



A Comparative Study of Social Media and Data Privacy of Minor in India and Australia

Dhanashree Vijaykumar Jadhavar^{1*}, Dr.Bhavna T Kadu²

^{1*} Institution Name School Of Law Mit-Adt University Loni Kalbhor Pune. dhanashree.jadhvar85@gmail.com

² Assistant Professor Mit -Adt University Loni Kalbhor Pune

Abstract

Social media has become an important space for education, expression, friendship and entertainment, yet its business model frequently depends upon the continuous collection and analysis of user data. Children are especially vulnerable because they may disclose personal information without understanding how long it will remain available, how it may be combined with other data, or how recommendation and advertising systems influence their choices. This paper comparatively examines the protection of minors' personal data on social media in India and Australia. It adopts a doctrinal and comparative method and studies the Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 in India, together with Australia's Privacy Act 1988, Online Safety Act 2021, Social Media Minimum Age scheme and proposed Children's Online Privacy Code. The study finds that India has chosen a broad, parental-consent model covering every person below eighteen, coupled with prohibitions on detrimental processing, behavioural monitoring and targeted advertising. However, the principal child-data obligations are subject to phased commencement and are not yet operative as at the date of this paper. Australia presently combines general privacy principles with an operational platform duty to prevent under-sixteen users from holding accounts on age-restricted social media platforms. Its model gives particular attention to privacy-preserving age assurance and is moving towards a detailed, child-centred online privacy code. The paper argues that neither access restriction nor parental consent alone is sufficient. Effective protection requires data minimisation, child-friendly transparency, limits on profiling, independent supervision, accessible remedies and meaningful recognition of the evolving capacities of adolescents.

Keywords: Social media, data privacy, minors, children, India, Australia, parental consent, age assurance.

1. Introduction

A child's social media profile may contain a name, photograph, school, location, contacts, interests and private conversations. Platforms can also generate less visible information, including device identifiers, browsing patterns, inferred preferences, engagement scores and estimates of emotional state. The resulting digital record can expose minors to targeted advertising, manipulation, identity theft, cyberbullying and unwanted contact. Even where a child voluntarily posts information, genuine consent is difficult when privacy notices are lengthy and the future use of data is uncertain (Office of the Australian Information Commissioner [OAIC], 2026).

Social media performs a dual role in the lives of minors because it offers valuable opportunities while also creating continuous exposure to commercial data collection. It allows children to communicate with friends, access educational material, express opinions and participate in public culture. At the same time, ordinary actions such as liking a post, watching a video or sharing a location can become inputs for detailed personal profiles. These profiles may influence the advertisements, recommendations and persuasive messages shown to a young user. The concern is not limited to information intentionally disclosed by a child because platforms can infer interests, habits and relationships from patterns of activity. Young users may also find it difficult to distinguish between content selected for their benefit and content promoted to increase engagement or commercial returns. Parents can provide valuable guidance, but they may not fully understand the technical systems through which a platform collects and combines data. Privacy protection must consequently be built into the service instead of depending entirely upon a child or parent navigating complicated settings. The international operation of major platforms further demonstrates why national laws must create clear responsibilities for companies offering services across borders. A comparative examination can reveal which safeguards are immediately effective and which require stronger implementation, oversight or recognition of children's developing autonomy (Government of India, 2023; OAIC, 2025).

The legal problem is therefore broader than deciding the age at which a child may open an account. It concerns what information a platform may collect, whether profiling is permissible, who can consent, how age can be verified without creating another sensitive database, and what remedies exist when harm occurs. India and Australia offer a useful comparison because both treat people below eighteen as children in important parts of their privacy frameworks, but their immediate regulatory strategies differ considerably (Government of India, 2023; Australian Government, 1988).

2. Objectives and Research Methodology

The objectives of this paper are to examine the laws governing minors' personal data on social media in India and Australia, identify similarities and differences in consent, profiling, age assurance and enforcement, and suggest measures for stronger child-centred protection. The study is doctrinal and comparative. It relies on legislation, statutory rules, official notifications and guidance issued by Indian and Australian regulators. The comparison is

functional: it considers how each system responds to the same risks rather than merely placing statutory provisions side by side. The legal position is assessed as at 21 July 2026.

3. Social Media and the Privacy Risks Faced by Minors

❖ Social media data is persistent, replicable and capable of being analysed at scale. A minor may delete a post but copies, screenshots or inferred profiles can remain. Publicly visible information may reveal daily routines, family relationships and location. Privately collected engagement data can be used to recommend content that maximises attention, even when prolonged use is not in the child's best interests (OAIC, 2026).

