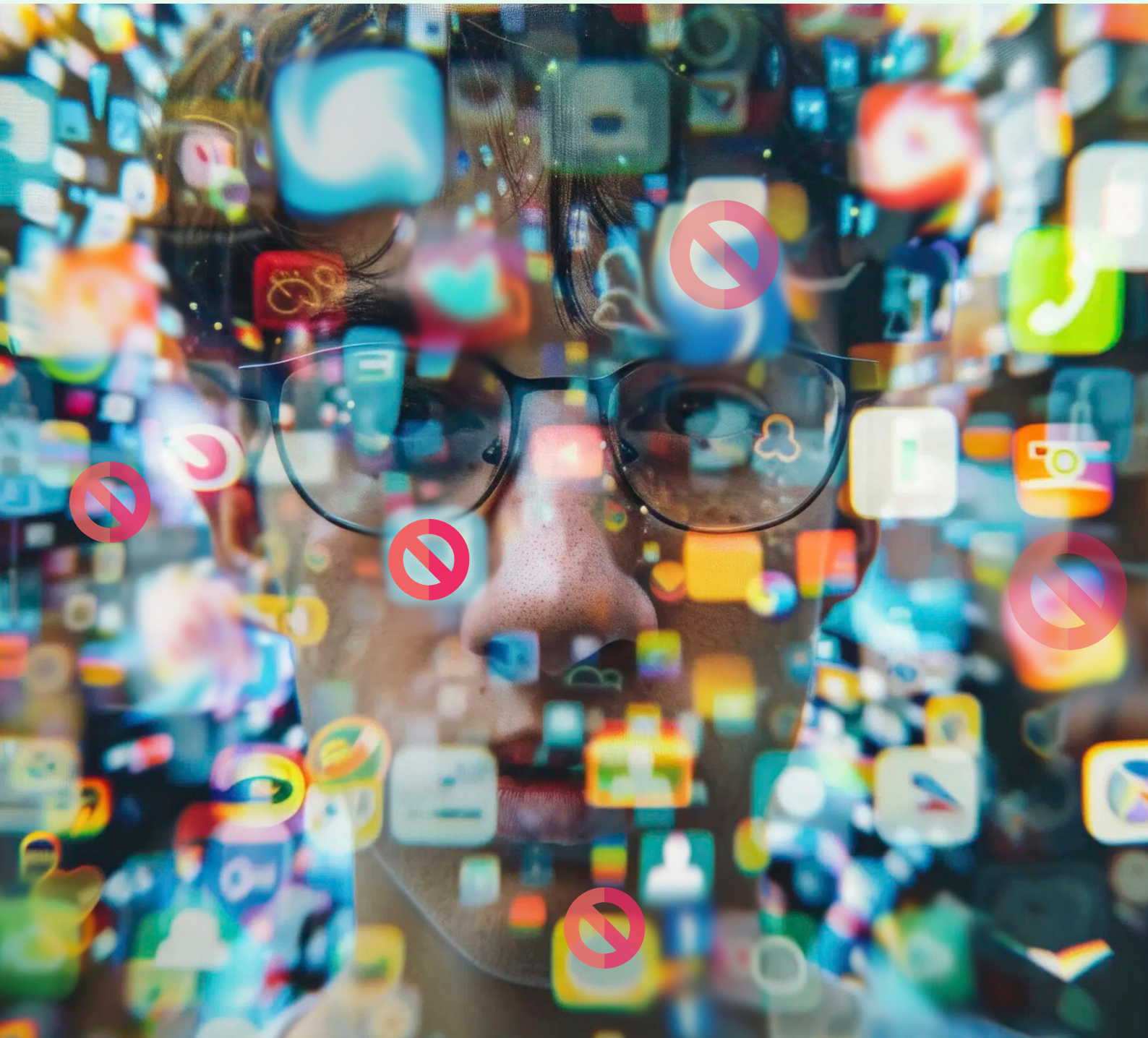


Regulating Childhood Online: **Australia's Social Media Minimum Age Law**



December 2025

REGULATING CHILDHOOD ONLINE: AUSTRALIA'S SOCIAL MEDIA MINIMUM AGE LAW

Published by

Indian Governance and Policy Project (IGAP)

Authored by

Ananya Agarwal and Akhila Nair

Designer

Manoj Murali

About IGAP

The Indian Governance and Policy Project (IGAP) is a policy, business advisory, and research studio working at the intersection of governance, technology, markets, and national development.

