

A Primus POV | October 2026

Regulating a Child's Social Network

Weighing a ban against the
alternatives for India







In brief

India is debating whether, and how, to restrict children's use of social media, as several countries move to act. Within eighteen months, keeping children off social media has moved from one country's action to a global movement. Australia's ban on accounts for under-sixteens is now in force, the United Kingdom has announced its own, and the European Commission has proposed EU-wide rules that would keep under-13s off social media and give 13- and 14-year-olds only limited accounts managed by a parent. India is watching closely, and its Economic Survey 2025-26 has already flagged digital addiction among the young, while courts and some states have urged firm age limits. In September 2026, the Centre told the Supreme Court that it would amend the IT Rules to stop platforms from letting under-18s open social media accounts. This note takes the view that the goal is right but the instrument matters. For a country as large and as digitally staggered as India, a promising path is to focus on how platforms are designed, and to enforce the strong child-protection rules India has only just finished building.

Table of contents

01

The Fundamental Question
Before Us 07

02

A Global Wave, Moving Fast 08

03

What A Ban Or Restriction
Actually Does, And Does
Not Do, In Practice 12

04

The Evidence Is Real, But
It Is Contested 15

05

The Real Lever Is
Design, Not Access 18

06

Why India Is Different:
Scale And Inequality 20

07

India Already Has The
Architecture (Of Protection) 22

08

The Primus View: A Design-
First, Inclusion-Aware Path 24

09

Conclusion 28

List of Abbreviations

AI	Artificial Intelligence
DPB	Data Protection Board of India
DPDP Act	Digital Personal Data Protection Act, 2023 (India)
DSA	Digital Services Act (European Union)
EU	European Union
I4C	Indian Cyber Crime Coordination Centre
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India)
KIDS Act	Keeping Internet Digital Spaces Accountable and Trustworthy Act (EU)
MeitY	Ministry of Electronics and Information Technology (India)
NASSCOM	National Association of Software and Service Companies
NCMEC	National Center for Missing & Exploited Children (United States)
NCPCR	National Commission for Protection of Child Rights (India)
NFHS	National Family Health Survey
NHRC	National Human Rights Commission (India)
NIST	National Institute of Standards and Technology (United States)
POCSO	Protection of Children from Sexual Offences Act, 2012 (India)
US	United States
VPN	Virtual Private Network

The Fundamental Question Before Us

1

The experience of childhood has changed significantly. Alongside families, schools and communities, social media platforms and recommendation algorithms now play a central role in shaping how children spend their time, access information and interact with the world, a shift that has accelerated since the pandemic.

Social media has also brought commendable advantages. It helps bridge geographic and socioeconomic disparities by ensuring that all children can access the same content, irrespective of location or household income. It has democratised access to information, enabling everything from free learning resources to professional networks. It has also created unprecedented opportunities for learning, employment and entrepreneurship that were not available to previous generations. For many children, it also provides a sense of community and belonging that may not always be available at school or home, helping them feel connected and less isolated. For young people in India, it is often the primary gateway to engaging with the wider world.

At the same time, the other side of the ledger is equally real and needs equal attention. Mental health concerns, cyberbullying, disrupted sleep and digital addiction are emerging as serious challenges among the young. Children are exposed to harmful content, and to risks such as 'grooming', in ways that earlier generations were not.

Furthermore, in contrast to the arguments of the previous paragraph, the displacement of offline interaction is also accentuating social awkwardness and other developmental concerns.

That shift has produced a genuine and widely shared worry about the wellbeing of the young, and governments are now acting on it.

This brief does not debate the need to protect children online. It examines whether a blanket age-based restriction on access to social media accounts is the right policy instrument to achieve that goal, and provides a rounded perspective of its impact in the Indian context.

A Global Wave, Moving Fast

2

What started as a national decision has turned into one of the most closely watched debates in digital policy. In November 2024, Australia passed its Online Safety Amendment (Social Media Minimum Age) Act, the first national law to prevent under-16s from having accounts on the big platforms. It entered into force on 10 December 2025.¹ The law puts the onus on platforms, not parents or children, and backs it up with penalties of up to 49.5 million Australian dollars (about ₹330 crore) for a systemic failure to take reasonable steps. It does not allow parental override. In June 2026, Australia announced that it would double the maximum penalty, and Parliament passed the change in September. Because the value of a penalty unit rose in July, the new maximum is about AUD 109 million (around ₹735 crore).²

The idea drew much of its public energy from the 2024 book *The Anxious Generation*, which linked the rise in adolescent distress to a phone-based childhood, and from parent-led campaigns. A YouGov survey found that around 77 per cent of Australians backed the measure.³ Since then, the movement has grown quickly. The UK announced on June 15, 2026, that it too will ban under-sixteens from using a range of social media sites, following Australia's lead. The regulations are expected to come into force in spring 2027. The British plan goes further in some respects, including restrictions on livestreaming and contact with strangers, a minimum age of 18 for romantic AI chatbots, and proposals for overnight curfews and breaks from infinite scrolling for older teenagers. Nine out of ten parents supported action, the government said.⁴

The European Union is moving on a parallel track. In November 2025, the European Parliament voted, by 483 to 92, for a harmonised digital age of sixteen (for social media, video-sharing and AI companions), and with thirteen as an absolute floor below which no child should hold an account even with a parent's consent. The resolution was not binding, but it asked the European Commission to act, and it paired age limits with a direct attack on addictive design and with an EU age-verification app built on the European Digital Identity Wallet.⁵

On 17 September 2026, the European Commission put forward a formal proposal, the EU KIDS Act. It would keep children under 13 off social media, apart from child-friendly video services used through a parent's account. From 13 until they turn 15, children could have a "mini account" managed by a parent, with limited features and a limit of one hour a day. From 15, they could open their own account. The proposal also covers video-sharing sites, online games and AI companions. It makes safer design the default: limits on infinite scroll and night-time notifications, no contact from strangers, private profiles for minors, and AI companions turned off by default. Platforms would have to check ages in a way that protects privacy, including through the EU's own age-verification app. The European Parliament and member states must still agree on the final text, which could take time.⁶ Commission President Ursula von der Leyen has argued that parents, not algorithms, should be raising children.⁷

These developments reflect a broader trend of countries adopting increasingly stringent measures to safeguard children in the digital environment. France went further in July 2026, when its Parliament approved a ban on social media for children under 15. In August 2026, however, France's Constitutional Council struck the ban down. It found that the law limited freedom of expression more than necessary, treated all platforms alike whatever their risks, and required age checks without enough privacy safeguards. In September, the government sent a revised bill to the European Commission. It drops the account ban and would instead switch off around ten risky features for under-15s, such as autoplay, night-time notifications and contact from unknown accounts. It still needs EU review and a fresh vote in Parliament.⁸ Additionally, Germany permits the use of social media by 13- to 16-year-olds with parental consent, Italy requires consent under 14, and Belgium has a minimum of 13. Norway now plans an age limit of 16, with a bill due by the end of 2026, and Denmark has agreed to a minimum age of 15 for some platforms.

Malaysia is blocking under-sixteens using identity-based checks (in force since June 2026)⁹ while Brazil, Indonesia and Canada have all introduced or announced restrictions outside Europe. While there isn't a federal ban in the US, several states have taken steps to limit the apps: Florida has banned under-14s, and Virginia passed a law limiting under-16s to one hour a day on each app unless a parent consents. A federal court blocked it in early 2026 on free-speech grounds, and an appeals court refused to revive it in August.¹⁰ In August 2026, New Zealand introduced its own bill to bar under-sixteens from social media. It targets platforms with high-risk features such as endless scrolling, algorithmic recommendations and streak-style rewards, and it would also require platforms to file annual child-safety risk assessments for every user under eighteen. Its passage is not certain, as parties within the governing coalition have said they will vote against it.¹¹ Parliament rose in September before the bill's first reading, so its fate now depends on who forms the government after the 7 November 2026 election.¹²

