arbitrary action.

V. COMPARATIVE ANALYSIS

5.1 United States: Children's Online Privacy Protection Act 1998

The United States dealt with this problem a generation ago. By the late 1990s American

[16]Ministry of Education, Government of India, DIKSHA Platform available at https://diksha.gov.in (last visited May 14, 2026). In 2022 and 2023 it was reported that DIKSHA exposed personal data of approximately six lakh students and shared children's data with third party advertisers without parental consent.
[17]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. A nine-judge constitutional bench of the Supreme Court of India unanimously held that the right to privacy is a fundamental right protected under Article 21 of the Constitution of India.
[18]Article 14, Constitution of India: The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India.

children were going online in large numbers and platforms were collecting their data freely. Congress passed the Children's Online Privacy Protection Act in 1998[19] to stop this. The Act covers websites and services directed at children under thirteen and makes verifiable parental consent mandatory before any personal information can be collected. What separates COPPA from India's Section 9(1) is that COPPA does not leave verification undefined. It tells operators exactly what will count a signed consent form, a credit card transaction, a phone call, a video conference, a government ID check. India's provision uses the same word verifiable but provides none of this guidance.

What makes COPPA work is not its intentions but its specificity. By listing exactly which verification methods are acceptable the law removes the ambiguity that platforms would otherwise exploit. The FTC's 2019 penalty of 170 million dollars against Google and YouTube[20] for COPPA violations is instructive not just as a deterrent but as evidence that enforcement is possible when the law is clear enough to know when it has been violated. India's Data Protection Board cannot build a similar enforcement record until India's law gives it equally clear standards to enforce.

5.2 European Union: GDPR and Age Appropriate Design Code

Europe approached the problem differently. Under the GDPR[21] children under sixteen cannot give valid consent to data processing on their own parental or guardian consent is needed instead. Individual member states have some flexibility to lower this threshold but the floor is thirteen and no member state can go below it. The United Kingdom went further with its Age Appropriate Design Code[22] which requires platforms to design their services with children's best interests in mind from the outset not as an afterthought.

[19]Children's Online Privacy Protection Act, 1998 (United States of America) as amended in 2013. The Act applies to operators of websites and online services directed at children under thirteen years of age.

[20]Federal Trade Commission v. Google LLC and YouTube LLC, Case No. 19-cv-2642 (United States District Court, District of Columbia, 2019). The FTC imposed a penalty of 170 million dollars on Google and YouTube for illegally collecting personal information from children without verifiable parental consent in violation of COPPA.

[21]Article 8, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) OJ L 119 (European Union, 2016). Where a child is below the age of sixteen years the processing of personal data of such child shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility.

[22]Information Commissioner's Office, Age Appropriate Design Code (United Kingdom, 2021) available at https://ico.org.uk (last visited May 14, 2026). The Code requires platforms to design their services with children's best interests as a primary consideration and specifies fifteen design standards including high privacy by default and no use of nudge techniques.

The Code specifies fifteen design standards including high privacy settings as the default for children, no use of nudge techniques to push children towards sharing more data and no use of children's data in ways that have been shown to harm their health or well-being. This moves the conversation from consent to design asking not just whether parents agreed but whether the platform itself was built to protect children.

5.3 What India Can Learn

What both of these frameworks demonstrate is that writing protective language into a statute is only the beginning. The United States learned that verifiable consent requires a list of specific methods. The European Union learned that consent alone is not sufficient and that platform design must itself be child-safe. India's Section 9 has the right intentions but needs the specific content that would make those intentions enforceable.

VI. CONSTITUTIONAL ANALYSIS

6.1 Article 21: Right to Privacy

In Justice K.S. Puttaswamy v. Union of India 2017[23] a nine-judge bench of the Supreme Court held unanimously that privacy is a fundamental right under Article 21 of the Constitution. The court was clear that privacy is not something the Constitution grants it is something the Constitution recognises as already belonging to every person by virtue of their humanity. Children are persons. They hold this right as fully as adults do.

The processing of children's personal data without verifiable parental consent, the sharing of children's data with advertisers, the behavioural monitoring of children and the targeting of advertising at children are all potential violations of the right to privacy of children under Article 21. The gaps in Section 9 of the DPDP Act 2023 mean that these violations can occur without any effective legal remedy.

6.2 Article 14: Right to Equality

Article 14 of the Constitution[24] guarantees the right to equality and prohibits arbitrary action

[23]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. The court held that privacy is not something the Constitution grants but is a natural right that inheres in every individual by virtue of their humanity and is protected under Article 21.

