# Consent in Childhood:

## Parental Control under India's DPDPA vs Children's Evolving Autonomy Online

**Prepared By: PIIR Foundation**

Proto Infans Internet Rights Foundation
www.piirf.org | 9782032358 | salik@piirf.org

# Abstract

India's Digital Personal Data Protection Act, 2023 (DPDPA) treats every person below eighteen as a single legal category. In that design, verifiable parental consent becomes the default legal key for processing children's personal data, while certain high-risk practices for children are restricted or prohibited. On paper, this reads as a tidy safety-first approach. In lived digital life, especially for teenagers, it creates a sharp mismatch. Adolescents routinely make fast, interface-led decisions about permissions, visibility, messaging, location and spending prompts, often without a parent present. The result is not just routine non-compliance; it is a predictable split between how the law imagines consent (parent-as-gatekeeper) and how consent is actually encountered (repeated taps inside product design).

This study examines that gap through a child-rights lens and through field evidence from Jaipur. First, it reads the DPDPA's child-consent architecture against global standards that explicitly recognise children's evolving capacities and their right to exercise autonomy in line with maturity, particularly the UN Convention on the Rights of the Child (UNCRC) and the Committee's General Comment No. 25 on children's rights in relation to the digital environment. These standards do not erase parents; they position parents as enabling guidance that evolves from control to support, while also placing responsibility on states and digital services to embed the best interests of the child into governance and design. The project also situates India's approach alongside privacy frameworks that combine age-calibrated rules with design obligations, including the GDPR's child-consent provisions, the UK Age Appropriate Design Code, and regulator guidance that emphasises privacy-by-default and limits on profiling for

children.

Second, the study grounds the debate in primary data collected through personal interviews with 200 school students in Jaipur, Rajasthan, over a three-month period. Respondents were drawn from different schools across the city, predominantly English-medium schools. This sampling choice was deliberate: these students generally have greater access to smartphones and social media features, and therefore confront a higher volume of everyday "consent" encounters. The instrument covered device access (personal or shared), who set up primary accounts, daily time online, weekly apps used, interpretations of "consent", immediate reactions to permission prompts (camera, microphone, contacts, location, notifications, photos), preferences on who should decide permissions, experiences of changing defaults (account visibility, direct messages, location sharing, ads or sponsored content, and in-app spending prompts), experiences of entering an inaccurate age to create accounts, and perceptions about parental capability in managing app settings.

The findings show a consistent pattern. Teenagers overwhelmingly describe consent in recognisable terms: being asked, giving permission, and having the option to say yes or no. Yet they experience consent less as a meaningful moment and more as a stream of friction screens designed to keep the app moving. Decisions cluster around defaults and "risky" features (open DMs, public profiles, geolocation, spending prompts) that shape safety and exposure. A significant share report entering a fake age at least once to create an account, demonstrating how a binary "child vs adult" architecture pushes teens toward age-bypass rather than safer pathways. Teens also report that parents are not consistently better at navigating settings, which matters

because a model built primarily on parental gatekeeping assigns the hardest privacy work to an actor with limited product support. Importantly, many teens prefer a shared approach: autonomy in routine, low-risk choices, and parental involvement at decision-points that carry clear risk or confusion.

Building on these results, the project argues that the consent debate is, in practice, a design and accountability debate. If the policy goal is meaningful choice and protection, it cannot depend solely on parental consent while leaving platforms free to ship risky defaults and persuasive nudges. The project therefore proposes a tiered shared-consent model for India that differentiates by age band and by processing-risk tier. In this model, routine core-use decisions shift toward teen self-consent as capacity grows, while high-risk features trigger shared checkpoints (clear consequence explanations, cooldown windows, and easy routes to invite a parent into that specific decision). Across tiers, platforms carry stronger privacy-by-default obligations and stricter limits on profiling and behavioural advertising.

Overall, the study offers a practical pathway for implementing children's data protection in India that reduces incentives for age-gate bypass, respects adolescent autonomy as a rights issue, and tightens safety where risk is real.

Keywords: children's data; consent; DPDPA; evolving capacities; age-appropriate design; UNCRC; General Comment No. 25; adolescents; shared decision-making; privacy by default.

# Table of Contents

# Chapter 1: Consent, Autonomy, and the Myth of the Always-Aware Parent

If you listen to how teenagers talk about apps, they rarely talk about "data". They talk about streaks, DMs, getting added to groups, the awkwardness of a public profile, the pressure of a purchase popup, or a map that shows where they are. Those are the lived forms of data processing. Privacy is not a policy page to them, it is a design choice that lands on their phone as a default and forces a quick decision.

The DPDPA creates a simple legal story: when the "Data Principal" is a child, the parent or lawful guardian steps into the child's shoes for the purpose of consent.[1] That story is tidy on paper. In practice, it collides with a digital life where Indian teens routinely self-consent inside apps, manage permissions, and calibrate visibility without a parent sitting beside them. The result is not just non-compliance, it is a predictable split between law and reality.

Global children's rights standards already offer a better lens. UNCRC Article 5 frames parental direction and guidance as something that should enable children to gradually exercise their rights in line with evolving capacities, not freeze autonomy until a fixed birthday.[2][3] General Comment No. 25 extends that logic explicitly to the digital environment, urging states to design governance that balances protection, participation and privacy, and to address the role of digital services in shaping children's rights in practice.[4] This paper reads the DPDPA's child-consent approach against that standard, and then asks a practical question: what would an age-appropriate, shared-consent model look like in India, especially for teenagers?

Children's privacy is not a niche technical issue. It is a question of how a society treats young people as citizens in the making. Data practices decide what children can see, who can reach them, what gets recommended, what becomes searchable, and what follows them as a digital trail into adulthood. A child's mistakes, curiosity, and experimentation deserve room to fade. When platforms default to retention, sharing, and profiling, they shrink that room.

In India, this question is amplified by the speed of smartphone adoption and the centrality of a few platform ecosystems in social life. For many teenagers, the phone is not an optional gadget. It is where homework groups run, where friendships are maintained, where identity is performed, and where entertainment is negotiated. So when policy talks about "consent", it is not talking about a niche checkbox. It is talking about the rules of teenage participation.