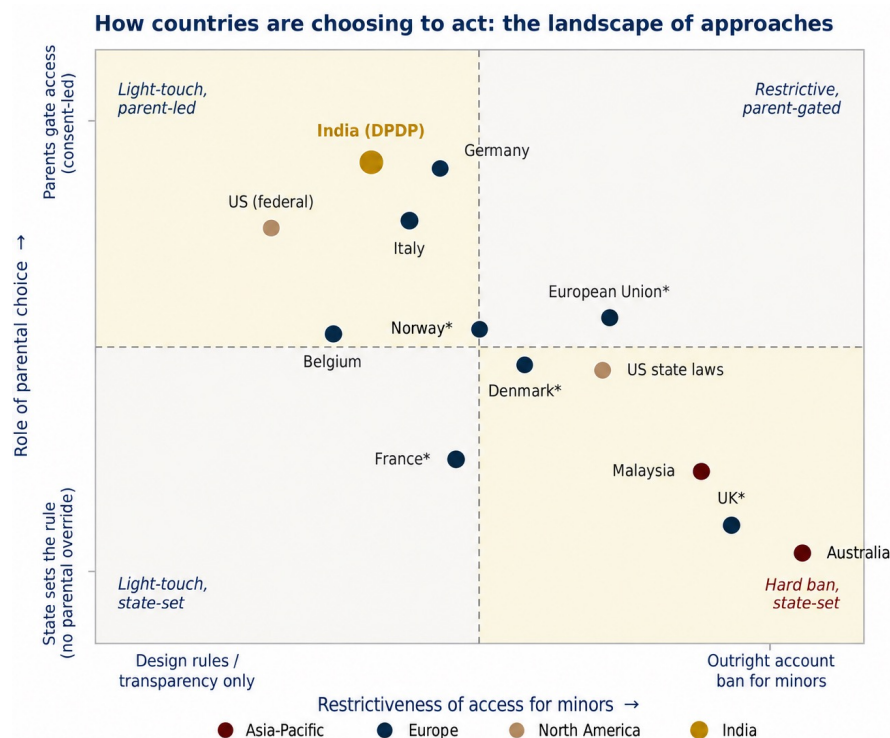


Figure 1. The landscape of approaches. Placement is a Primus qualitative assessment.

	Jurisdiction	Core approach	Key age	Status
	Australia	Ban on accounts for minors; no parental override	Under 16	In force (Dec 2025); penalties doubled (Sep 2026)
	United Kingdom*	Account ban plus limits on certain features	Under 16	Enforcement expected 2027
	European Union*	EU KIDS Act: no social media under 13; limited, parent-managed accounts until 15; safer design by default	Under 13, then 15	Proposed Sep 2026; needs Parliament and Council approval
	France*	Revised bill limits about ten risky features for under-15s; earlier account ban struck down (Aug 2026)	Under 15	Revised bill sent to EU (Sep 2026)
	Germany / Italy / Belgium	Parental consent or floor age	13–16	In force
	Norway / Denmark*	Raising the minimum age	16 (Norway) / 15 (Denmark)	Proposed / agreed
	United States (federal)	Data consent only; no access ban	Under 13	Ban bills pending
	United States (states)	Ban, parental consent or daily time limits (some blocked in court)	14–16	In force in some states; blocked in others
	Malaysia	Account block with ID age checks	Under 16	In force (Jun 2026)
	India (DPDP framework)	Parental consent and design limits; no access ban	Under 18	Effective May 2027
	India (planned IT Rules change)*	Platforms to be potentially barred from letting under-18s open social media accounts; details awaited	Under 18	No draft yet

* Announced or proposed, not yet in force.

Global approaches have converged around two broad models. One, exemplified by Australia and now the UK, sets a firm minimum age and holds platforms accountable for enforcing it. The other, followed across much of Europe, allows children to access platforms with parental consent. A third approach is now emerging: switching off risky features for younger users, as France's revised bill and the EU KIDS Act both propose.

The real design choice is not simply between these models, but in determining the appropriate balance between state oversight and parental discretion. That is the choice India now faces. The case for firm action is serious and is gaining ground: courts, several state governments and child-safety advocates in India have all argued that clear age limits may be necessary to protect children, and the question is which mix of measures will work best.

“

Age gating social media through laws and regulations was bound to see wider adaptation. The balance was inexorably tilting more towards harms than relevance and protective measures undertaken by platforms were falling short. Harmonising such laws across jurisdictions may now be a welcome move.

”



N. S. Nappinai
Senior Advocate,
Supreme Court of India,
and Founder, Cyber Saathi



What A Ban Or Restriction Actually Does, And Does Not Do, In Practice

3

Supporters argue that the only policy that is both powerful enough to change platform behaviour and easy to implement on a large scale is a clear age limit. Thus far, the evidence complicates that assertion.

It is important to be specific about the requirements of the Australian model. The word 'ban' is perhaps a misnomer here. Covered platforms must take reasonable steps to prevent minors under the age of 16 from creating or maintaining accounts. It doesn't stop children from accessing the open internet or seeing content that doesn't require a login; it restricts account-based access, which is what matters in practice. The Rules do not apply to stand-alone messaging services, online games and largely educational or health services, which reflect their place in communication and learning.

Early signs show the constraints of the method. In the weeks that followed the ban, platforms restricted or removed nearly five million accounts. But soon reports came out that many children were still online.¹³

Some used alternative or fake accounts; some moved to smaller or newer apps (which may inadvertently come with their own safety concerns); some moved their conversations into gaming and messaging tools that sit outside the ban; and many just used a VPN. Media reporting of the latest data shows that some 26% of children between the ages of 13 and 15 were on TikTok as of July 2026, just one percentage point below the rate prior to Australia's rules coming into effect.

The rate for children between the ages of 10 and 12 is higher now than before the ban, according to the data.¹⁴ The regulator's own first evaluation, published in July 2026, points the same way. Three months in, the share of under-16s with an account had fallen from 52% to 42%. Even so, about 82% were still using social media in some form, down only slightly from 86%, and most who had accounts before the ban had kept them or opened new ones. There was one positive sign: fewer children said they felt they were missing out (36%, down from 43%).¹⁵





Age verification or estimation tools

Moreover, Age-estimation tools, which infer age from behaviour or a face scan, were found to misjudge age by one to three years, and several major platforms are under investigation for failing to keep younger users out. Australia's Prime Minister compared the law to drinking-age rules: imperfectly observed, yet still worth setting as a clear national standard.¹⁶ How well these checks work varies sharply by age.

A reading of this is that an outright ban is simple to propose, but difficult to implement. On a massive scale, any form of age verification will either require invasive forms of ID checks (with their own inherent privacy problems), or estimation techniques which aren't quite reliable for the age of sixteen. This is the practical backdrop against which India should be evaluating its own options.

A recent assessment reinforces this. In July 2026, the United Kingdom's regulator Ofcom reported that the age-inference methods platforms currently use are unlikely to be reliable enough to support a social media ban for under-sixteens, and that stronger checks would be needed to tell reliably whether a user is over or under that age. Its review also found that adult-content sites had largely adopted robust age checks while most social media platforms had not, several of which are now under investigation. This is a reminder that enforcement, and not legislation alone, decides whether such a measure works.¹⁷ The field is also beginning to standardise, with the first international standard for age-assurance systems, ISO/IEC 27566, published in December 2025.