Grounded in a clear understanding of how state capacity, market forces, and emerging technologies shape India's strategic trajectory, IGAP addresses key questions that define the country's future — from the governance of AI and digital infrastructure to financial innovation, sustainability, and national security.

Bringing together lawyers, policy thinkers, and strategists with deep business and geopolitical insight, IGAP delivers solutions that balance India's developmental and security priorities with its democratic values and constitutional principles.



This study is published under the Creative Commons Attribution-CC BY-SA License. This license allows others to copy, distribute, remix, adapt, and build upon the material in any medium or format, provided appropriate credit is given to the creator and any derivative works are shared under the same license.

TABLE OF CONTENTS

- A. Background 04
- B. Core Legal Framework 05
- C. Enforcing the Ban 06
- D. Legal Challenge 08
- E. Operational Implications of the Social Media Minimum Age Law 09
- F. International Response 13
- G. Conclusion 14

A | Background

It has been over a week since Australia's social media minimum age law came into force, and the effects are already being felt in uneven and, in some cases, predictable ways. Major platforms have begun removing accounts¹ flagged as belonging to users under 16, but for many families, the rollout has been confusing. Parents and teenagers alike have reported unclear age checks, patchy appeal processes, and sudden loss of access to group chats and online communities.² Some teenagers say they've been locked out even though they're close to the age cut-off, while others, including some who have figured out ways to bypass these restrictions, seem to have stayed online entirely, prompting early questions about how consistently age verification is working in practice.

These inconsistencies echo longstanding concerns about voluntary age enforcement. In 2024, around 95% of Australians aged 13–15³ reported using social media despite platform age rules. At the same time, an estimated 1.3 million children aged 8–12⁴ were accessing social media services below the stated minimum age. Among those younger children who had their own accounts, 77% said a parent or carer had helped set them up, suggesting that enforcement gaps are not new, but rather deeply embedded in how families and platforms have operated for years.⁵

The pressure to act had been building well before the law came into force. Reporting⁶ over recent years has linked intensive platform



What Do Parents Think?

Support for Externalised Enforcement

"I was worried that they would feel like something was taken away from them or they would respond in a negative way, but they have been winding down their social media use even before the ban, so it's nice to have them present in the house again."

"Now I feel backed by the government and relieved that our country is taking the online safety of our youth seriously. Many parents are blind to what their kids get up to online."

"We see this as a lifeline. Our daughter is hopelessly addicted to her phone, and less time on socials – and with more meaningful connection – has to be a good thing."

Concerns About Implementation and Trust

"My 13-year-old daughter had no trouble passing Snapchat, TikTok and Instagram age verifications. She's now doing them for all of her friends."

"The internet is resilient in circumventing blocks and new social media tools will appear that will be worse."

"It has made the children feel alienated, patronised and distrusted. They (and I) would rather see regulation of the social media companies than the children. We know that is impossible to achieve in this world where money is valued over wellbeing."

use among adolescents to disrupted sleep, heightened anxiety, academic distraction, and constant pressure to remain online. Educators have described classrooms shaped by algorithmic attention, while parents have spoken about the difficulty of setting limits in environments where social participation increasingly depends on platform presence.

Against this backdrop, support for a clear, externally enforced boundary grew, with almost 65% of Australian parents backing⁷ a statutory minimum age.