Consent in the digital world also differs from consent in offline transactions. Offline, a teenager can often walk away from a shop or a conversation. Online, withdrawal is harder. An account history persists, screenshots circulate, and recommendations keep surfacing the same content. That is why global child-rights guidance increasingly treats privacy as part of a wider package: safety, dignity, participation, and best interests.

The DPDPA's under-eighteen category tries to keep things simple, but simplicity is not neutrality. A single threshold at eighteen treats early childhood and late adolescence as the same compliance problem. It also assumes families have the time, access, and knowledge to function as privacy administrators for every app, every update, and every new feature. In many households, even engaged parents struggle with rapidly changing settings and confusing permission language.

At the level of platform design, the difference between “low-risk” and “high-risk” is not abstract. Low-risk decisions look like choosing a profile picture or turning on notifications. High-risk decisions look like making an account public, allowing unknown people to message, sharing live location, syncing contacts, enabling personalised ads, or turning on in-app spending features. Teenagers can often manage the first category with light guidance. The second category is where shared decision-making and stronger defaults matter.

A consent regime that treats everything as high-risk ends up being ignored, because it asks for too much approval for too many routine actions. A consent regime that treats everything as low-risk creates avoidable harm. The practical answer sits in the middle: match safeguards to the risk and match autonomy to the child’s evolving capacity.

This is the logic behind the project’s focus on a shared-consent approach. It does not romanticise teen autonomy, and it does not demonise parents. It treats both as real actors in a real ecosystem, and it treats platforms as responsible designers rather than neutral pipes. The goal is to reduce the incentives for age-faking, increase the meaningfulness of choices, and keep the strongest safeguards for the moments that actually matter.

Finally, this project uses empirical data not as decoration, but as a reality check. What teenagers say about consent, defaults, and parental involvement matters because it shows where policy assumptions collide with lived experience. If policy is built without that reality check, it becomes a compliance script that no one follows.

Under the DPDPA, a “child” is any person under eighteen.[1] For a child, the law folds the parent or lawful guardian into the definition of “Data Principal” for decision-making, effectively treating parental consent as the legal key for processing children’s personal data.[1] In the same breath, the Act also prohibits certain processing practices for children (for example, forms of tracking, behavioural monitoring or targeted advertising), subject to future rulemaking and exemptions.[1] What the Act does not do is recognise adolescence as a distinct stage in which a child’s capacity for meaningful choice grows rapidly, and where autonomy is not a luxury but part of the child’s rights.

The problem is not that parents have no role. UNCRC Article 5 assigns parents a crucial role, but it describes that role as enabling: guidance should evolve with the child, steadily shifting from control to advice and then to near-equal exchange as maturity grows.[2][3] This is the logic of evolving capacities, and it is not a sentimental add-on. It is a legal principle that prevents arbitrary family control and treats children as rights-holders in their own right.[3] General Comment No. 25 brings that same principle into digital policy, pressing states to ensure that children’s rights to protection, privacy, participation and access to information are supported through laws and through the design of digital services.[4]

PIIR Foundation's earlier research on sharenting makes one thing obvious: the law's faith in "parental consent" often runs ahead of parents' actual ability to protect children's privacy. In its digital parenting study of 150+ Indian parents, the most common sharing happened on WhatsApp (36%), a space that feels private and "family-only" but still normalises oversharing of names, birthdays, school uniforms, and locations. Over 58% of parents reported posting milestone moments, and even where risk awareness existed, protective action lagged: only 42.7% consistently used privacy settings while 28.1% never used them at all. The consent gap is sharper: 71.9% agreed children should have a say in their digital presence, yet only 38.5% actually asked before posting. The takeaway for this study is direct: if regulation assumes parents are equipped gatekeepers by default, it will keep failing children in the places that matter, inside everyday app settings, defaults, and routine family sharing.[13]

When a law makes parents the sole gatekeepers for all under-eighteens, it breaks the bridge that evolving capacities tries to build. It forces a hard cliff at eighteen, while the lived reality is a slope. That cliff has consequences. It creates legal incentives for teens to misstate age and route around consent gates, because the only legal pathway offered to them is 'parental permission', even for everyday low-risk use. A child-rights approach does the opposite: it narrows adult intervention to the moments when risk is real, and it expands child agency where the choice is routine and understandable.

The findings become sharper when you stop treating consent as a form and start treating it as interface. Platforms are not neutral pipes. They stage decisions, they pre-select defaults, and they make some paths smoother than others. This is why global child-rights standards keep returning to design and best interests, not only to consent signatures.[4][6][11]

Risky features are rarely labelled as risky. Open DMs can expose children to unwanted contact. Location-sharing can expose patterns of movement. Public-by-default profiles expand visibility far beyond a child's intent. Microtransaction prompts turn spending into habit. These are not rare edge cases. They are mainstream product choices. If the law wants meaningful consent, it cannot ignore how these choices are packaged and pushed.

The DPDPA's model assumes parents can intervene upstream, but the product reality is that decisions occur in the child's hand, in the moment. That creates two failures: it deprives teens of a lawful, age-appropriate way to consent for routine use, and it lets platforms avoid building child-respecting defaults by outsourcing responsibility to families.[1][6][8] A rights-respecting approach flips this: it makes platforms carry the burden of safer defaults and clearer choice architecture, while it reserves parental involvement for the highest-risk processing or where the child requests support.[3][4][6]

DPDPA does not need to abandon parents to recognise adolescent autonomy. It needs calibrated lanes. A tiered model can be implemented through rules and guidance that: (i) define age bands for consent capacity, (ii) define processing-risk tiers relevant to child safety, and (iii) impose age-appropriate design obligations on platforms that are likely to be accessed by children, similar in spirit to the UK Children's Code.[6][7]

The best interests principle should be explicit in how children's provisions are interpreted and enforced, borrowing from child-rights guidance and the practical toolkits developed by regulators.[4][8][11] This also pulls India closer to the global shift away from 'notice and consent' as the only privacy solution, and toward design and accountability.

# Chapter 2: Literature Review, Legal Context, and Best Practices on Child Data

This chapter reviews the main global standards and regulatory approaches that inform a child-rights respecting approach to personal data processing. It focuses on standards that explicitly recognise children's evolving autonomy, and on frameworks that shift attention from paper consent to privacy-by-design, safer defaults, and limits on profiling.