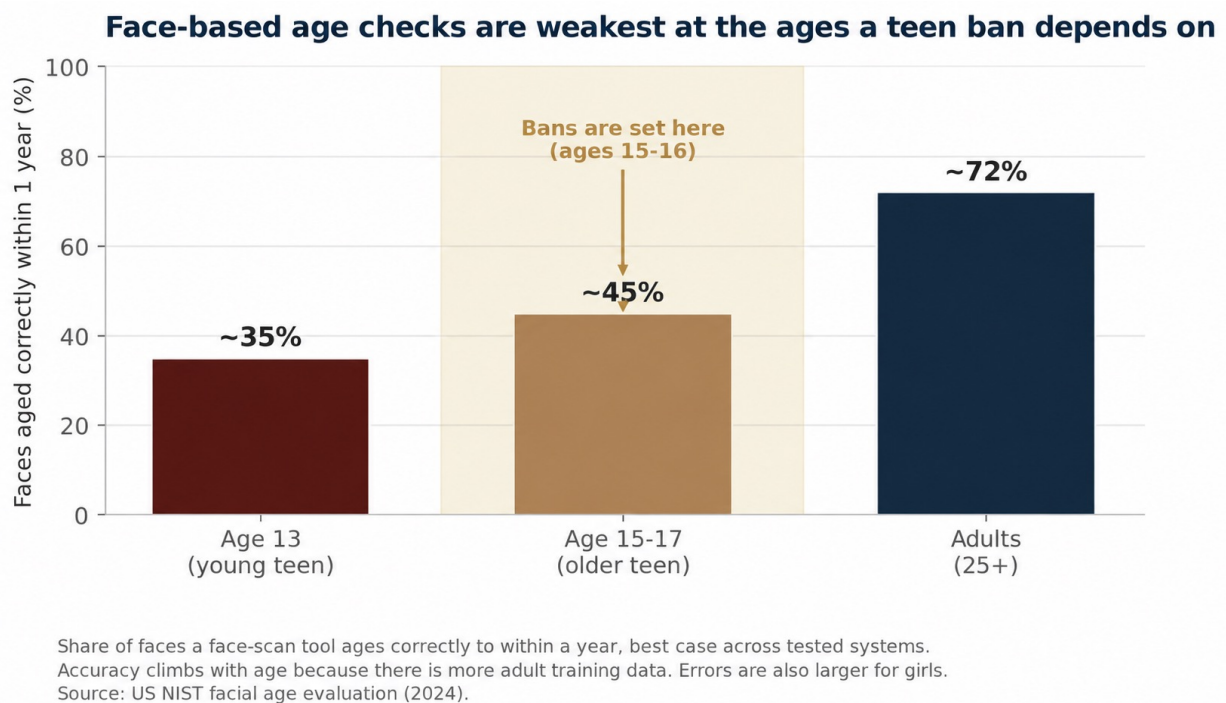


Figure 2. Face-based age-check accuracy by age group. Source: US NIST facial age evaluation (2024)



The Evidence Is Real, But It Is Contested

4

The concern behind these laws is not imaginary or assumed. In several countries, rates of anxiety, depression and self-harm in adolescents have risen over the last decade, and heavy social media use is linked with poorer sleep, lower self-esteem and increased distress. In a 2024 study of Indian teenagers between the ages of thirteen and nineteen, nearly 38 per cent exhibited signs of depression, a third showed anxiety and more than 40 per cent reported high stress, with screen time and social media use among the correlates.¹⁸

What is far less settled is how much of this social media actually causes. The scientific debate here is genuine and unresolved. Jonathan Haidt, an American social psychologist and author, argues that the timing and the international spread of the decline point to a causal role for phones and social media. A substantial group of researchers, including Candice Odgers, Amy Orben, and Andrew Przybylski, reply that most of the evidence is correlational, that the measured effects are small, and that the relationship may even run the other way, with struggling teenagers turning to social media rather than being harmed by it.¹⁹

The evidence is real, but contested: how big is the effect?

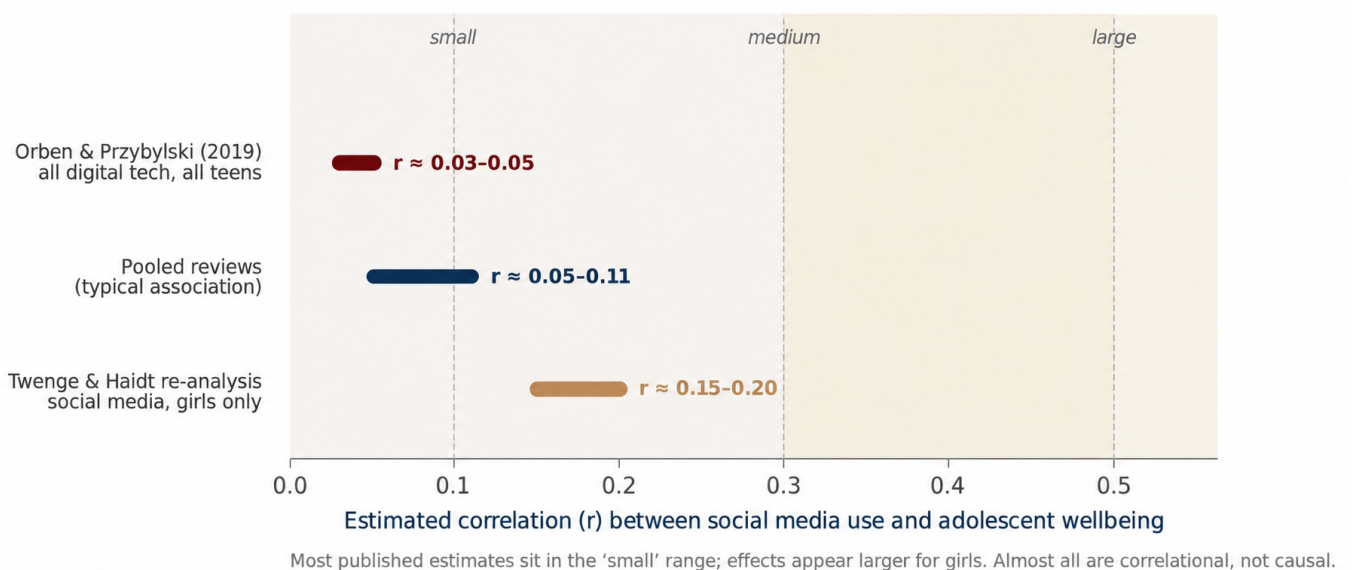


Figure 3. Competing estimates of the social media and wellbeing link. Sources: Orben and Przybylski (2019); Twenge and Haidt; published reviews.

Figure 3 above captures the disagreement. The most-cited large studies found the association (between social media use and adolescent wellbeing) to be **very small in practical terms**. Analysis focused specifically on girls and social media use found a somewhat stronger link, though still modest. None of this means the concern is misplaced. It means the evidence is strong enough to justify acting, while leaving room for reasonable disagreement about which instrument fits best.

Both a strict age limit and a gradual, design-led approach can be justifiable when the evidence is this ambiguous. Selecting a course of action that can be implemented and modified as the data matures vis-à-vis develops, is crucial.

Int ▾

The Guardian

News Opinion Sport Culture Lifestyle

The Guardian view Columnists Cartoons Opinion vid

Opinion

🕒 This article is more than 1 year old

Adolescence's message has echoed around the world - but a social media ban is the wrong move

Katrina vanden Heuvel

The dangers young people face online are all too clear. But the solution is pragmatism, not prohibition

Wed 16 Apr 2025 15:00 BST

🔗 Share





Dr. Nimesh G. Desai
Senior Psychiatrist and
Former Faculty Member at
NIMHANS, Bengaluru

“

A high level of concern, bordering on alarm, for the protection of the young generation is quite legitimate. The danger is that the solutions chosen tend to be driven by idealism and a repressive instinct, rather than being pragmatic and grounded in science. If there is one lesson we have learnt about human behaviour, particularly personal behaviour, it is that a total ban or prohibition does not work and often misfires. This is all the more true for behaviours that are pleasurable or exciting, and more so for those carried out in private, which are very difficult to monitor. Extremist parental responses can be appealing and even politically tempting, but they often make the situation worse. Reasonable positions that trust the innate sense of human beings, including children, may not be sensational, but are likely to yield better results in the long run, especially for mass-based initiatives.

”



The Real Lever Is Design, Not Access

5

There is one part of the picture on which there is far more agreement: the way these products are built. Several platforms are engineered to hold attention through infinite scrolling, autoplay, notification cascades, recommendation engines, and reward loops such as likes and shares. These are not neutral features. They are built to maximise the time a user spends on the platform, and there is good reason to think their pull on the developing adolescent brain differs from their pull on adults.

The law is starting to see the design itself as the problem. In March 2026, a California jury found Meta and Google potentially negligent in how they designed their platforms, the first time a jury had found social media companies liable under a product-design theory, after viewing internal messages in which the company discussed winning over “tweens” and noted how much more often eleven-year-olds returned to Instagram. A day earlier, a New Mexico jury found Meta liable for failing to protect children and ordered it to pay \$375 million. Separately, the European Commission has provisionally found that Instagram and Facebook breached the Digital Services Act (DSA) by not keeping under-thirteens off their services.²⁰ In July 2026, it also provisionally found that their addictive design, including infinite scroll, autoplay, push notifications and personalised feeds, breaches the same law. It had made a similar finding against TikTok in February. A final decision can bring a fine of up to 6% of a company's global annual turnover.²¹

The clearest example came in August 2026, when Meta agreed to pay up to \$16.68 billion to settle claims brought by a group of US states. The states had alleged that its platforms were built to attract and hold the attention of children. Meta denies the allegations and any liability. What matters for policy is not the money alone, but the obligations attached to it. Meta must build an age-assurance system that is tested every year by an independent third party against set error limits. Teenagers get an overnight block on access, daily time limits across its apps, and reminders after set periods of use. Like counts are hidden by default, teen accounts on Instagram stay private, and teenagers must be offered a feed that is not personalised. Parents receive alerts about their child's activity, including repeated searches on harmful topics. An independent auditor will check whether the changes are actually delivered.