[24]Article 14, Constitution of India. The Supreme Court has consistently held that any executive action that is

by the State. The non-publication of the Fourth Schedule to the DPDP Act 2023[25] is an arbitrary exercise of executive power. It creates a situation where certain platforms may claim exemption from children's data protection requirements without any published legal basis for that exemption.

Similarly the failure to define detrimental effect on well-being and safe processing gives Data Fiduciaries and the Central Government unconstrained discretion that can be exercised arbitrarily. This unconstrained discretion is itself a potential violation of Article 14.

VII. RECOMMENDATIONS

The most pressing reform needed is a clear technical standard for verifiable parental consent under Section 9(1). The Rules must specify which verification methods are acceptable government ID verification, Aadhaar based verification, digital signature based consent and video conferencing should all be included. A parent ticking a checkbox or a child pretending to be their own parent must not satisfy this requirement.

Section 9(2) needs a definition of detrimental effect on well-being that legislators are currently avoiding. Parliament must amend the provision to specifically cover algorithmic exposure to harmful content, psychological harm from engagement-maximising design, financial harm from targeted advertising and physical harm from addictive platform features. Without this specificity the prohibition is a statement of good intentions rather than an enforceable legal standard.

Enforcing Section 9(3) against foreign platforms requires mechanisms that the Act currently lacks. In my opinion the DPDP Rules must give the Data Protection Board power to direct internet service providers to block access to persistently non-compliant platforms and to impose penalties on Indian representatives of foreign platforms. Because India cannot directly compel foreign companies to appear before its regulatory authorities it must work through intermediaries within its jurisdiction. These are not novel tools they are adaptations of enforcement mechanisms India already uses in other contexts.

arbitrary, unreasonable or not based on any intelligible principle is violative of Article 14.

[25]Section 9(4) read with the Fourth Schedule, The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). The non-publication of the Fourth Schedule is an arbitrary exercise of executive power that creates legal uncertainty for platforms, parents and regulators alike.

The Fourth Schedule must be published. The continued non-publication means that the entire exemption framework under Section 9(4) is operating in legal uncertainty and that uncertainty benefits platforms rather than children.

Safe processing under Section 9(5) must be defined with enough precision to be enforceable. The Rules must specify which Data Fiduciaries qualify, what conditions apply and what ongoing oversight mechanism will ensure continued compliance. A definition that is vague enough to cover anything protects no one.

VIII. CONCLUSION

Section 9 of the Digital Personal Data Protection Act 2023 is the first time Indian law has specifically addressed children's data protection. That matters. But a provision that identifies the right problems and then leaves them all undefined is not yet a solution.

The DIKSHA breach involved six lakh children whose personal data was shared with advertisers without anyone's knowledge or consent. That happened before Section 9 existed. The question this paper has been asking is whether Section 9 as currently drafted would have prevented it and the honest answer is that it is not clear that it would. India has 250 million children in the digital space whose data is commercially valuable to platforms that have every incentive to collect it and limited reason to handle it carefully. They need a law that actually constrains those platforms.

The reforms this paper recommends are not complicated. They are specific. They require the Central Government to publish a schedule it has already promised to publish, to define terms it has already used without defining them and to prescribe standards it has already committed to prescribing. The question is not whether these reforms are possible. The question is whether they will happen before the next breach.

REFERENCES

I. STATUTES

1. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)

2. The Digital Personal Data Protection Rules, 2025 (notified November 13, 2025)

3. Children's Online Privacy Protection Act, 1998 (United States of America) as amended in 2013

4. 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 (General Data Protection Regulation) OJ L 119 (European Union, 2016)

5. Constitution of India, Articles 14 and 21

II. CASES

6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

7. Federal Trade Commission v. Google LLC and YouTube LLC, Case No. 19-cv-2642 (United States District Court, District of Columbia, 2019)

III. REPORTS AND OFFICIAL DOCUMENTS

8. Ministry of Electronics and Information Technology, Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018)

9. Internet and Mobile Association of India, India Internet Report 2023 available at https://www.iamai.in (last visited May 14, 2026)

10. Information Commissioner's Office, Age Appropriate Design Code (United Kingdom, 2021) available at https://ico.org.uk (last visited May 14, 2026)

11. Ministry of Education, Government of India, "DIKSHA Platform" available at https://diksha.gov.in (last visited May 14, 2026)

IV. JOURNAL ARTICLES

12. Pavan Duggal, "Cyber Law and Data Protection in India" 54 Journal of Indian Law Institute 201 (2012)

13. Vrinda Bhandari, "The Digital Personal Data Protection Act 2023: A Critical Analysis" 1 Indian Law Review 1 (2024)