Global privacy frameworks that take children seriously have moved beyond a simple 'parent or no parent' model. They do two things at once: they tune consent to age, and they make platforms responsible for safer defaults.

The European Union's GDPR is often treated as the classic consent benchmark: for information society services offered directly to a child, consent is valid if the child is at least 16, and member states can lower that threshold as far as 13.[5] Crucially, GDPR does not claim that every under-18 decision must be parental. It defines a narrower band and still requires controllers to make reasonable efforts to verify parental authorisation below the relevant threshold.[5]

The UK's Age Appropriate Design Code pushes even further by shifting attention away from "consent forms" and towards product design. The code applies to online services likely to be accessed by children under 18 and sets design standards that operationalise the 'best interests of the child' through defaults: high privacy by default, data minimisation, limits on profiling, and careful handling of geolocation and nudges.[6][7] The point is blunt: if children are likely to be there, the service has to be built like children are there.

Ireland's Data Protection Commission has distilled a similar approach in its 'Fundamentals' guidance, emphasising a floor of protection and child-oriented interpretation of data protection principles.[8] And the OECD's Recommendation on Children in the Digital Environment frames children's safety and empowerment as a shared responsibility spanning states, industry and society, rather than something solved by pushing consent upward to parents.[9][10] UNICEF's best-interests work (2025) drives the same stake into the ground: policy should actively embed the best-interests principle into digital governance, including business practices and meaningful participation of children in decisions that affect them.[11]

Put together, these standards sketch a clear direction: children's privacy cannot be treated only as parental permission. It is also about age-appropriate explanations, safer-by-default systems, limits on profiling, meaningful choice architecture, and mechanisms that let children steadily exercise rights as capacity grows.[2][4][6][8][11]

Across these standards, the direction is consistent: children's data protection is not a one-time consent event. It is an ecosystem of design choices, governance duties, and age-calibrated support that expands autonomy as capacity grows.

# Chapter 3: Research Objectives and Methodology

## 3.1 Research Problem

The study examines how India's DPDPA child-consent model, which assigns consent authority to parents or lawful guardians for all under-eighteens, aligns or conflicts with children's evolving autonomy online, and how teenagers in a high-access urban context actually interpret and navigate consent, permissions, and default settings in everyday app use.

## 3.2 Research Objectives

- To compare the DPDPA's child-consent approach with global child-rights standards and data protection frameworks that recognise evolving capacities.
- To document how teenagers interpret "consent" and respond to common permission requests and default settings in real-world app use.
- To assess whether a strict parental-consent model encourages age-gate bypass and reduces meaningful engagement with privacy controls.
- To propose a tiered shared-consent model for India that differentiates by age band and by processing-risk tier, balancing autonomy and protection.

## 3.3 Research Design

The study uses a descriptive cross-sectional design, combining doctrinal policy analysis (of DPDPA and global standards) with primary field evidence from structured, in-person interviews.

## 3.4 Type of Data Used

Two types of data are used: (1) primary data from interviews with school students in Jaipur, and (2) secondary sources including statutory text, regulator guidance, and international child-rights instruments cited in the reference list.

## 3.5 Data Collection Method

The empirical section draws on a survey conducted through personal interviews with approximately 200 students in Jaipur, Rajasthan, over a period of three months. Respondents were drawn from different schools across Jaipur, predominantly English-medium schools. The sampling choice was deliberate: these students generally have greater access to smartphones, higher exposure to social media features, and therefore face a more intense set of everyday consent decisions. The goal was not to measure "digital literacy gaps" as a deficit. It was to observe how teens with access to phones (shared or personal) actually move through consent screens, permissions, defaults, and risky feature prompts.

The instrument covered: device use, who set up accounts, time spent online, weekly apps used, interpretations of "consent", reactions to permission requests, who should decide permissions, experiences of changing defaults (visibility, DMs, location, ads, spending prompts), and the perceived role of parents in decisions. Figures in this paper are produced directly from the interview dataset supplied with this study.

## 3.6 Sample and Sampling Technique

Sample size: n = 200 school students in Jaipur, Rajasthan.

Sampling approach: purposive, school-based sampling focused on students with greater likelihood of smartphone access and frequent app use (predominantly English-medium schools), to capture repeated everyday consent encounters.

## 3.7 Data Analysis Tools and Approach

Responses were coded into categorical variables (e.g., age band, account setup, time online, consent interpretation categories). Descriptive analysis was used to summarise distributions, and the results are presented through figures with narrative interpretation.

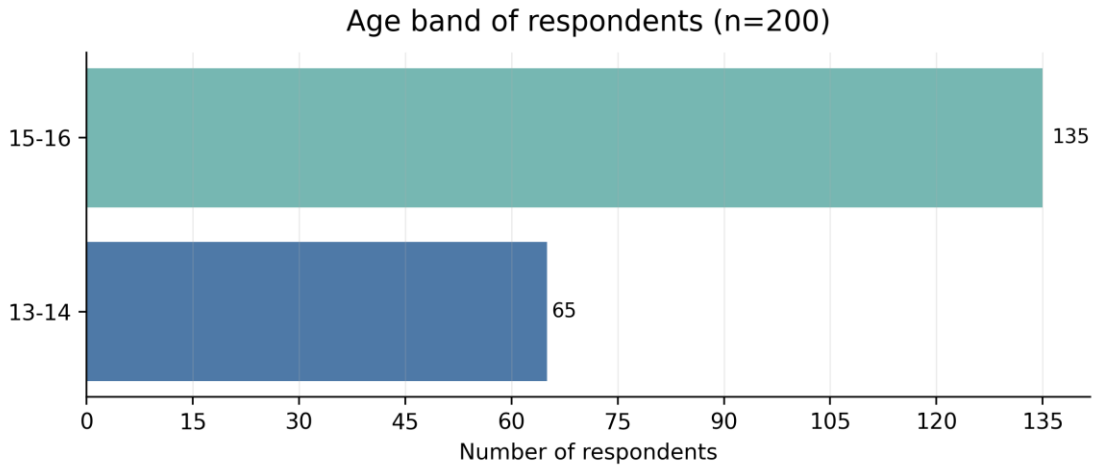
## 3.8 Ethical Considerations

The study reports findings at an aggregate level and does not include personally identifying information. The focus is on patterns of interpretation and experience rather than on individual cases.