This is, in effect, a design code enforced through a court, and it shows that the design route is practical rather than theoretical. It also raises a direct question for India, because the agreement covers users in the settling US states, and it is not yet clear how much of it Meta will extend to Indian users.

There is a thread joining these decisions and it matters for India. The problem is not only that children have social-media accounts. It is also how platforms are built and designed to keep them engaged once they are online. Rules that only target accounts can be easily circumvented, including by using VPNs. Rules targeting addictive or harmful design features get to the point more.

This is not a far-off or hypothetical risk. In early July 2026, an Indian media outlet looked into paid ads on a major platform that promoted content about child sexual abuse and sent users to channels where it was sold. In one case, the platform's automated systems had flagged the content as not a violation when it was reported. The Indian authorities issued a notice to the company asking for an explanation within seven days as to why the content was allowed and asked for the blocking of the offensive ads and content, highlighting in particular the algorithmic amplification which had increased their reach. It is a reminder that the platform design and monitoring practices that fail to address age restrictions at the account level are often the most damaging to children.

The government also tightened the wider rules this year, requiring platforms to follow SOPs (standard operating procedures) for handling content with child sexual abuse material (CSAM) and take down such information within three hours of a legal order, rather than (previously) thirty-six. This is enforcement of existing law in action and shows how much can be done without any hard stance.



Professor Shakuntala Banaji

Professor of Media, Culture and Social Change,
London School of Economics and Political
Science (LSE)



Many decades of work with children, young people and new media, including around social media, has convinced me that social media bans targeting children and young people rather than concentrating on regulating the platforms, products, environments and architectures on offer to children and young people are misguided, unenforceable and increase harm to children and young people significantly. Bans on children drive children and young people to find work arounds, some of which can endanger them further and make them more vulnerable to exploitation and predatory cross-platform actors; while turning parents and teachers into enforcers rather than carers and pedagogues. The status quo is one where platform governance has been loosened in favour of profit. Platforms used to have huge trust and safety and integrity teams, all of whom have in the past three years been removed from their jobs of keeping information clean and users safe which is bad for adults and children alike. India should, in my view, take a stern line with the tech platform companies and app developers as Brazil is doing, making them responsible for removing pornographic content, disinformation, misinformation, hateful content, and unwanted behaviours so that we have a social media sphere that is “safe-by-design” and young people and children who are free to learn, explore and be creative with the tools that many of them will be required to use at 17 for work and further education.



Why India Is Different: Scale And Inequality

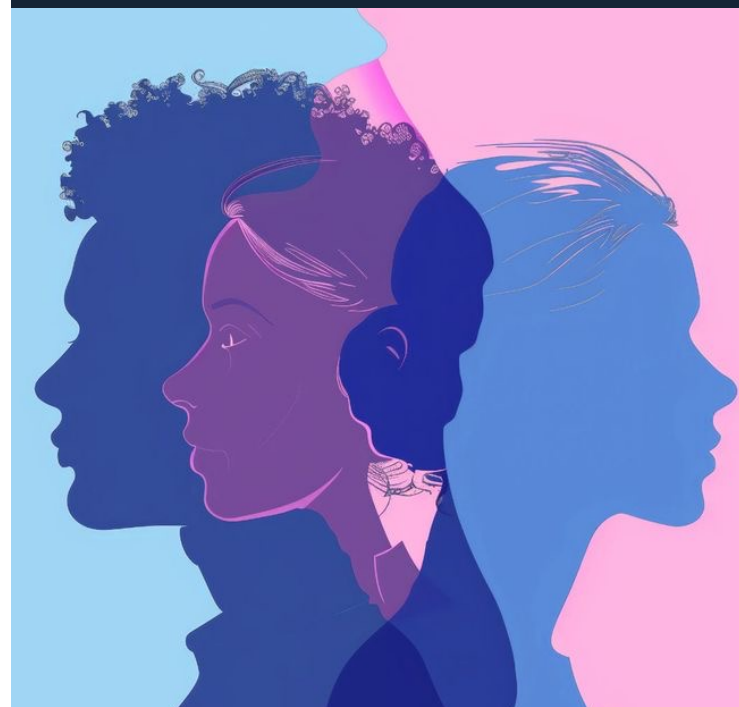
6

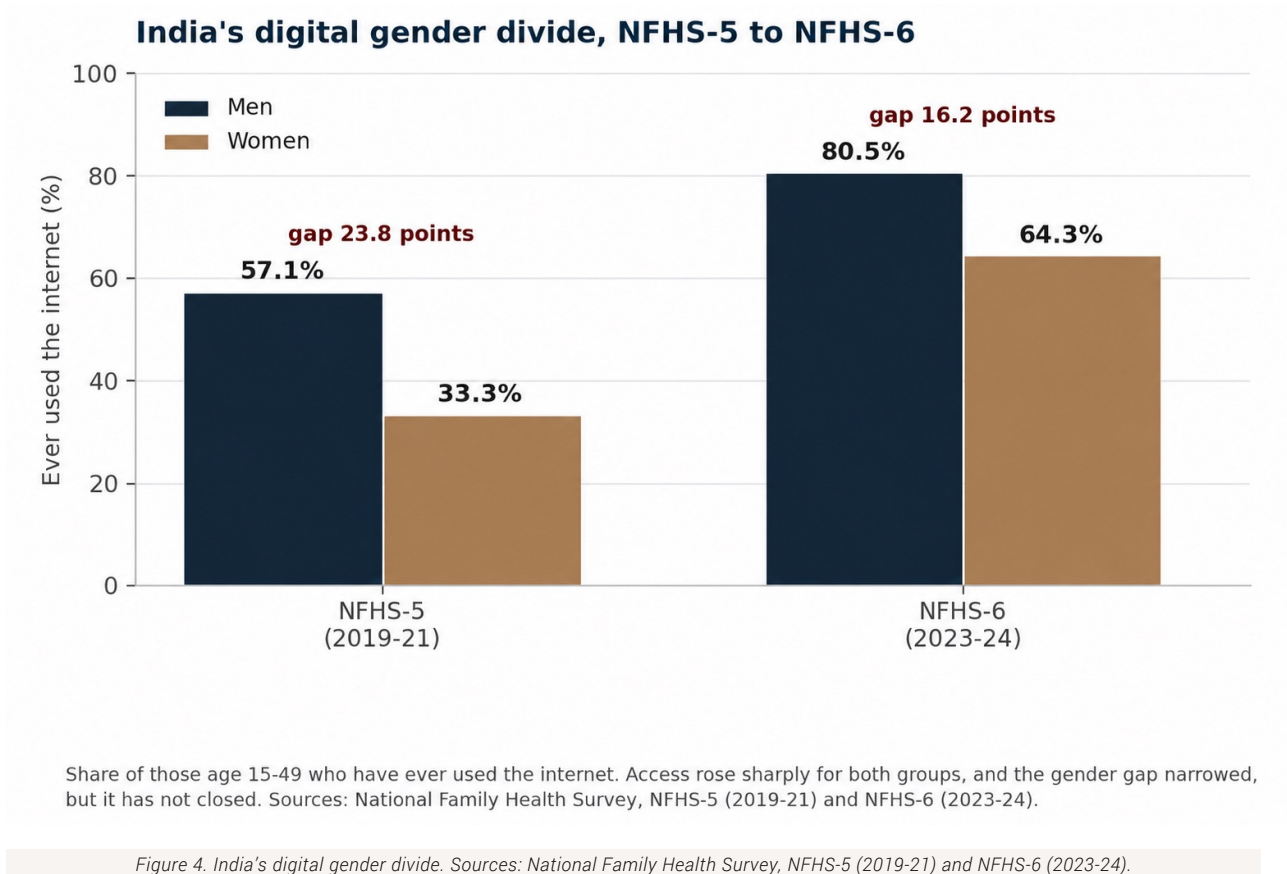
India would not be considering such measures in isolation, but within the context of one of the world's largest and most digitally diverse populations. The country is home to around one billion internet users, alongside half a billion social media users, with teens being one of the fastest-growing demographics, and a 2024 survey found that nearly ninety per cent of kids between ages fourteen and sixteen had a smartphone at home.²² The Economic Survey has officially noted that digital addiction is becoming more common among youth, and the importance of age verification. Meanwhile, in the states of Karnataka and Andhra Pradesh there have been moves toward a limit of under sixteen, and under thirteen respectively.