It is in response to these concerns that the Online Safety Amendment (Social Media Minimum Age) Act 2024 (**SMMA**) was introduced.

The policy rationale behind the law is threefold: to protect children from online harms, to reduce the pressure placed on families to regulate access individually, and to provide parents and schools with a clear, nationally consistent standard.

By shifting responsibility away from households and onto platforms, the law seeks to replace ongoing negotiation with a clear legal boundary, one that parents and schools no longer have to continually justify or enforce on their own.

B | Core Legal Framework

The SMMA amended the Online Safety Act 2021⁸ to introduce a mandatory minimum age of 16 for accounts on designated social media platforms. Under the SMMA, providers of Age-Restricted Social Media Platforms (**ARSMPs**) are required to take “reasonable steps” to prevent Australians under 16 from creating or maintaining accounts. Importantly, as the enforcement responsibility rests entirely with platforms, the legislation does not impose penalties on children or their parents where underage access occurs.

C | Enforcing the Ban⁹

AGE VERIFICATION MECHANISMS

Platforms must implement age assurance measures, but are expressly prohibited from relying solely on government-issued identification, including Digital ID. This has led to layered approaches combining multiple methods:

Facial age estimation, used by platforms such as TikTok and Snapchat, is often done through third-party providers such as Yoti or k-ID. Meta employs “video selfies” or government ID for users changing their self-declared birth date.

Internal data signals, whereby Google platforms such as YouTube assess age based on information associated with linked accounts and usage signals.

Appeals processes, allowing users whose accounts are removed or restricted to contest decisions through additional verification methods, including video or selfie-based age estimation, bank card checks, or a government ID.

In practice, regulators also expect platforms to take steps to detect and investigate circumvention methods such as the use of virtual private networks (**VPNs**).¹⁰ This may involve cross-referencing a user’s IP address with historical GPS coordinates and location data to identify active VPN connections.



How Platforms Estimate a User’s Age

1 Biometric Inference (Facial Age Estimation)

This refers to the use of artificial intelligence to estimate a person’s age based on facial features, typically through a photo or short video. Rather than identifying who someone is, these systems assess visual markers, such as facial structure, skin texture, and proportions, to estimate an age range.

2 Behavioural Signals

Platforms may assess how an account behaves to infer whether the user is likely to be underage. This can include patterns such as:

- types of content viewed or interacted with,
- time of day the account is most active,
- interaction styles that differ between children and adults.

3 Cross-Account or Linked-Account Analysis

Some platforms infer age by drawing on information from related or linked accounts within the same service ecosystem. For example, activity or age information associated with a linked email account, family account, or other services operated by the same company may inform age assessment decisions.

DATA PROTECTION & PRIVACY SAFEGUARDS

The use of age assurance technologies under the SMMA significantly expands the volume and sensitivity of personal data that platforms must process, particularly where verification relies on biometric inference, behavioural signals, or cross-account analysis.¹¹ While the handling of this information continues to be governed by the Privacy Act 1988, the SMMA introduces heightened scrutiny through additional obligations under Part 4A¹² of the Online Safety Act, which applies specifically to the collection and use of data relating to children.

The SMMA requires platforms to adopt a data minimisation-by-design approach to age assurance. Platforms must limit data collection to what is strictly necessary to determine age eligibility, avoid retention of raw biometric or verification data once an assessment has been made, and ensure that verification systems are designed to prevent function creep.

Platforms are also subject to strengthened obligations around secure handling and disposal. Age assurance data must be stored separately from general user data where possible, protected through appropriate technical and organisational safeguards, and deleted once its purpose has been fulfilled.

Importantly, the SMMA places clear limits on secondary use. Where platforms seek to use age assurance data for purposes beyond compliance, such as targeted advertising, recommendation optimisation, or internal research, explicit, informed user consent is required.