# Chapter 4: Data Analysis and Results

This chapter presents descriptive findings from 200 in-person interviews with school-going adolescents in Jaipur, focused on real, day-to-day consent moments on smartphones: account set-up, time spent online, how permission prompts are handled, how "consent" is understood, and when (if at all) parents enter the decision. The figures are arranged to move from respondent profile and exposure (age and time online), to control over accounts and settings (who set up the device), to consent behaviour in the most common high-friction points (permissions and age-gating), and finally to the teenager's own view of who should decide and when parental support becomes relevant. Together, these results set up the central argument of the paper: Indian children, especially adolescents, already act as the primary decision-makers online, so a child-rights aligned consent design must recognise autonomy while adding smarter safeguards where risk is high.

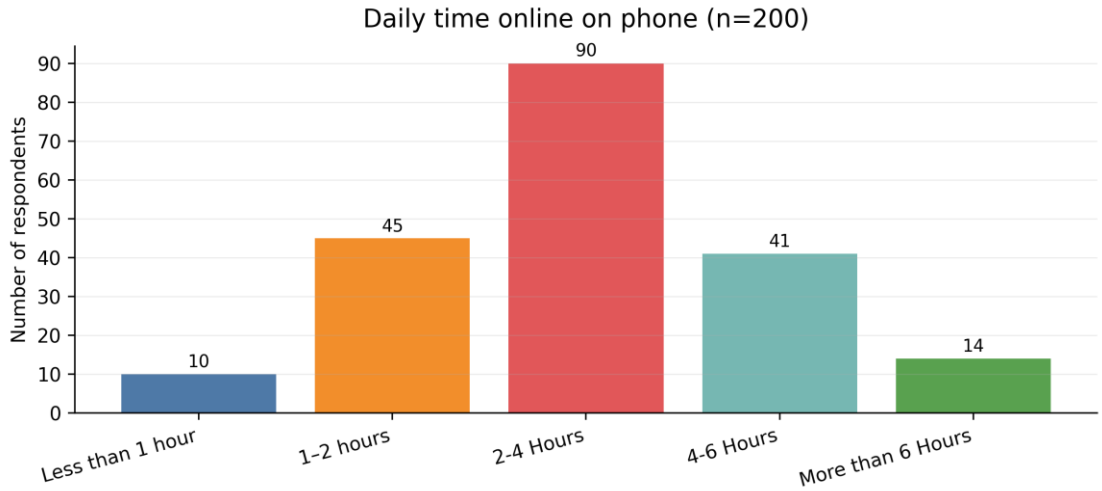
**Figure 1. Age band of respondents (n=200).**




The sample is dominated by mid-adolescents, with 135 respondents (67.5%) in the 15–16 band and 65 respondents (32.5%) in the 13–14 band. This matters because the consent debate in India

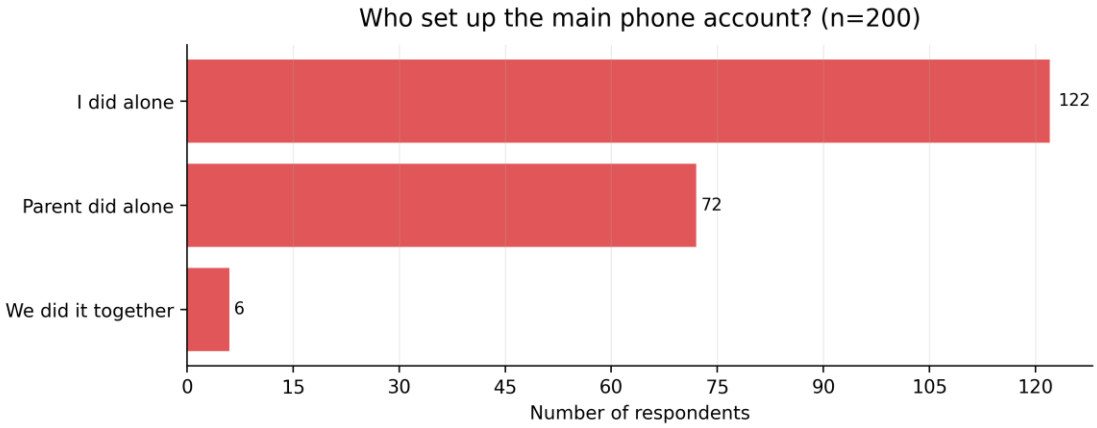
often treats “child” as a single bucket up to 18, while the lived reality of agency, comprehension, and digital behaviour changes sharply across early and mid adolescence. With two-thirds of respondents in 15–16, the dataset strongly represents the age where teens already manage apps, accounts, and privacy decisions without adult involvement, even when law and policy still assume parent-led control.

**Figure 2. Daily time online on phone (n=200).**



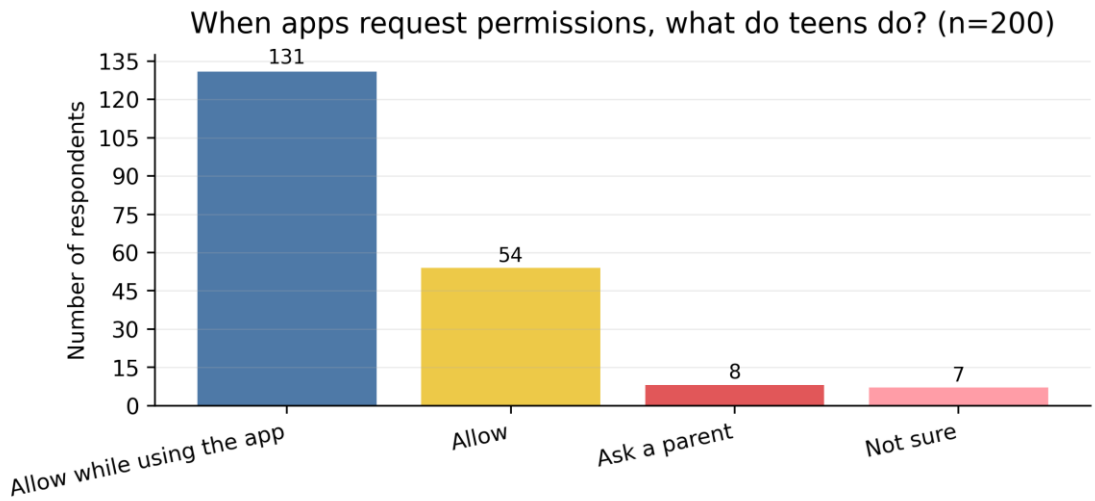

Daily exposure is high. The largest group, 90 respondents (45%), spend 2–4 hours online per day, while 55 respondents (27.5%) spend 4+ hours (41 in the 4–6 hour bracket, and 14 over 6 hours). Only 10 respondents (5%) reported less than one hour. This is not “occasional internet use”; it is a core daily environment. When screen time sits at multiple hours a day, consent cannot be treated as a rare legal checkbox. It becomes an ongoing stream of micro-decisions shaped by defaults, nudges, and friction.