However, the scale of digital adoption is only one dimension of the policy challenge. Equally important is understanding which sections of society would be most affected by any age-based access restrictions. In this regard, India's socio-economic and digital landscape differs significantly from countries such as Australia and the United Kingdom, necessitating a policy approach that is tailored to its unique demographic, developmental, and digital realities.

India's digital divide cuts across both gender and geography. NFHS-6 shows that **64.3% of women** have used the internet, compared with **80.5% of men** - a gap of 16.2 percentage points. The divide is deeper in rural India: only **58.6% of rural women** have used the internet, and the gender gap there is 18.5 points - almost twice the 9.8-point gap in urban India.

Women's internet use has nevertheless nearly doubled from 33.3% in the previous survey. Access is expanding rapidly, but rural women remain furthest behind. This expansion must be considered in any policy that restricts online access: such a measure would now affect a large and growing section of women and girls, not a small minority. Industry estimates put Indian women around a third less likely than men to use mobile internet. In households that share a single device, restrictions on social media tend, in practice, to fall on daughters before sons.





For many girls in smaller towns and villages, a social media account is one of the few dependable windows onto information about health, careers, scholarships and peer support that an urban teenager may take for granted. The point is sharpened by the mental-health component. India has roughly 0.75 psychiatrists per 100,000 people,²³ which is far less than the World Health Organization's recommended minimum, according to the Indian Journal of Psychiatry. Therefore, an online community may be the only source of assistance available to a young person struggling with anxiety, familial abuse, or identity issues. Age restrictions may result in digital marginalization and the loss of peer support networks, experts have warned.²⁴

There is a risk that a measure meant to protect children instead widens the very divide India is trying to close, falling hardest on the girls and rural users who depend most on being online.

That is not to suggest that protection should be abandoned or ignored, but rather that any restrictions should be accompanied by safeguards and substitutes so that the children most dependent on the internet are not made worse off.

India Already Has The Architecture (Of Protection)

7

There is a further reason for India to be wary of reaching first for a ban. It would be reaching past a set of tools it has only just finished building, and that framework is already among the most demanding in the world.

The core is the "Digital Personal Data Protection Act of 2023," which is effective with notifications in November 2025 and will come into force in May 2027. This Act defines all individuals below eighteen years as children, and this is more stringent compared to the US,

where the age limit is thirteen, and the EU where the range varies between thirteen to sixteen. A platform must get verifiable parental consent before processing a child's data, and the regulations specify how this might be done, including using DigiLocker for verification. The most notable aspect of this discussion is that the Act forbids any processing that could be harmful to a child's welfare, including tracking, behavioural monitoring, and targeted advertising aimed at anybody under the age of eighteen. Platforms that violate the rules face fines of up to ₹200 crore.²⁵

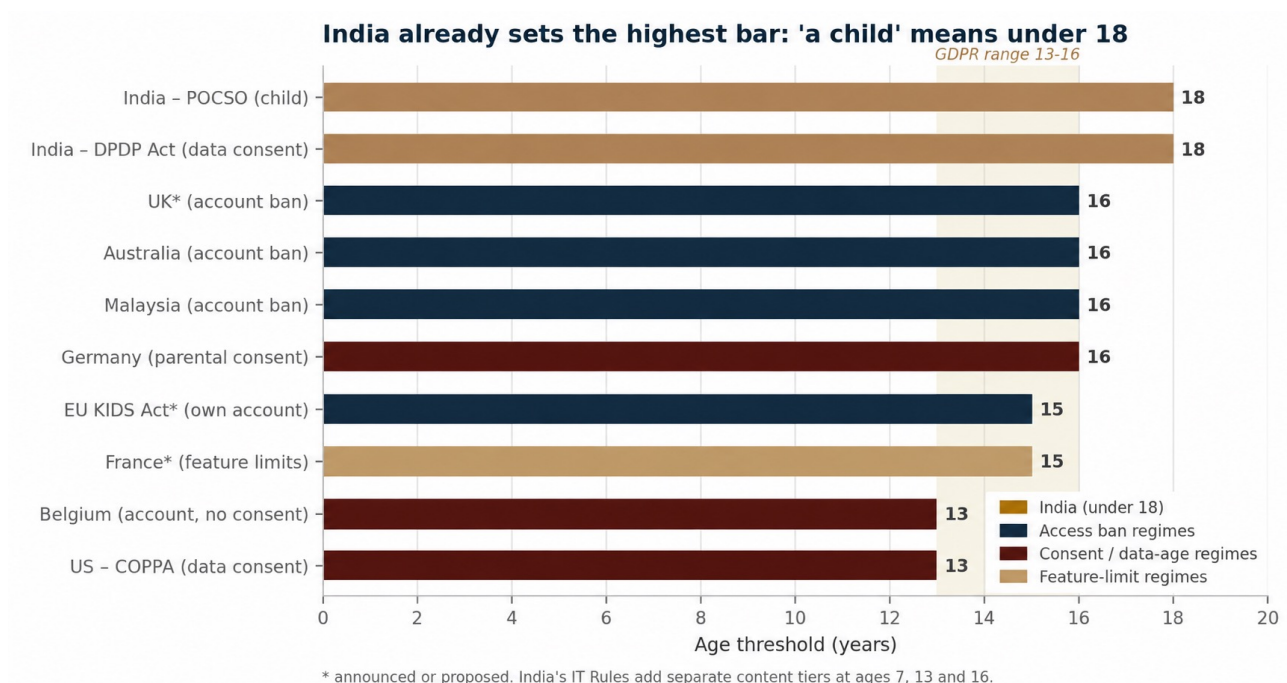


Figure 5. Age thresholds across jurisdictions. India sets the highest bar at eighteen.

Two additional pillars also stand beside it. The Information Technology Act and 2021 Intermediary Rules place due diligence obligations on the platforms, require them to have grievance officers and timely removal of unlawful content, and offer safe-harbour protection only after compliance. They require streaming platforms to categorize the content according to age and provide parental lock as well. The Protection of Children from Sexual Offences (POCSO) Act brings the online sexual exploitation of children within criminal law.²⁶

India's own process moved quickly in August 2026. On 20 August, the Delhi High Court disposed of a petition seeking limits on children's access to social media, holding that this is a policy matter for the government rather than something a court should order. It asked the Centre to examine the concerns raised and to consult stakeholders, including the platforms, and set no deadline.²⁷

In August itself, MeitY held a consultation on age restrictions for children, chaired by the Secretary and attended by child-rights bodies, researchers and civil society groups.²⁸ The discussion concluded that a complete ban would not be effective, and several participants.

The question has since reached the Supreme Court. In September 2026, the Court took up a public interest petition from the Just Rights for Children Alliance, which asks for compulsory age checks and verified parental consent before children can open social media accounts. The petition does not ask for children to be kept off platforms altogether. At a hearing on 28 September, the bench said such safeguards should have the force of law. In response, the Solicitor General said the Centre would amend the IT Rules so that platforms do not let under-18s open social media accounts, while children could still join educational websites with a parent's consent. No draft rules have been published yet, and it is not yet clear what role parents would have. The case is due back in court in late October.²⁹

argued instead for safety by design and a legally enforceable duty of care on platforms. Participants also noted that the risks extend beyond social media to AI chatbots and gaming. Following the consultation, the National Commission for Protection of Child Rights is preparing a code of conduct for children's safety online, working with MeitY, the Department of Telecommunications, the Indian Cyber Crime Coordination Centre and the platforms. The code is expected to work as guidelines, though the Commission can fall back on its statutory powers if they are ignored.



Ashish Aggarwal

Vice President and Head of Public Policy,
NASSCOM



Keeping children safe online is one of the defining questions for India's digital policy. We need open, evidence-led debate to get this right, especially given India's scale and diversity. Access-based measures, design obligations, age assurance, parental tools and enforcement all need to be assessed against the same tests. They should be effective, privacy-preserving, proportionate and workable at scale. India has already set out one of the most demanding frameworks anywhere for children's data protection through the DPDP Act, which comes into full force in May 2027. The work ahead is to put that framework into practice through safer product design, genuine accountability for how platforms engage young users, and credible enforcement. We should protect all young people, boys and girls, urban and rural, while keeping open the pathways that give them learning, opportunity and support.