❖ Three concerns deserve particular attention. First, children may not have the maturity or bargaining power required for informed consent. Second, behavioural advertising converts ordinary childhood activity into a commercial profile. Third, age-verification measures may themselves demand identity documents, facial analysis or location data. A protective law must therefore reduce exposure to harmful data practices while ensuring that the method used to identify children does not create a new privacy risk (OAIC, 2025).

4. Legal Framework in India

❖ The constitutional foundation of informational privacy in India lies in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), where the Supreme Court recognised privacy as a fundamental right under the Constitution. The Digital Personal Data Protection Act, 2023

(DPDP Act) now provides the principal statutory framework for digital personal data. It applies to digital data processed in India and, in specified circumstances, to processing outside India connected with offering goods or services to persons in India (Government of India, 2023).

❖ Section 2(f) defines a child as an individual who has not completed eighteen years. Section 9 requires a Data Fiduciary to obtain verifiable parental consent before processing a child's personal data. It also prohibits processing likely to have a detrimental effect on a child's well-being and prohibits tracking, behavioural monitoring and targeted advertising directed at children. These are significant protections for social media because they address both entry into the service and the commercial practices that continue after registration. Breach of the obligations relating to children may attract a monetary penalty of up to ₹200 crore under the Schedule to the Act (Government of India, 2023).

❖ The Digital Personal Data Protection Rules, 2025 explain how parental status may be verified. Rule 10 requires appropriate technical and organisational measures and due diligence to establish that the person claiming to be a parent is an identifiable adult. Verification may rely on reliable details already held by the Data Fiduciary, voluntarily supplied identity and age details, or a virtual token issued by an authorised entity, including verification through a Digital Locker service provider. The Rules also provide limited, purpose-based exemptions for areas such as health, education, safety and specified public functions (Ministry of Electronics and Information Technology [MeitY], 2025).

❖ The framework contains a degree of flexibility. Under section 9(5), the Central Government may exempt processing above a notified age where a Data Fiduciary demonstrates that its processing is verifiably safe. This may eventually allow a more proportionate approach for older adolescents. At present, however, the default statutory line remains eighteen (Government of India, 2023).

❖ A timing qualification is essential. The commencement notification brought institutional and rule-making provisions into force on 13 November 2025, but sections 3 to 17, including section 9, are scheduled to commence eighteen months from that date. Consequently, the substantive child-data obligations described above form the enacted Indian framework but are not yet operative on 21 July 2026. During this transition, platform practices remain affected by existing information-technology law, contractual terms, sectoral rules and constitutional principles, but the specialised DPDP child protections have not reached full enforcement (Government of India, 2025).

5. Legal Framework in Australia

Australia's Privacy Act 1988 regulates the handling of personal information by Australian Government agencies and covered private organisations through the Australian Privacy Principles

(APPs). The APPs address transparency, collection, use and disclosure, direct marketing, crossborder disclosure, security, access and correction. They protect personal information regardless of the individual's age. The Act does not establish a universal age at which a child can make an independent privacy decision. Official guidance states that capacity should ordinarily be assessed case by case, with maturity and understanding being central. Where individual assessment is impractical, an organisation may generally presume that a person over fifteen has capacity unless there is reason for doubt (Australian Government, 1988; OAIC, 2022).

Australia has added a platform-specific layer through Part 4A of the Online Safety Act 2021, inserted by the Online Safety Amendment (Social Media Minimum Age) Act 2024. From 10 December 2025, providers of age-restricted social media platforms must take reasonable steps to prevent Australians under sixteen from creating or retaining accounts. The responsibility falls on platforms, not on children or parents. As at July 2026, eSafety identifies services including Facebook, Instagram, Reddit, Snapchat, TikTok, Twitch, X and YouTube as covered, while various messaging, gaming and educational services are outside the current scheme. A corporation that fails to take reasonable steps may face a civil penalty of up to 150,000 penalty units, currently stated by eSafety as A\$54.6 million (Australian Government, 2024; eSafety Commissioner, 2026).

Age assurance creates an obvious privacy tension. Section 63DB prevents a platform from requiring government-issued identification or an accredited Digital ID service as the only method; a reasonable alternative must be available. Section 63F restricts secondary use and disclosure of information collected for age assurance. It also requires that information to be destroyed after it has served the purpose for which it was collected. Non-compliance is treated as an interference with privacy under the Privacy Act. The Office of the Australian Information Commissioner (OAIC) and eSafety therefore share complementary roles: eSafety supervises the reasonable-steps obligation, while the OAIC oversees privacy compliance (Australian Government, 2021; OAIC, 2025).