**Figure 3. Who set up the main phone account? (n=200).**



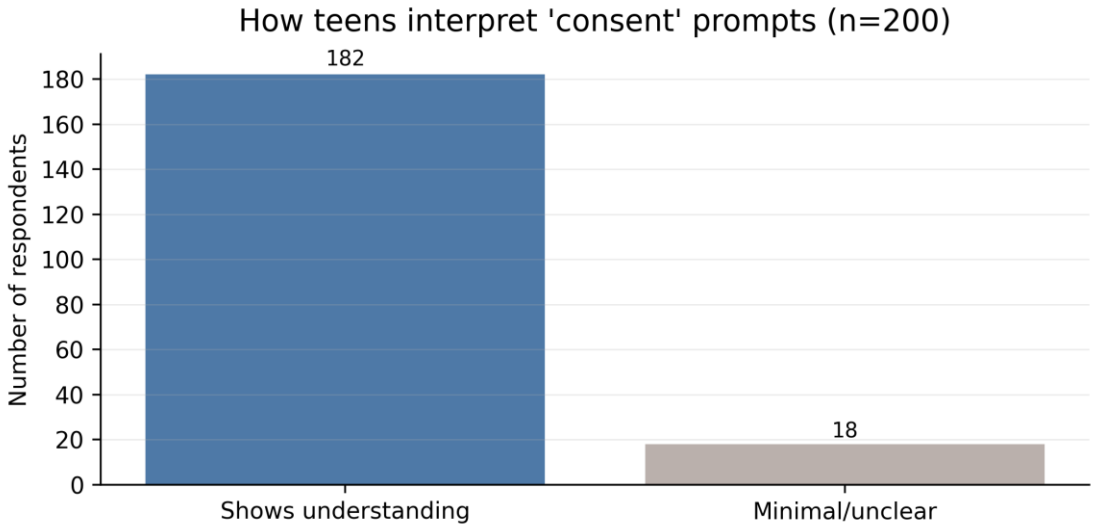

A clear majority, 122 respondents (61%), set up the main phone account on their own. Another 72 (36%) said a parent set it up alone, and only 6 (3%) reported setting it up together. Account set-up is the first moment where privacy defaults and data permissions get locked in, and here, teens are overwhelmingly the ones doing it. This directly undercuts the policy fantasy that parental consent naturally sits at the start of the digital journey. In practice, the "first consent" is often a teen-led set-up followed by inherited defaults.

**Figure 4. When apps request permissions, what do teens do? (n=200).**



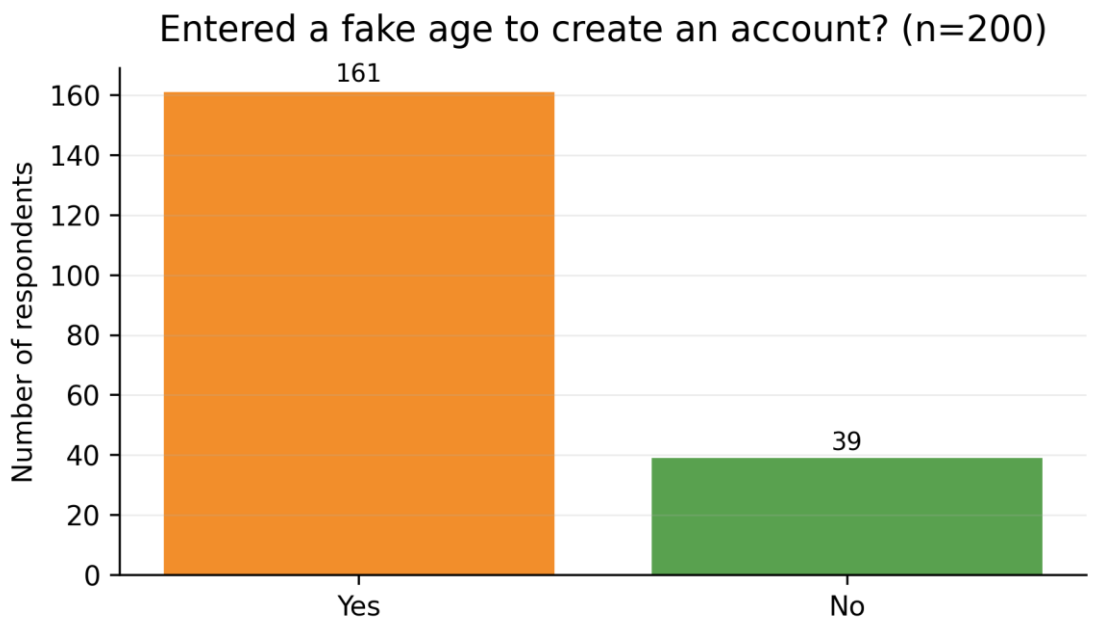

The dominant behaviour is fast acceptance. 131 respondents (65.5%) said they "allow while using the app," and 54 (27%) simply "allow," meaning 92.5% grant permissions in the moment. Only 8 respondents (4%) said they ask a parent, and 7 (3.5%) were not sure. This is the most revealing behavioural result in the dataset: permission prompts are treated as speed bumps, not decisions. The design of consent here is failing on its own terms, because it is training users to click through to get on with life.