COMPLIANCE & PENALTIES

Failure to meet these obligations exposes platforms to regulatory enforcement under privacy law, including investigation by the Office of the Australian Information Commissioner, compliance orders, and potential civil penalties up to A\$49.5 million. In serious cases, mishandling of age verification data may also trigger liability under Australia's statutory tort¹³ for serious invasions of privacy.

To counter the foreseeable outcome of underage users migrating to unregulated alternatives, the SMMA allows the government to expand coverage to additional platforms where necessary.

D | Legal Challenge

The SMMA is currently being challenged before the High Court through multiple proceedings.¹⁴ One of these has been brought on behalf of **two 15-year-olds, with the backing of a civil liberties organisation**. Their core argument is that *a blanket ban on under-16s using major social media platforms places an unjustified burden on the implied freedom of political communication under the Australian Constitution*. They argue that the law effectively cuts young people off from spaces where political information is shared and debated, operating as a form of prior restraint that is neither proportionate nor reasonably tailored to the Act's stated child-protection aims. *The challenge also raises broader privacy concerns*. In particular, it points out that enforcing age limits at scale is likely to require platforms to collect, infer, or process personal data from all users, not just children.

A parallel challenge has been filed by Reddit Inc., which takes aim at the design and practical operation of the SMMA. Like the youth-led challenge, Reddit argues that the law restricts political communication by excluding young users from online spaces that function as forums for civic discussion. Beyond that, *Reddit contends that the Act relies on an overly blunt, one-size-fits-all approach that ignores differences between platforms, their risk profiles, and the safety measures they already have in place*. In its view, less restrictive alternatives, such as age-appropriate design requirements, targeted moderation, or graduated access models, have not been meaningfully considered.

Reddit also focuses heavily on the privacy consequences of compliance. It argues that the pressure to verify age is likely to push platforms toward intrusive methods such as identity checks, biometric estimation, or behavioural inference, again affecting all users rather than only minors. This, Reddit says, risks normalising widespread identity verification online, with knock-on effects for data security and user anonymity. Finally, Reddit questions the coherence of the regulatory scheme itself, warning that selective or uneven platform designation could create a fragmented regulatory landscape. This, it argues, may simply push young users toward smaller, less regulated, or offshore services, undermining child safety goals while splintering the digital public sphere.

E | Operational Implications of the SMMA

While the SMMA establishes a clear legal boundary, its impact will depend on how the regulation operates across technical, behavioural, and governance dimensions in practice.

01. Implementing Age-Based Regulations in Digital Environments

Context

Early rollout suggests that determining age online is rarely a clean or mechanical exercise. Age assurance systems work in probabilities, not certainties, which means they are designed to make informed estimates rather than verify age conclusively. Unsurprisingly, this has produced mixed outcomes at the margins: some younger users appear to have passed checks, while others have been excluded despite being close to the threshold. These outcomes point less to system failure than to the practical limits of inferring age in digital spaces, where appearance, behaviour, and identity cues are often partial, fluid, or deliberately ambiguous.

Key Considerations

If age verification is intended to support child safety at scale, what tools are best suited to do so accurately while minimising the risk of misidentification?

When age is inferred through facial analysis, behavioural patterns, or social network data, how should systems account for margins of error, particularly for adolescents close to the age threshold?

What safeguards are necessary to ensure that errors in age determination do not undermine trust in the system or create unfair exclusions?

02. Balancing Age-Based Controls and Safety-by-Design

Context

This shift offers a tangible form of relief to many educators and parents: by restricting access altogether, the law promises an immediate reduction in exposure to algorithm-driven feeds and engagement systems that are widely perceived as ill-suited to younger adolescents.¹⁵ Age policing functions as a clear, enforceable boundary in an environment where platform design has historically been difficult for families and schools to influence.

However, expert responses have consistently emphasized that age restrictions complement rather than replace platform safety obligations.¹⁶ While restricting access may reduce exposure for younger users, it does not alter the underlying design features, recommender systems, engagement-driven feeds, and attention-maximizing interfaces that shape online experiences. Experts caution that treating age as the primary safety lever risks framing harm as a problem of who should be excluded, rather than how platforms are structured.