Australia is also developing a Children's Online Privacy Code under section 26GC of the Privacy Act. The OAIC released an Exposure Draft on 31 March 2026, with the final Code required to be registered by 10 December 2026. Because it remains a draft, its provisions should not be presented as current law. Nevertheless, it shows the future direction of regulation: privacy by default, strict necessity, the best interests of the child, age-appropriate notices, controls over direct marketing, accessible complaint mechanisms and privacy impact assessments. The draft permits children aged fifteen or above to consent, generally requires parental consent below fifteen, and preserves limited circumstances in which a younger child may independently seek legal or health-related support (OAIC, 2026).

6. Comparative Analysis

India's model is broader in age but narrower in its immediate technique. It places every person below eighteen within a parental-consent framework and directly prohibits tracking, behavioural monitoring and targeted advertising. Australia currently uses a more differentiated structure. General privacy capacity depends on maturity, the social media account restriction operates below sixteen, and the proposed Code would recognise independent consent from age fifteen in covered settings (Government of India, 2023; OAIC, 2026).

The two jurisdictions also differ in regulatory status. Australia's social media minimum-age obligation is already operational and backed by a specialised regulator with public guidance.

India's DPDP system has created a strong statutory standard, but its principal duties are still within the phased commencement period. India may therefore appear stricter on paper while Australia presently has the more immediate platform-access enforcement mechanism (eSafety Commissioner, 2026; Government of India, 2025).

- Australia pays unusually close attention to the privacy of age assurance itself by limiting reliance on government identification, restricting secondary use and requiring destruction. India's Rules provide several verification routes, including tokens and Digital Lockersupported verification, but the broader implementation challenge remains ensuring that parents and children are not forced to disclose excessive identity information merely to establish age (MeitY, 2025; OAIC, 2025).

- India's express ban on behavioural monitoring and child-directed targeted advertising is a major substantive strength. Australia's APPs regulate collection, use and direct marketing, while the draft Code would add child-specific safeguards and a best-interests test. Until that Code is registered, however, Australia does not mirror India's simple statutory prohibition across the same under-eighteen class (Government of India, 2023; Australian Government, 1988; OAIC, 2026).

Table 1. Comparative Framework for Children's Digital Privacy

Feature	India	Australia
Primary Legislation	Digital Personal Data Protection (DPDP) Act, 2023	Privacy Act 1988, Online Safety Act, Social Media Minimum Age framework
Definition of Child	Below 18 years	Varies by law; social media restriction generally below 16 years
Consent Requirement	Mandatory parental consent for all children under 18	Capacity-based approach; independent consent generally recognized around age 15 in proposed Children's Online Privacy Code
Regulatory Authority	Data Protection Board of India (phased implementation)	Office of the Australian Information Commissioner (OAIC) and eSafety Commissioner
Current Enforcement	DPDP implementation is being phased	Social media minimum-age obligation is operational

Table 2. Comparison of Key Privacy Protections

Privacy Measure	India	Australia
Parental Consent	Mandatory for all under 18	Depends on maturity and applicable law
Behavioural Monitoring	Expressly prohibited	Regulated but not completely prohibited
Targeted Advertising	Prohibited for children	Restricted through privacy principles and proposed Code
Child Profiling	Restricted	Limited through Privacy Act and proposed Code
Best Interests Principle	Not expressly stated	Proposed Children's Online Privacy Code introduces bestinterests requirement
Data Security	Mandatory safeguards	Mandatory under Australian Privacy Principles

Table 3. Age Assurance and Identity Verification

Aspect	India	Australia
Verification Methods	Digital Locker, tokens, government-approved methods	Privacy-preserving age assurance methods
Government ID	May be used where applicable	Discouraged unless necessary
Secondary Use of Identity Data	Rules aim to minimise unnecessary disclosure	Strict limitation on secondary use
Data Retention	Subject to DPDP obligations	Age verification data should be destroyed after use
Country	Major Strengths	Key Challenges
India	Strong statutory prohibition on behavioural monitoring and targeted advertising; broad child protection	Mandatory parental consent until 18 may reduce adolescent autonomy and encourage false age declarations
Australia	Operational social media age restriction; privacy-preserving	Protection mainly applies to covered platforms; excluded
	ageAssurance; regulatory guidance	strong services and public content remain outside full protection