**Figure 5. How teens interpret 'consent' prompts (n=200).**



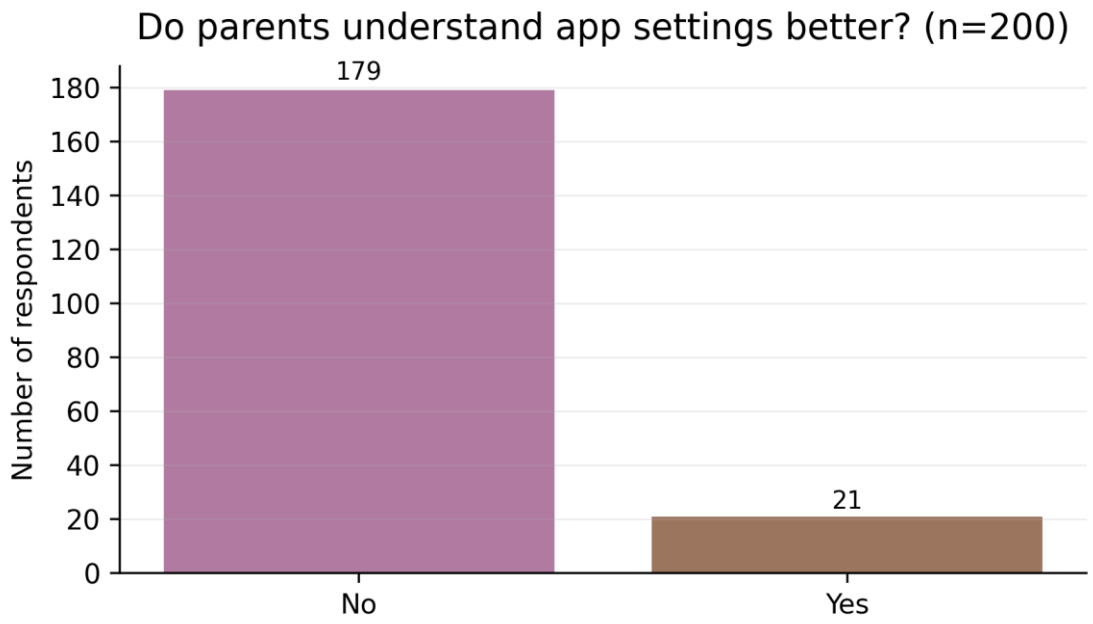

Importantly, understanding is not the main problem. 182 respondents (91%) showed a clear, meaningful interpretation of what consent means, while only 18 (9%) were minimal or unclear. This flips a common assumption in Indian discourse that children do not “get” consent. They do. The issue is not comprehension, it is context: prompts arrive at the wrong time, with weak choices, and with an incentive structure that rewards quick acceptance. It means we are not dealing with a blank slate where children have no concept of consent. We are dealing with an environment that treats their understanding as irrelevant because the flow is not built to respect it. In other words, the design problem is bigger than the comprehension problem.

**Figure 6. Entered a fake age to create an account? (n=200).**



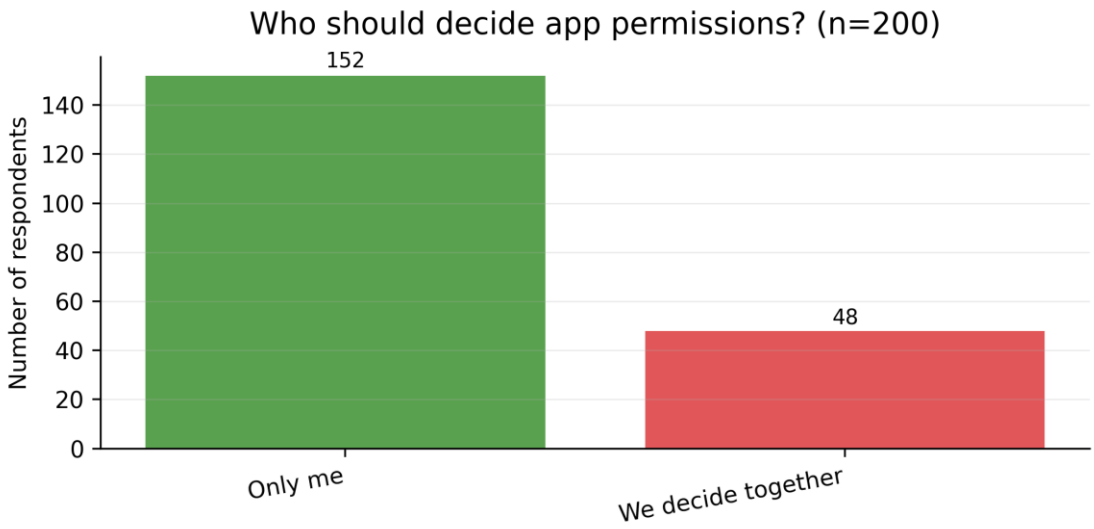

A significant share of respondents report entering a fake age at least once to create an account. This is the predictable downstream effect of a legal and platform architecture that offers teens a binary choice: either declare childhood and trigger parental involvement, or declare adulthood and proceed. The DPDPA's under-18 gatekeeper model strengthens the incentive to take the second path, because it does not offer a legitimate adolescent lane.

**Figure 7. Do parents understand app settings better? (n=200).**



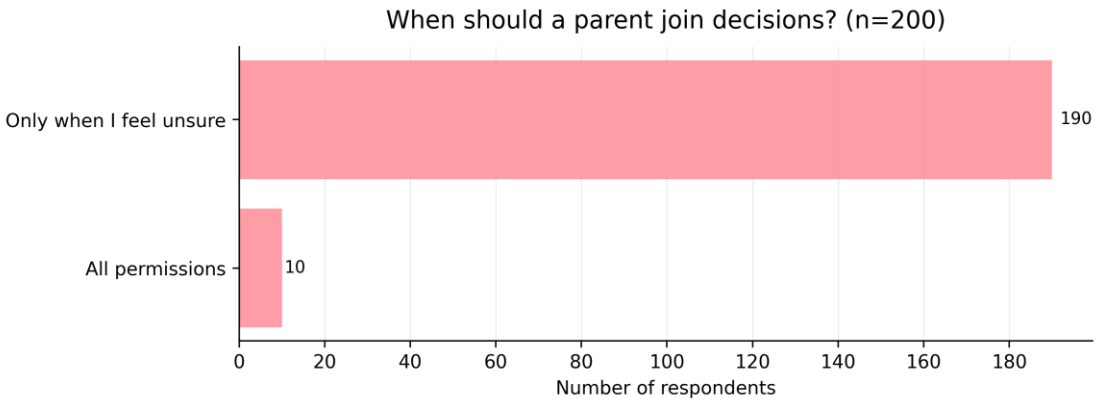

The dataset also complicates the assumption that parents can function as reliable privacy administrators. Many teens do not perceive their parents as more capable in changing settings or fixing app issues. This paper does not treat that as a moral failure or a literacy deficit; it treats it as a design reality. If settings are hard for adults, they are hard because platforms are not incentivised to make privacy controls simple, legible, and stable. Relying on parental gatekeeping as the primary solution therefore hands the hardest part of privacy to the least supported actor.