Several experts therefore argue for a complementary approach: graduated access frameworks that link participation to developmental maturity, alongside sustained investment in digital literacy. Tools like the Bark Phone Starter Plan¹⁷ already reflect this model, allowing calls and texts while removing apps, browsers, and social media for younger children, staging access rather than prohibiting connectivity altogether.

Key Considerations

|| To what extent does enforcing a minimum age reduce exposure to harmful content, compared to requiring platforms to modify design features that affect users of all ages?

|| Can age-based access restrictions and safety-by-design obligations operate as complementary regulatory tools, or does prioritising age policing risk slow momentum for deeper platform reform?

|| Should exclusion be understood as an effective protective measure in itself, or as a temporary mechanism while longer-term design and governance reforms take effect?

03. Youth Adaptation to Age-Based Digital Boundaries

Context

Age-based restrictions are designed to delay entry into mainstream social media environments during early adolescence, a period often associated with heightened vulnerability to peer pressure, social comparison, and impulsive decision-making.¹⁸ However, today's adolescents have grown up with digital platforms as part of their everyday routines. For many, navigating apps, privacy settings, and online workarounds is not exceptional but habitual, and their practical digital literacy often exceeds that of the adults tasked with supervising them.

Early indications suggest that young people are therefore not passive recipients of access limits. Many adolescents are already familiar with informal ways of navigating platform

rules: some report having adjusted their age when first signing up to meet minimum age requirements, others rely on a parent's details, an older sibling's account, or shared devices to maintain access. As access controls tighten, many young users rely on familiar technical workarounds, including the use of tools such as VPNs.

Key Considerations

Do age-based access limits help establish healthier digital boundaries for younger adolescents, or do they incentivise circumvention in ways that weaken trust between young people, families, and institutions?

Does delaying access contribute to more responsible digital behaviour over time, or does early exposure to evasion strategies shape how young people relate to online rules more broadly?

In seeking to reduce harm through restriction, how can policymakers ensure that youth interactions are not displaced into less visible or less moderated online spaces?

04. Age-Based Regulation and the Allocation of Responsibility

Context

For years, parents and schools have been expected to manage children's online exposure through household rules, device restrictions, and school policies, often without meaningful leverage over platform design or enforcement. The SMMA responds directly to this imbalance by shifting primary responsibility for access control from households to platforms. Early reporting suggests that responsibility in practice may remain diffuse. When age checks are bypassed, whether through misclassification, appeals, or informal workarounds, questions arise about who is expected to intervene. Parents may still find themselves navigating decisions about supervision and compliance, while platforms balance error tolerance against regulatory risk, and regulators assess what constitutes "reasonable steps."

Key Considerations

When age-based restrictions are circumvented, how should responsibility be understood in practice between parents, platforms, and regulators, particularly given that families face no formal penalties?

Can a single age threshold adequately account for variation in developmental readiness, family context, and levels of parental involvement, or should flexibility be incorporated elsewhere in the regulatory framework?

05. Uneven Effects of Age-Based Access Limits

Context

While age-based access limits are designed to reduce exposure to online harms for younger users overall, their effects may not be evenly distributed. For the majority of adolescents, online spaces function not primarily as entertainment platforms but as sources of social connection, peer support, and identity affirmation, particularly where such support is limited or unavailable offline. This is especially true for young people in remote or rural communities where local peer networks are limited, adolescents who face social exclusion or lack of support within their family or school environments, and those who use online communities to connect with others who share experiences or identities that may not be visible or supported offline.

Uneven reliance on social media is not only social, but in some cases economic. A smaller subset of families engage with online platforms as a source of supplementary or primary income through child-led or family-run content creation,⁵ including influencer activity and monetised social media channels. While this activity raises its own regulatory and ethical questions, it underscores that access to social media may, for some households, carry economic significance alongside social value.