The Primus View: A Design-First, Inclusion-Aware Path

8

A blanket ban has clear appeal as a decisive, visible measure, and it may well form part of India's eventual response. Our view is that, for a country of India's scale and inequality, a ban on its own is unlikely to be the panacea and should not be the first or only step, but rather a gradual afterthought. Drawing the threads together, we set out below where India's effort is best directed, and how the main options compare.

Weighing the options: a Primus assessment of four paths

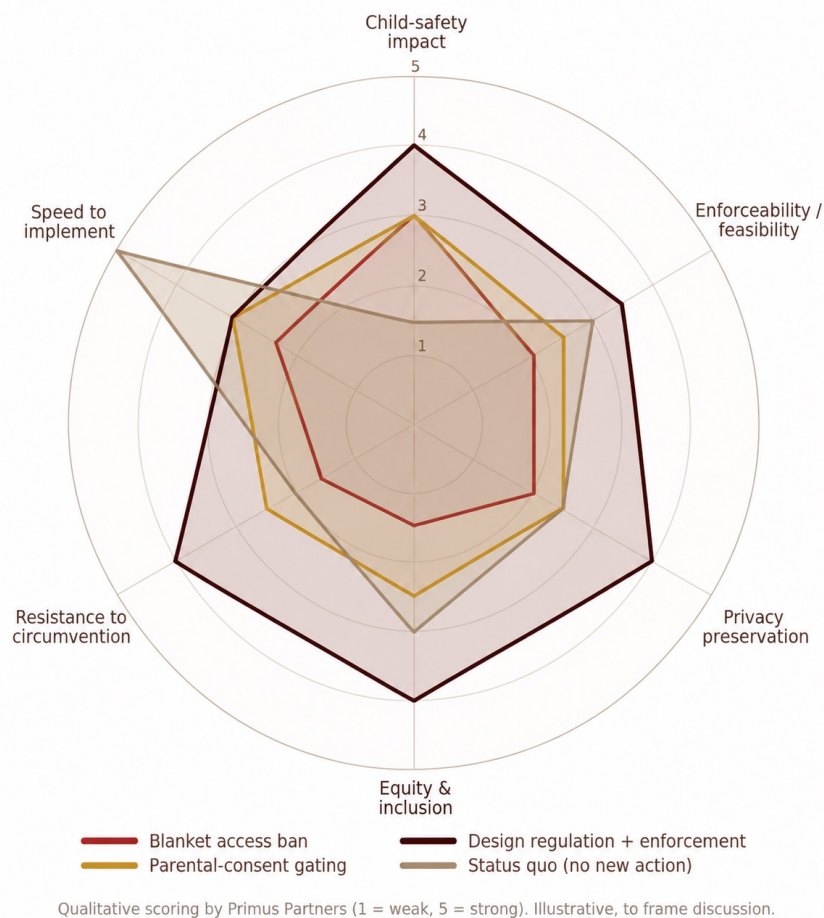


Figure 6. A Primus assessment of four policy paths (1 = weak, 5 = strong) basis expert opinions and inputs gathered. Illustrative, to frame discussion.



Regulate design, not access

The strongest protection comes from changing how platforms behave, not from trying to keep children off them. In line with the UK's Age-Appropriate Design Code, India should impose **a design code for significant social media intermediaries** that prohibits minors from using autoplay by default, limits the frequency of notifications, eliminates infinite scroll, and mandates that recommendation engines provide age-appropriate content by default for users under the age of eighteen.

A lot of this is already implied by the existing prohibitions of the DPDP Act; and a code-based approach would make it concrete and testable.

This code should be risk-based rather than a static, binary list of prohibited features. It should require platforms to assess how combinations of features such as autoplay, notification, personalised feeds affect children's ability to disengage and its impact on child behaviour on social media platforms.

[The recent settlement between Meta and US states shows what this could look like in practice. For users under 18 in the settling states, it requires Meta to introduce \(see below\):](#)



A two-hour daily limit for users under 18



Break reminders or pauses after every 15, 60 and 90 minutes of use



Night-time access restrictions



Limits on school-hour notifications



Stronger age assurance mechanisms



Options for minors and parents to switch off personalised feeds in favour of chronological feed

This code-based approach should therefore place more impetus on pushing platforms to conduct extensive child-safety impact assessments and report the same to concerned authorities, before introducing or materially changing algorithmic nuances. This should also distinguish between different age nuances rather than treating it as a **"one-size-fits-all"** approach.



India can also learn from the European Union's planned Digital Fairness Act, which focuses on addictive design and deceptive features targeted at young users. The proposed EU KIDS Act, which would make safer settings the default for children, offers a second model.

A July 2026 European Commission consultation with nearly 5,000 children found that 48% wanted rules addressing addictive design features that keep users online for longer, indicating that children's own views are increasingly informing how these frameworks are being developed.

The takeaway is simple: regulations should focus on how something is made, not just who can open an account.



Enforce what already exists before adding restrictions

The DPDP guidelines come fully into effect in 2027, and it is imperative that we begin ensuring their implementation, which would include building an age-assurance and consent-verification infrastructure, adequately resourcing the Data Protection Board, and holding platforms accountable under what is already in the lawbooks. Any further restrictions without enforcing the existing rules may create the impression of action, but will not solve the problem at hand.

In a similar vein, platforms are currently required by the IT Act and the 2021 Intermediary Rules to ensure safety and due compliance.

A clear template for how platforms show content to younger users is provided by the parental-lock and content classification regulations now in place for streaming services. And as previously mentioned, the POCSO Act makes online exploitation illegal, and current events demonstrate the need for strict and public enforcement of this obligation. Within DPDP, appointing the Board is the pivotal first step. Once seated, the Board's first task should be defining what "verifiable" consent requires in practice by outlining accepted verification methods, acceptable error rates, and a dispute mechanism for when a platform's age-check gets it wrong. It should also require Significant Data Fiduciaries to file periodic compliance reports that go beyond attestation: verification volumes, error and appeal rates, and the resulting reduction in unverified or underage accounts.

There is already a useful precedent for strengthening direct accountability without introducing new legislation. Following the NCPCR's inquiry into child sexual abuse material linked to advertisements on Instagram, and a separate examination by the NHRC, Meta agreed to report child-safety matters directly to India's cybercrime reporting system through I4C, rather than relying primarily on the US-based NCMEC channel. This could provide a useful model for other major platforms as well. The government can build on the existing roles of NCPCR, NHRC, MeitY and I4C to establish clearer reporting and escalation arrangements for child-safety cases. Once the Data Protection Board is operational, the respective roles could also be made clearer, with data-processing, consent and privacy issues handled through the DPB, while matters involving harmful content, child exploitation or potential criminal offences continue to be taken up through I4C and the relevant child-protection or law-enforcement authorities. This would give platforms greater clarity on where different types of concerns should be reported, while making the overall system easier to coordinate and enforce.



Build genuine algorithmic accountability

Meta's Oversight Board is one example of a voluntary structure that functions with minimal formal ties to Indian regulators. In terms of interaction with upstream algorithmic design, even the IT Rules Grievance Appellate Committee, which offers a mechanism for user complaints, falls short.

India should require every significant social media intermediary to file an annual, India-specific **algorithmic impact assessment** covering what is served to users under eighteen, and should create a standing channel between the Data Protection Board or an equivalent body or figure, the oversight bodies and platform Trust-and-Safety teams; so that accountability is both internal to the platform and externally verified. Recent events, where advertisements promoting illegal content were approved by automated systems and then amplified, show why this accountability should extend specifically to how platforms approve advertising and recommend content to young users. The Meta settlement offers a working model here, because it places an independent auditor between the company and the regulator, with access to the data needed to check what has actually changed.

The assessment should test what platforms actually do, not only what their policies say.

For example, regulators could create a test account for a minor and examine whether recommendations expose it to harmful content, how quickly this happens, and whether viewing such material leads to more extreme recommendations. This would not require access to the platform's source code - only enough access to test how the system behaves and affects users.

This is closer to how the EU is approaching recommender-system enforcement, where regulators can investigate whether platforms have properly assessed and mitigated systemic risks rather than merely asking whether they have published information about their algorithms.



The recent Meta settlement provides a much more concrete model for how this external accountability could work. The August 2026 agreement requires an independent auditor to review Meta's compliance annually for five years, while Meta will also establish an independent social-media research foundation and provide it with consented user data for research into teen wellbeing. The lesson for India is not to reproduce the settlement's specific controls, but to establish a three-part accountability mechanism: platform assessment, independent testing and regulatory oversight.