**Figure 8. Who should decide app permissions? (n=200).**




When asked who should decide permissions ‘today’, many teens lean toward a shared approach. They want autonomy in routine choices, and they want parents involved when the decision carries risk or when something feels confusing. That preference is aligned with the evolving capacities principle: guidance as scaffolding, not surveillance. This is not a rejection of parents; it is a clear demand for agency. It also aligns with the idea that consent must map to the actual decision-maker. When teens are the ones tapping “Allow,” the law’s design job is to make that tap safer and more meaningful, not to pretend it is happening elsewhere.

**Figure 9. When should a parent join decisions? (n=200).**




The ‘when should parents join’ responses are particularly useful because they point to timing. Teens do not want parents hovering over every tap. They want parents available at decision-points that matter: account creation, risky feature activation, unexpected prompts, or moments of harm. This is exactly the kind of procedural question the DPDPA currently sidesteps by collapsing all minors into one legal posture. This is the cleanest expression of a workable middle path: teens want autonomy for routine choices, and adult support as a safety net for high-risk or confusing situations. That logic is exactly what a tiered shared-consent model formalises.

# Chapter 5: Findings and Conclusion

The interviews make one point impossible to dodge: teenagers do understand what "consent" is, but the way apps ask for consent rarely treats them as real decision-makers. Consent shows up as a set of fast prompts and default settings, not as an informed choice. That gap matters because policy often assumes that a parent can step in and manage consent on a child's behalf, while the actual decision moments happen on the teen's screen, in seconds, under social pressure.

**Key finding 1**: Teenagers overwhelmingly define consent as permission or agreement, and they recognise the idea of having a choice.

**Key finding 2**: Permission prompts (camera, microphone, contacts, location, photos) are treated as functional hurdles, not as meaningful privacy moments, because the interface rewards quick acceptance.

**Key finding 3**: A strict under-eighteen parental gatekeeping model encourages predictable workarounds, including age misrepresentation, rather than safer, more honest pathways.

**Key finding 4**: Many teens prefer shared decision-making: autonomy for routine, low-risk choices, and parental involvement when the decision is risky, confusing, or has long-term consequences.

Taken together, these findings point to a policy-design mismatch. If the law treats every under-eighteen as incapable of routine privacy decisions, it undermines teen agency and it reduces compliance. If platforms are not required to ship safer defaults and clearer choice architecture, then parental consent becomes a symbolic shield while risk remains embedded in product design.

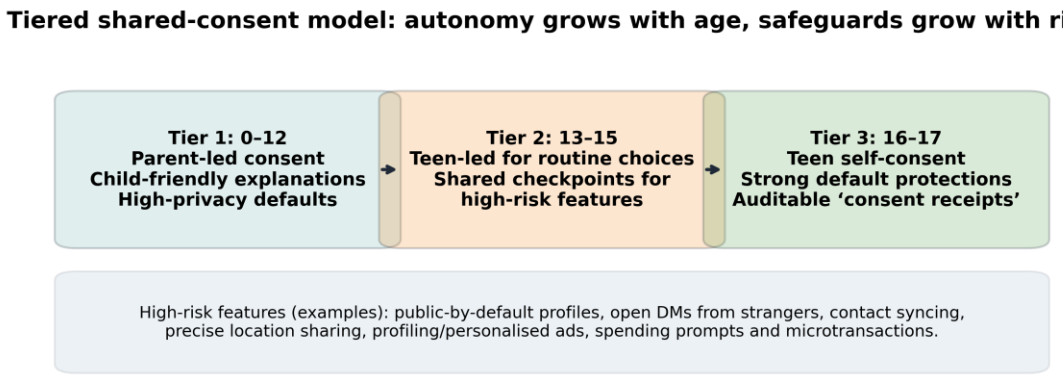
The project's conclusion is therefore practical and normative. Practically, children's data protection in India will work better when autonomy and safeguards are calibrated by age and by

risk. Normatively, this approach fits a rights-respecting view of children as developing rights-holders: parents guide, children grow into decision-making, and platforms are required to design for the child's best interests rather than for maximum disclosure.

## 5.1 Proposed Tiered Shared-Consent Model

India needs a consent model that fits how adolescence works: not a switch at eighteen, but a gradual transfer of choice, paired with stronger guardrails where the stakes are high. The model proposed here uses two axes: age band (as a proxy for evolving capacity) and processing-risk tier (as a proxy for harm potential). The objective is simple: expand teen autonomy for routine, low-risk processing while hardening defaults and creating shared checkpoints for features that can realistically expose teens to harm.

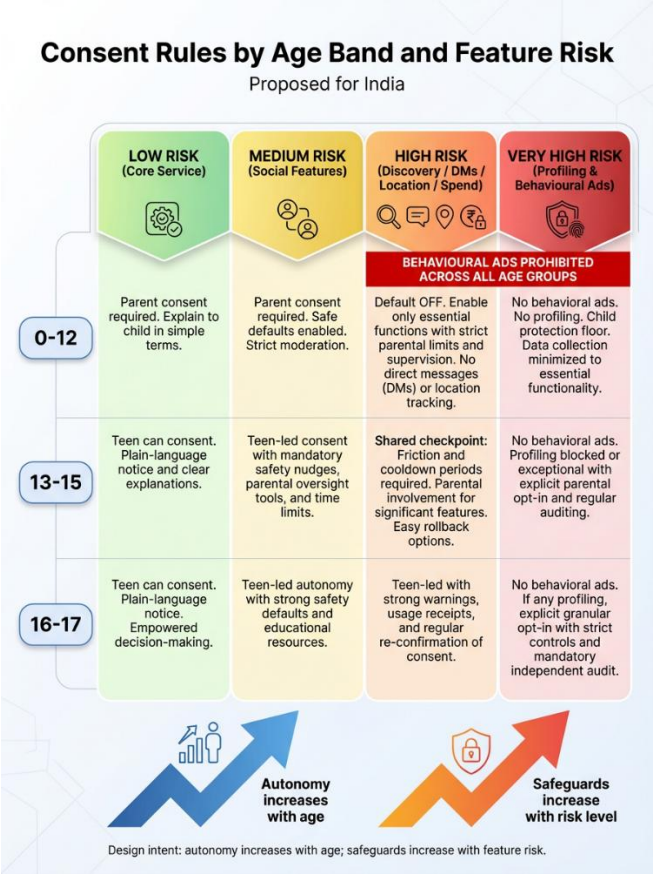
**Figure 10. Model overview: three age tiers and the logic of shared checkpoints.**