Policy discussions around minimum age standards have increasingly acknowledged this uneven reliance on digital spaces. Leading mental health experts have cautioned that for vulnerable groups, particularly LGBTIQ+ adolescents, removing access to these spaces without commensurate offline alternatives may risk exacerbating isolation, loneliness, and psychological distress.¹⁹

Key Considerations

How can age-based restrictions reduce exposure to harm while preserving access to meaningful social connections for young people who rely on online communities as a primary source of support?

To what extent might age-based access limits interact with existing socio-economic differences, where some young people retain access through private supervision or workarounds while others are excluded entirely?

F | International Response

The SMMA is being closely observed internationally and is frequently described by regulators as a potential precedent for future platform regulation.²⁰ This has sparked global debate on balancing child safety with digital rights.

Jurisdiction	Minimum Age Mandate	Policy Difference from Australia
Denmark (Proposed)	15 (Ban with dispensation)	Allows parental dispensation for children aged 13 to 15, acknowledging family autonomy.
Malaysia (Planned)	16 (Planned Ban)	Closely reviewing Australian mechanisms indicates a likely alignment with the Exclusion Model .
Singapore	None (Age Assurance Code)	Adopted an Age Assurance -focused approach that emphasises platform and app-store obligations to implement verification and content controls without imposing a blanket ban on account creation.

G | Conclusion

The SMMA is less important for what it enforces today than for what it signals about where responsibility now lies. By setting an enforceable legal threshold and placing primary obligations on platforms rather than families, the law marks a clear departure from years of child-safety debates that implicitly treated online harm as a parental management problem. For parents and educators long outmatched by the scale, speed, and design of social media systems, this represents a meaningful shift in institutional posture.

This is not to say the law resolves the hard questions. It brings them into sharper focus. Age verification at scale requires infrastructure that affects not just children, but everyone who gets verified. The SMMA tries to limit this through strict data rules; even so, the trade-off remains real. For many parents, these measures seem justified if they actually work. For regulators, the challenge is keeping them proportionate and aligned with privacy, expression, and young people's growing capacity to participate in digital life.

What makes the SMMA particularly significant is that its impact does not hinge solely on flawless implementation. The law reshapes expectations about what platforms owe their users, what risks are no longer tolerated as inevitable, and where accountability should sit when systems fail. The legislation thus operates as much as a tool of norm-setting as one of compliance.

The more difficult questions may be this: Can we protect children without expanding surveillance across entire platforms? How will platforms adjust their design incentives in response to legal risk? How will young users adapt, route around, or resist imposed constraints? And how unevenly will these effects fall across different social and economic groups?

Framed this way, the debate isn't really about whether children should be online. It's about the conditions under which they encounter digital spaces, how they exercise agency within them, and how they learn to navigate participation over time. Maybe the question isn't **"Should kids be online?"** but **"How should they learn to be?"** and whether that's something a law can answer, or whether it requires something more adaptive, more responsive, and ultimately more human.