Design for inclusion, not exclusion

Before any access restriction is adopted, its **effect on the digital gender and rural divides should be assessed** openly. Any safety measure should be paired with investment in digital literacy and access for girls, and with offline alternatives for young people, like the United Kingdom has paired its ban with funding for youth services. A measure that ends up widening the divide would not truly serve the goal of child protection.

This would be one of the essential tenets towards realising the goal of a 'Viksit Bharat'.

9 Conclusion

The harder task for India is to make sure that visible measures are also effective ones. An age-based ban may have a role to play, but on its own it does not resolve the underlying issues of platform design, weak enforcement and digital inequality, and it brings real challenges of implementation and circumvention that need to be planned for rather than assumed away.

The first step India should take would be to implement already existing protection measures, such as enforcing limits on targeted ads and tracking of children, creating trustworthy age assurance and parental consent systems, as well as regulating the addictive nature of algorithms of certain platforms.

Along with parental guidance, improved community-level digital education and awareness can help improve protection. Regardless of the tools India uses, the objective should be to create an online space that is safe for children. That is a more demanding path than any single measure, and it is the one most likely to protect children without shutting them out.



Annexure | What social media platforms are saying about age-based bans and restrictions

The need for more robust internet safeguards for children is widely acknowledged by major platforms.

Platform	Public position on bans / restrictions	What it argues for instead
Meta - Instagram, Facebook, Threads	Meta says cutting teenagers off from social platforms is not the best solution and may produce inconsistent protection as young people move across apps. It also argues that reliably distinguishing a 15-year-old from a 16-year-old is technically difficult, while requiring ID from every user creates privacy and identity-theft risks. In August 2026, Meta also accepted a detailed set of design and age-assurance obligations as part of its settlement with US states, while continuing to deny the allegations.	Age verification and parental approval at the app-store or operating-system level , combined with protected teen experiences such as Instagram Teen Accounts. Meta notably supports an EU-wide "digital majority age" where younger teens can access services with parental approval rather than through an outright ban.
TikTok	TikTok's stated position is that "blunt age bans won't work" and can push younger users towards less regulated parts of the internet where safety tools and protections are weaker.	Safety-by-design measures differentiated by age: default screen-time limits, restrictions on direct messaging and other features, Family Pairing and stronger age assurance.
Snap - Snapchat	Snap argues that Snapchat is principally a messaging service , rather than conventional social media, and says its inclusion in Australia's ban is misplaced. It also warns that disconnecting teenagers from friends and family could drive them towards less safe and less private alternatives .	Privacy-preserving age checks at the device, operating-system or app-store level, rather than requiring every platform separately to collect or verify age information.
Google - YouTube	YouTube argues that it is primarily a video and learning platform rather than a conventional social network. More importantly, it says Australia's model can be counterproductive: under-16s can still watch YouTube while logged out, but lose supervised accounts, content controls, bedtime reminders and other protections available to logged-in teenagers.	Age-appropriate and supervised access , with parental choice, wellbeing settings and differentiated experiences for children and teenagers rather than removing account access altogether.
Reddit	Reddit has gone furthest, challenging Australia's law in the High Court. It argues that a blanket account ban raises privacy and political-expression concerns , can exclude teenagers from age-appropriate communities and imposes age checks on adults as well as children. It also disputes a regulatory model in which broadly similar online services are treated differently.	More targeted restrictions, including content-specific protections, together with privacy-preserving age assurance at the device or app-store level . Reddit has described the UK's more targeted approach to particular kinds of content as more balanced than an account-wide prohibition.

10 References

1. Online Safety Amendment (Social Media Minimum Age) Act 2024 (Australia); eSafety Commissioner. In force 10 December 2025.
2. Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Bill 2026 (Australia), passed by Parliament on 10 September 2026; Prime Minister of Australia, Stronger powers and double the penalties for world-leading social media law (28 June 2026): <https://www.pm.gov.au/media/stronger-powers-and-double-penalties-world-leading-social-media-law>; MLex (14 September 2026). The Commonwealth penalty unit rose from AUD 330 to AUD 364 on 1 July 2026. Rupee values at about ₹67 to the Australian dollar.
3. YouGov survey, reported 2024; CNBC, December 2025.
4. UK Government / Department for Science, Innovation and Technology, announcement of 15 June 2026; Children's Wellbeing and Schools Act 2026; rules expected in force spring 2027.
5. European Parliament resolution on the protection of minors online (2025/2060(INI)), adopted 26 November 2025; non-binding.
6. European Commission, EU KIDS Act (Keeping Internet Digital Spaces Accountable and Trustworthy), proposal of 17 September 2026: https://commission.europa.eu/news-and-media/news/eu-kids-act-helping-children-navigate-safer-online-world-2026-09-17_en
7. https://ec.europa.eu/commission/presscorner/detail/en/ac_26_1630
8. Conseil constitutionnel decision of 14 August 2026; Euronews, France submits new proposal to ban social media for under-15s after failed attempt (14 September 2026): <https://www.euronews.com/my-europe/2026/09/14/france-submits-new-proposal-to-ban-social-media-for-under-15s-after-failed-attempt>
9. Government of Norway, Norwegian social media age restrictions law on track to be introduced this year (24 April 2026): <https://www.regjeringen.no/en/whats-new/norwegian-social-media-age-restrictions-law-on-track-to-be-introduced-this-year-this-is-how-the-age-limit-for-social-media-will-work/id3157276/>; Malaysia's Child Protection Code under the Online Safety Act 2025, in force from 1 June 2026 (The Rakyat Post, 3 June 2026).
10. NetChoice v. Jones (E.D. Va.), preliminary injunction of early 2026; US Court of Appeals for the Fourth Circuit, order of 24 August 2026 (MediaPost, 25 August 2026): <https://www.mediapost.com/publications/article/417439/appeals-court-rejects-virginia-bid-to-enforce-soci.html>
11. Online Safety (Minimum Age and Child Safety Risk Assessment) Bill 2026 (New Zealand), introduced 24 August 2026; MinterEllisonRuddWatts, What the Online Safety Bill means for digital platforms operating in New Zealand (28 August 2026)
12. 1News, Govt says no time for social media bill after Labour backs it (25 August 2026): <https://www.1news.co.nz/2026/08/25/govt-says-no-time-for-social-media-bill-after-labour-backs-it/>
13. <https://news.sky.com/story/worrying-study-shows-australias-social-media-ban-has-made-no-meaningful-difference-to-teenagers-13557426> | C. Barns, Alix Hall, et al, Assessing early effects of Australia's Social Media Minimum Age Act on adolescents' social media use: observational study, The BMJ (2026)
14. <https://www.bloomberg.com/news/articles/2026-08-25/teens-return-to-tiktok-after-world-s-first-usage-ban-data-show>

15. eSafety Commissioner, Early days, early insights: understanding experiences of social media age restrictions (31 July 2026), comparing surveys before the ban and three months after it: <https://www.esafety.gov.au/newsroom/media-releases/early-insights-from-esafetys-comprehensive-evaluation-project>
16. eSafety Commissioner and Australian news reporting, December 2025 to early 2026.
17. Ofcom, Use of Age Assurance Report 2026 (July 2026); a further assessment of how to determine whether a user is over sixteen is due to Parliament by October 2026.
18. S.M. Saleem and S.S. Jan, Cross-sectional study of adolescent mental health and social media use, Journal of Nature and Science of Medicine, 2024 (depression 37.9%, anxiety 33.3%, high stress 43.7%).
19. J. Haidt, The Anxious Generation (2024);

C. Odgers, The great rewiring: is social media really behind an epidemic of teenage mental illness?, Nature (2024);

A. Orben and A. Przybylski, The association between adolescent well-being and digital technology use, Nature Human Behaviour (2019);