Table 4. Strengths and Challenges

Country	Major Strengths	Key Challenges
India	Strong statutory prohibition on behavioural monitoring and targeted advertising; broad child protection	Mandatory parental consent until 18 may reduce adolescent autonomy and encourage false age declarations
Australia	Operational social media age restriction; privacy- preserving age assurance; strong regulatory guidance	Protection mainly applies to covered platforms; excluded services and public content remain outside full protection

Table 5. Overall Comparative Analysis

Comparison Area	India	Australia
Age Threshold	Under 18	Under 16 for social media; maturity-based privacy framework

Regulatory Status	Strong legislation with phased implementation	Operational enforcement mechanisms
Platform Responsibility	High	High
Child Privacy Protection	Very strong statutory protections	Strong regulatory protections with proposed child-specific Code
Adolescent Autonomy	Limited due to universal parental consent	Greater recognition of mature minors
Identity Privacy During Age Verification	Verification through multiple approved methods	Strong emphasis on privacy Preserving verification

Both systems recognise platform responsibility, consent, security and regulatory remedies. Yet neither model is complete by itself. Australia's access restriction can reduce exposure on covered platforms, but it does not protect children on excluded services or public content viewed without an account. India's parental-consent model may protect younger children, but treating a seventeen-year-old exactly like a very young child can reduce autonomy and encourage false age declarations or parental-consent formalities that do little to change platform design.

7. Challenges and Recommendations

➤ The central challenge is to avoid equating consent with safety. Parents may approve a service without understanding profiling, recommender systems or data sharing. Platforms should therefore be required to minimise data, disable profiling and location sharing by default, and explain privacy choices in language suited to the child's age. Consent should supplement these duties, not replace them (OAIC, 2026).

➤ India should use the transition period to publish detailed, privacy-preserving standards for age assurance, independent audits and child-friendly notices. It should clarify how the section

9(5) safe-processing exemption will be assessed and consider graduated autonomy for older adolescents. The Data Protection Board should have expertise in child rights and technology, and complaint channels should be accessible to children without unnecessary procedural barriers.

➤ Australia should ensure that the final Children's Online Privacy Code retains the draft's best-interests standard, strict-necessity principle and limits on manipulative consent. The social media minimum-age scheme should be independently evaluated for accuracy, exclusion, circumvention and the quantity of data collected during age checks. Children wrongly classified as under sixteen need simple and timely review procedures.

➤ Both countries should require impact assessments for high-risk recommendation and advertising systems, meaningful deletion rights, rapid breach notification and transparent reports on children's data practices. Regulators should cooperate across borders because the major platforms operate globally. Most importantly, children should participate in the design and evaluation of rules that directly shape their digital lives.

8. Conclusion

India and Australia share the objective of protecting minors from data exploitation, but they have chosen different routes. India has enacted a high-threshold model based on parental consent up to eighteen and direct restrictions on harmful processing and advertising, although its central obligations are not yet operative as at July 2026. Australia combines general privacy principles with an enforceable under-sixteen account restriction and specific privacy safeguards for age assurance, while a more comprehensive Children's Online Privacy Code is still being finalised. The comparison shows that effective protection cannot rest on one age threshold. A sound framework must combine restricted data collection, privacy-protective design, age-appropriate transparency, proportionate recognition of evolving capacity and strong enforcement. The best measure of success is not how many consent boxes are clicked or accounts removed, but whether minors can participate in the digital environment without surrendering their dignity, autonomy and future privacy.

References

1. Australian Government. (1988). Privacy Act 1988 (Cth). Federal Register of Legislation.
2. Australian Government. (2021). Online Safety Act 2021 (Cth). Federal Register of Legislation.
3. Australian Government. (2024). Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth). Federal Register of Legislation.
4. eSafety Commissioner. (2026). Social media 'ban' or delay FAQ.
5. Government of India. (2023). Digital Personal Data Protection Act, 2023. India Code.
6. Government of India. (2025). Enforcement Timeline for the Digital Personal Data Protection Act, 2023, Notification G.S.R. 843(E). India Code.
7. Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025.
8. Office of the Australian Information Commissioner. (2025). Privacy guidance on Part 4A (Social Media Minimum Age) of the Online Safety Act 2021.