Endnotes

1. Snap Inc. (2025, November 22). *Implementing Australia's social media minimum age law*. <https://newsroom.snap.com/australia-social-media-minimum-age-law>
2. Kaur, D. (2025, March 18). *Australia's social media use: Kids bypass existing restrictions*. TechHQ. <https://techhq.com/news/australias-social-media-use-kids-bypass-existing-restrictions/>
3. *Social Media Age Restriction and Young People (eSafety brief)* – cites eSafety https://bravehearts.org.au/wp-content/uploads/2025/11/Social-Media-Age-Restriction-and-Young-People_Briefing-Paper.pdf
4. Kaur, supra note 2.
5. Kaur, supra note 2.
6. ABC News. (2025, September 15). *Social media platforms will not be required to prove accuracy of under-16 bans*. <https://www.abc.net.au/news/2025-09-15/social-media-ban-final-rules-announced/105776730>
7. Reuters. (2025, December 10). *Australia begins enforcing world-first teen social media ban*. <https://www.reuters.com/legal/litigation/australia-social-media-ban-takes-effect-world-first-2025-12-09/>
8. Australia. (2024). *Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth)*. https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/num_act/osammaa2024409/
9. Reuters. (2025, December 9). *Australia social media ban set to take effect, sparking global crackdown*. <https://www.reuters.com/business/media-telecom/australia-social-media-ban-set-take-effect-sparking-global-crackdown-2025-12-09/>
10. Kohlion, C. (2025, December 8). *How will platforms monitor VPN usage when under-16 social media ban begins in Australia?* MediaNama. <https://www.medianama.com/2025/12/223-vpn-detection-australia-esafety-guidelines-under-16-social-media-ban/>
11. eSafety Commissioner. (2025). *Social media age restrictions*. <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>
12. Office of the Australian Information Commissioner. (2025, October 23). *Social Media Minimum Age*. <https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-minimum-age>
13. Office of the Australian Information Commissioner. (2025, June 19). *Statutory tort for serious invasions of privacy*. <https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/statutory-tort-for-serious-invasions-of-privacy>
14. Reuters. (2025, December 11). *Reddit sues Australia over social media ban, citing free speech threat*. <https://www.reuters.com/legal/litigation/reddit-files-lawsuit-against-australias-social-media-ban-2025-12-11/>
15. Amnesty International Australia. (2024, November 29). *Social media ban: what it is and what it will mean for young people*. <https://www.amnesty.org.au/social-media-ban-explained/>
16. Science Media Centre. (2025, December 8). *Australia's teen social media ban takes effect: Expert reaction*. Science Media Centre New Zealand. <https://www.sciencemediacentre.co.nz/2025/12/08/australias-teen-social-media-ban-takes-effect-expert-reaction/>
17. Perez, S. (2025, March 10). *The Bark Phone lets you prioritize your children's safety and right now you can save 30% on it*. CNET. <https://www.cnet.com/deals/the-bark-phone-lets-you-prioritize-your-childrens-safety-and-right-now-you-can-save-30-on-it/>

18. The Australian. (2025, December). *Social media has reduced Australian children's reading, participation in art*. https://www.theaustralian.com.au/subscribe/news/1/?sourceCode=TAWEB_WRE170_a&dest=https%3A%2F%2Fwww.theaustralian.com.au%2Fbusiness%2Ftechnology%2Fsocial-media-has-wiped-out-creative-pursuits-for-a-generation-new-research-reveals%2Fnews-story%2F760165231963b9095335ef723813d175&memtype=anonymous&mode=premium&v21=GROUPB-Segment-2-NOSCORE&V21spcbehaviour=append

19. Rosenkrantz, A. B., Prabhu, V., & Giorgianni, A. (2021). *Social media and adolescent health: A multidisciplinary overview of benefits, risks, and recommendations*. *Journal of Adolescent Health, 68*(2), 186–197. <https://pmc.ncbi.nlm.nih.gov/articles/PMC8093609/>

20. Cyprus Mail. (2025, December 11). *Australia's social media youth ban draws US applause, UN warning, and global debate*. <https://cyprus-mail.com/2025/12/11/australias-social-media-youth-ban-draws-us-applause-un-warning-and-global-debate>



The Indian Governance And Policy Project (IGAP) is an emerging think tank focused on driving growth, innovation, and development in India's digital landscape. Specializing in areas like AI, Data Protection, FinTech, and Sustainability, IGAP promotes evidence-based policymaking through interdisciplinary research. By working closely with industry bodies in the digital sector, IGAP provides valuable insights and supports informed decision-making. Core work streams include policy monitoring, knowledge dissemination, capacity development, dialogue and collaboration.

For more details visit: www.igap.in

relations@igap.in | igap.in