This model converts the behavioural findings into a policy structure: autonomy increases with age, and safeguards increase with risk. Tier 1 (0–12) stays parent-led with child-friendly explanations and strong privacy defaults. Tier 2 (13–15) is teen-led for routine decisions, but introduces shared checkpoints for high-risk features that deserve slower, clearer choices. Tier 3

(16–17) recognises teen self-consent with strong defaults and auditable "consent receipts," so the system keeps a traceable record of what was agreed to, when, and why.

**Figure 11. Consent rules by age and feature risk (proposed).**




Tier 1 (0–12) stays close to parental authorisation, but with a non-negotiable design obligation: child-friendly explanations and high-privacy defaults. Tier 2 (13–15) is the adolescent lane: teens can self-consent for routine processing and core service use, while high-risk features trigger shared checkpoints. Tier 3 (16–17) recognises late adolescence as a near-adult zone: teens can self-consent broadly, but platforms must still apply strong protective defaults and keep auditable consent receipts. Across tiers, behavioural advertising and profiling should be blocked for

children as a baseline, consistent with the direction of child-rights and child-design standards.[4][6][8]

In practice, a shared checkpoint is not a parental veto built into every screen. It is a moment of friction where the platform pauses the flow: the teen sees clear consequences, gets a cooldown window, and can either proceed, roll back, or invite a parent into that specific choice. This is not about infantilising teens. It is about acknowledging that the highest-risk features are engineered to be sticky, and that protecting autonomy sometimes requires slowing a decision down.

# Chapter 6: Recommendations and Limitations

## 6.1 Recommendations

1. Introduce an age-banded framework under DPDPA child rules that distinguishes early childhood from adolescence, with a clear pathway for increasing teen autonomy.
2. Adopt a risk-tier model for processing: routine low-risk processing should not trigger heavy parental verification; high-risk processing should require stronger safeguards.
3. Make privacy-by-default mandatory for services likely to be accessed by children, including default private accounts, restricted discoverability, and closed DMs from unknown users.
4. Require separate, explicit "high-risk feature" checkpoints for open DMs, public profiles, location-sharing, contact syncing, and in-app spending prompts.
5. Mandate plain-language, consequence-first explanations at the moment of decision (what changes, who can reach you, what becomes visible, how to undo it).
6. Ban or strictly limit behavioural advertising and profiling for children, including inference-based targeting and engagement-optimised recommendations tied to sensitive attributes.
7. Reduce incentives for age-faking by allowing supervised teen self-consent for routine features, combined with platform duties to detect and mitigate risky settings.
8. Standardise child-friendly permission prompts with meaningful alternatives (e.g., "Allow once", "Allow while using", "Not now") and simple revocation paths.
9. Require accessible "child mode" and "teen mode" dashboards that surface the most important controls without burying them in settings.

10. Add an obligation for periodic "settings checkups" for child and teen accounts (short, timed prompts that review key safety settings).
11. Create a duty to log and explain meaningful changes to defaults affecting child accounts (no silent shifts from private to public or from restricted to open contact).
12. Encourage co-use and shared decision-making through feature-level invitations for parents, instead of blanket parent control for the entire account.
13. Invest in public guidance that speaks to families and schools using concrete scenarios (DM risks, location-sharing, spending prompts), not abstract legal vocabulary.
14. Prioritise enforcement on design practices that increase exposure and harm (dark patterns, confusing opt-outs, manipulative nudges), not just on paperwork compliance.
15. Support independent audits of child-facing design and recommender systems for major platforms used by children in India.

## 6.2 Limitations and Future Research

- The sample is focused on an urban context (Jaipur) and may not represent rural or low-access environments.
- Respondents were predominantly from English-medium schools, which may correlate with different platform use patterns and parental digital familiarity.
- The study relies on self-reported behaviour (e.g., age misrepresentation), which can be affected by recall or social desirability.
- The dataset captures a cross-section in time and does not track changes as children grow older or as platforms update features.

- The research does not separately measure digital literacy or school-based internet education, which would require a distinct study design.
- Platform-specific differences (across apps) are not fully disentangled; future work could compare consent and defaults app-by-app.
- The study focuses on teenagers aged roughly 13–16; further research is needed for younger children and for late adolescents closer to eighteen.

This study is focused on a specific urban context: Jaipur students aged 13–16, largely from English-medium schools with higher access to smartphones. The results are not a statewide prevalence estimate and should not be used as one. Future work should expand into Hindi-medium and rural contexts, compare shared-device versus personal-device dynamics more granularly, and study how age assurance or ‘floor of protection’ approaches would affect real use patterns.

# Appendix

## Appendix A: Interview Instrument (Summary)

- Age band; class/grade; gender
- Devices used at least weekly; whether phone is personal or shared
- Who set up the main phone account
- Daily time online on phone
- Apps or sites used weekly in last 30 days; top two apps
- Understanding of "consent" when an app asks
- Reactions to common permission requests (camera, microphone, contacts, location, notifications, photos/gallery)
- Views on who should decide permissions today, and why
- Defaults encountered on first use (account visibility, direct messages, location sharing, ads/sponsored content, in-app spending prompts)
- Whether any defaults were changed later
- Whether a fake age was entered to create an account
- Perception of whether parents understand app settings better
- When and how parents should join decisions (shared-consent triggers)