9. Office of the Australian Information Commissioner. (2022). Children and young people.
10. Office of the Australian Information Commissioner. (2026). Exposure Draft: Privacy (Children's Online Privacy) Code 2026.
11. Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
12. Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. *London School of Economics Media Policy Brief*, 28, 1–24.
13. Livingstone, S., Third, A., & Stoilova, M. (2023). The evolving capacities of children in the digital environment. *New Media & Society*, 25(8), 1845–1862.
14. Mascheroni, G., & Cuman, A. (2014). Net Children Go Mobile: Final report. *Educatt Electronic Publishing Journal*, 1(1), 1–132.
15. Stoilova, M., Livingstone, S., & Nandagiri, R. (2021). Digital by default: Children's capacity to understand online privacy and consent. *Information, Communication & Society*, 24(14), 2158–2175.
16. Montgomery, K. C., & Chester, J. (2015). Data protection for youth in the digital age. *Journal of Children and Media*, 9(2), 165–172.
17. Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, 140(4), 32–48.
18. Zuboff, S. (2019). Surveillance capitalism and the challenge of democratic governance. *Journal of Information Technology*, 34(4), 377–384.
19. Van der Hof, S. (2016). I agree, or do I? A rights-based analysis of children's consent in digital environments. *Wisconsin International Law Journal*, 34(2), 409–445.
20. Koops, B. J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. *International Review of Law, Computers & Technology*, 28(2), 159–171.
21. Edwards, L. (2018). Protecting children's privacy in the age of big data. *Communications Law*, 23(2), 45–56.
22. Leiser, M. R. (2020). Children's privacy online and the General Data Protection Regulation. *Computer Law & Security Review*, 36, 105368.
23. Bietti, E. (2020). Consent as a mechanism for protecting privacy: A critical assessment. *Harvard Journal of Law & Technology Digest*, 33, 1–17.
24. Richards, N. M., & Hartzog, W. (2018). Privacy's trust gap. *Yale Law Journal Forum*, 126, 118–128.
25. Wisniewski, P., Jia, H., Xu, H., Rosson, M. B., & Carroll, J. M. (2015). Preventive versus reactive: How parental mediation influences youth online privacy behaviors. *Proceedings of the ACM Conference on Computer Supported Cooperative Work*, 302–316.
26. Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051–1067.
27. Kumar, P., & Prasad, A. (2024). Child data protection under India's Digital Personal Data Protection Act, 2023: Emerging challenges and opportunities. *Indian Journal of Law and Technology*, 20(1), 45–68.
28. Sharma, R., & Singh, V. (2025). Parental consent and child privacy in India's digital ecosystem. *Journal of Indian Law and Society*, 16(2), 89–114.
29. Greenleaf, G. (2022). Data privacy reforms in Australia: Implications for children and young people. *Privacy Laws & Business International Report*, 177, 12–17.
30. Goggin, G., & Ellis, K. (2021). Digital inclusion, children and online safety in Australia. *Media International Australia*, 178(1), 86–99.
31. Carlson, B., Frazer, R., & Jones, L. (2020). Indigenous young people and digital privacy in Australia. *Information, Communication & Society*, 23(11), 1597–1613.
32. Thomas, J., Barraket, J., Wilson, C., Cook, K., Louie, Y., Holcombe-James, I., & Ewing, S. (2023). Children's online participation, privacy and digital rights. *Australian Journal of Social Issues*, 58(3), 511–529.
33. Lievens, E., & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights online. *Computer Law & Security Review*, 34(2), 269–278.
34. Kloza, D., & Van Dijk, N. (2021). Age verification and privacy in digital services: Balancing protection and rights. *International Data Privacy Law*, 11(4), 325–339.
35. Fiesler, C., Lampe, C., & Bruckman, A. (2016). Reality and perception of copyright terms of service among social media users. *Proceedings of the ACM Conference on Human Factors in Computing Systems*, 1985–1996.
36. Milkaite, I., & Lievens, E. (2019). Child-friendly transparency and data protection in online services. *International Data Privacy Law*, 9(3), 164–189.
37. Stoilova, M., Livingstone, S., & Nandagiri, R. (2023). Children's rights and privacy in digital environments: Regulatory responses and future directions. *International Journal of Child Rights*, 31(2), 255–279.
38. Krivokapić, D., Adamović, M., & Seitz, C. (2022). Best interests of the child and personal data protection. *Computer Law & Security Review*, 45, 105661.
39. ++++++Taylor, E., & Rooney, T. (2024). Regulating social media platforms for child safety and privacy: Comparative perspectives. *Internet Policy Review*, 13(1), 1–24.