J. Twenge and J. Haidt, Specification curve analysis shows that social media use is linked to poor mental health, especially among girls, Elsevier (2024).
20. Los Angeles Superior Court and New Mexico verdicts, March 2026 (CNN, NPR, Fox Business); European Commission preliminary findings on the Digital Services Act.
21. European Commission, Commission preliminarily finds the addictive design of Instagram and Facebook in breach of the Digital Services Act (10 July 2026): https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1579; on TikTok, press release of 6 February 2026: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312
22. ASER Centre, Annual Status of Education Report (ASER) 2024, Pratham (2025)
23. S. Garg et al., Number of psychiatrists in India: baby steps forward, but a long way to go, Indian Journal of Psychiatry (2019); also quoted in PIB in November 2025
24. O. Prakash, Is it time for India to set social media age limits for adolescents?, Indian Journal of Psychiatry (2025); Misc. reports
25. Digital Personal Data Protection Act, 2023; DPDP Rules 2025 (notified 13 November 2025); substantive obligations effective 13 May 2027; Section 9 and Rule 10.
26. Information Technology Act, 2000; IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Protection of Children from Sexual Offences Act, 2012.
27. <https://www.thehindu.com/news/cities/Delhi/restricting-childrens-access-to-social-media-is-centres-domain-delhi-high-court/article71370077.ece>
28. <https://www.medianama.com/2026/08/223-meity-social-media-consultation-children/>
29. Just Rights for Children Alliance v. Union of India, W.P.(C) No. 1120/2026, Supreme Court of India: notice issued on 10 September 2026 (LiveLaw, 10 September 2026); hearing of 28 September 2026 (Business Standard, 29 September 2026): https://www.business-standard.com/india-news/centre-to-amend-it-rules-to-bar-under-18s-from-social-media-accounts-126092900418_1.html

Authors



Nilaya Varma
Group CEO & Co-Founder



Indranuj Pathak
Manager



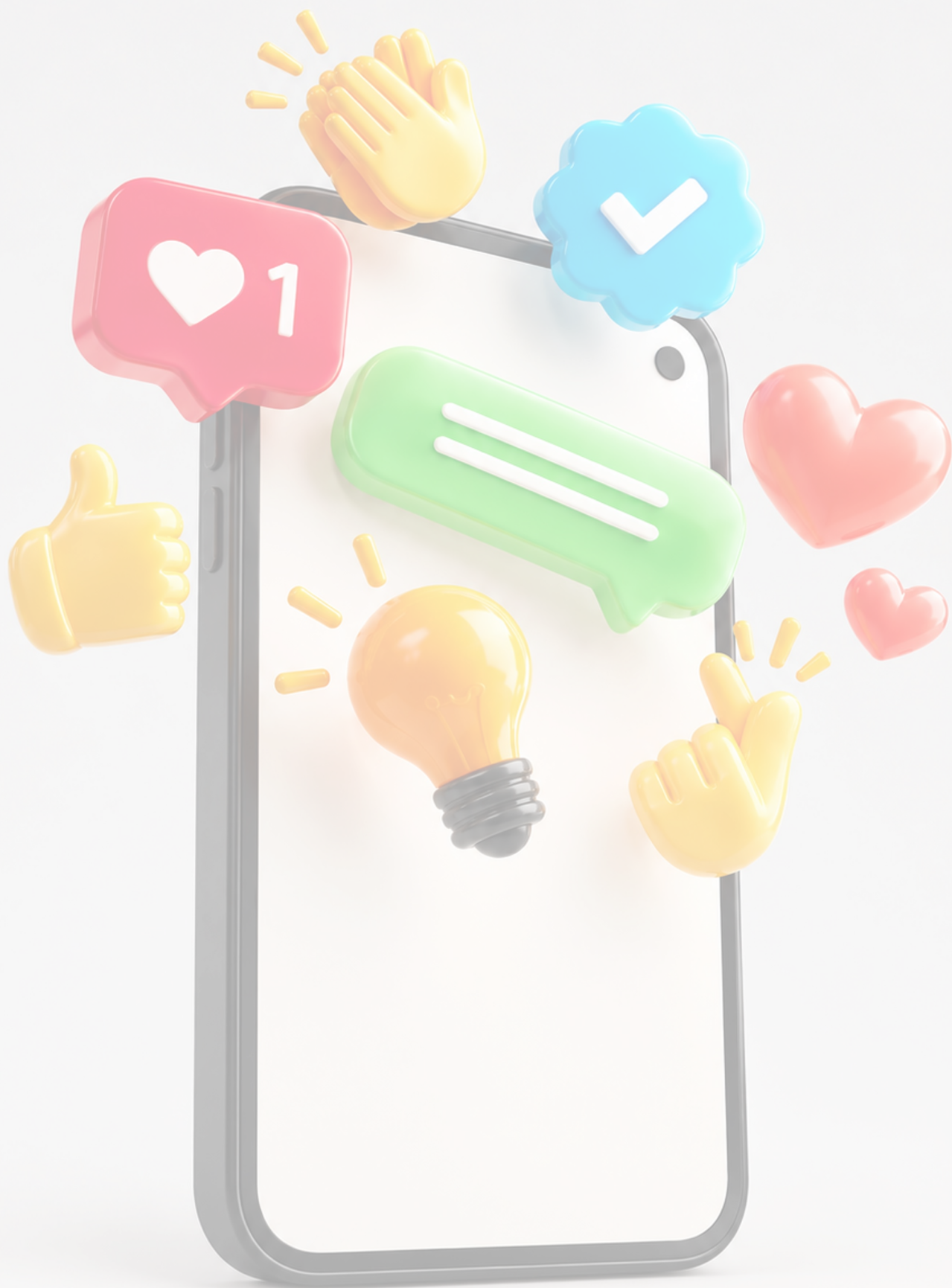
Sakshi Naphade
Senior Consultant



Ankush Sharma
Senior Consultant



Parul Kataria
Consultant



PRIMUS

PASSION

for providing solutions to help clients achieve their goals

RESPECT

for all and alternate viewpoints

INTEGRITY

of thoughts and actions

MASTERY

of our chosen subject to drive innovative and insightful solutions

US

representing the Primus collective, where each individual matters

STEWARDSHIP

for building a better tomorrow



PRIMUS PARTNERS®

Solutions for Tomorrow

Primus Partners is India's largest homegrown management consulting and policy advisory firm, partnering with clients to navigate India and translate ideas into practical outcomes. Founded in 2019 by seasoned industry leaders with decades of experience in global organisations, the firm draws its core strength from its founding partners' hands-on experience, recognised subject expertise and focus on results.

Built on the principle of "Idea Realization", Primus examines forward-looking ideas for the growth of an organisation, sector or geography through the lens of their practical implementation on the ground. This philosophy brings "experience in action" to every engagement, connecting strategy with delivery.

The firm has grown to a team of 400+ consultants, supported by advisors, and has delivered 240+ engagements across 13+ sectors. These include technology, aerospace and defence, automotive, tourism, urban development, healthcare, FMCG, energy, climate and sustainability, finance, and investment promotion.

Primus operates from offices in six Indian cities, with delivery experience spanning 18+ States and Union Territories. Its growing international footprint includes offices in the USA, the UAE and Saudi Arabia, serving clients and institutions across 14+ countries. Through its specialist arms, Primus Solutions and Primus GCC, the firm extends its capabilities to technology-enabled delivery and Global Capability Centre advisory.

Primus works closely with governments, regulators, private industry, and leading multilateral and international organisations. It serves five of the world's top technology companies and holds one of the top two media Share of Voice rankings among consulting firms globally. This reflects the firm's commitment to research and thought leadership as strategic investments supporting its advisory work.

India Offices



Bengaluru

91 Springboard
Business Hub 175, 176
Bannerghatta Rd,
Dollars Colony,
Bengaluru – 560076



Chandigarh

2nd Floor, Netsmartz,
Plot No. 10, Rajiv
Gandhi Chandigarh
Technology Park,
Chandigarh – 160019



Chennai

147, Pathari Rd, Door #3,
WorkEz Hansa Building,
RK Swamy Centre,
Thousand Lights,
Chennai, TN - 600006



Delhi

1 to 7, UG Floor,
Tolstoy House,
Tolstoy Road,
Connaught Place
New Delhi - 110001



Kolkata

Collab Deck (Cabin
W1021)
Kankaria Centre,
2/1 Russel Street, Park
Street Area,
Kolkata - 700071



Mumbai

156/157, 15th Floor,
Nariman Bhavan,
NCPA Road,
Nariman Point,
Mumbai – 400021

International Offices



Dubai

United Arab Emirates
(UAE)



Dammam

Kingdom of Saudi Arabia
(KSA)



Washington D.C

United States of America
(USA)

www.primuspartners.in

info@primuspartners.in

[in](#) Primus Partners India

[X](#) @partners_primus

[v](#) @primuspartners7128