Age Verification on Social Media: Implications for Privacy and Data Security

28 JULY 2026

Tommaso Colonetti and Chamaidi Provatou



Photo by Julian on Unsplash

The political rationale underpinning age verification

Digital environments have become a constitutive and structural element of contemporary childhood, exposing them to risks such as sexualised content, cyberbullying, and algorithmic systems designed to maximise attention and emotional engagement. This understanding has provided the principal justification for policymakers' intervention, driving the adoption of age-based restrictions and prompting legislative efforts to rely increasingly on minimum-age thresholds as primary regulatory responses (Köhler-Dauner et al., 2025). However, this approach presents significant limitations. Early evidence from Australia suggests that age-based restrictions have so far produced only modest changes in platform use (eSafety

Commissioner, 2026). Moreover, despite the entry into force of the Online Safety Amendment (Social Media Minimum Age) Act, reports indicate that approximately 40 per cent of Australian adolescents attempted to circumvent age-based restrictions through measures such as VPNs and using alternative platforms (Köhler-Dauner et al., 2025, pp. 6-7).

Furthermore, the empirical basis underpinning blanket bans remains contested. As Champion et al. (2025) suggest, Australia's social media ban emerged less from a settled scientific consensus than from growing parental frustration with the challenges posed by adolescents' online lives. While concerns regarding the relationship between social media use and youth mental health are legitimate, existing research has been unable to establish a clear causal relationship between platform use and psychological harm. Although acknowledging the need to address online risks, the latter argue that prohibition alone is unlikely to provide a comprehensive and long-lasting solution. Moreover, blanket bans risk reinforcing existing social inequalities (Champion et al., 2025). For psychosocially vulnerable children, social media is often more than a leisure activity; it serves as a critical source of social support (Stott et al., 2016). Restricting access may therefore push these users toward less regulated digital environments while depriving them of valuable networks and resources (Champion et al., 2025). These shortcomings raise a broader question: can children be effectively protected online without resorting to measures that are both easily bypassed and potentially exclusionary?

Nevertheless, the limitations of blanket bans should not be interpreted as undermining the fundamental responsibility of states to protect children in digital environments. As emphasised by the United Nations Committee on the Rights of the Child (2021) in General Comment No. 25, such an environment – although not originally designed for children – has become vital to their present lives and future development, creating a positive obligation for states to ensure that their rights are protected online. This extends beyond voluntary platform initiatives and requires governments to establish regulatory frameworks that address commercial exploitation, data-driven harms, and unsafe digital design. However, the Committee stresses that such mechanisms must comply with data protection and privacy requirements, preventing child protection objectives from being used as a justification for disproportionate surveillance or unlawful processing of personal data.

The central challenge, therefore, is not whether states should regulate children's access to digital spaces, but how to reconcile safety, privacy, and online participation. General Comment No. 25 marks a departure from purely protectionist approaches towards a more comprehensive understanding of children's rights in online environments, recognising protection, privacy, access to information, and participation as interdependent (Sylwander & Livingstone, 2025). From this perspective, age assurance is only one element of a broader regulatory architecture in which the

child's best interest must be operationalised through rights-based digital governance, rather than being reduced to a purely technical verification mechanism.

This approach is further developed by the European Data Protection Board (EDPB, 2025), which outlines the principles that should govern the design and deployment of age assurance. Rather than treating age assurance as an objective in itself, the Board frames it as a risk-based and proportionate mechanism. Such a measure should rely on the least intrusive means available to determine whether a user meets a given age threshold, while ensuring that the processing of personal data is limited to what is strictly necessary. It also emphasises that information collected for age verification processes must not be repurposed for profiling, tracking, or other unrelated purposes, reinforcing the principle that child protection should not become a gateway to disproportionate surveillance.

These debates also extend beyond the technical design of age verification systems and into questions of European digital governance. The European Commission has increasingly framed age verification as a matter of Union-wide digital governance, seeking to harmonise national approaches while preventing fragmented regulatory responses, such as unilateral social media bans. Accordingly, the regulation of children's access to digital platforms has become intertwined with broader objectives of the Digital Single Market, revealing that child protection and privacy are no longer discrete policy concerns but rather central components of the European Union's digital governance agenda (Marcu & Hales, 2026).

Taken together, these considerations demonstrate that the political rationale for age assurance cannot be separated from the implications of its technical and legal implementation, nor from the broader question of how Member States wish to shape the European service market. If states have a positive obligation to protect children online, the means through which this obligation is operationalised become equally important: the central policy dilemma therefore shifts from whether age assurance is desirable in principle to how it can be implemented without jeopardising the safeguard of privacy, children's participation rights, and the digital sovereignty of the European Union.

Age verification implications for privacy and data security

Once age verification moves to operational practice, it faces rigorous scrutiny under the EDPB's (2025) proportionality and necessity standards. Regardless of the technological method deployed, any such system immediately stumbles upon an inherent paradox: to successfully isolate and protect a minority of underage users, it must systematically screen the entire user population, minors and adults alike (Goldman, 2025). Such screening raises a substantial data-minimisation challenge, since any processing must remain limited to what is necessary and proportionate to

establish the relevant age threshold. Yet, this obstacle is only the starting point. Platforms have proposed a range of age-assurance methods, each of which entails considerable costs to user privacy and data security. Concerns were recently validated when France's Constitutional Council struck down mandatory social media age restrictions for under-15s, ruling that, without clear technical safeguards, the latter violates the right to privacy and is not proportionate to freedom of expression and communication of minors (Le Monde & Agence France-Presse, 2026).

The most established verification method is document-based and involves uploading a scan, photo, or video of a formal identity document such as a passport, driver's license, or national ID (European Digital Rights [EDRi], 2023). While it may seem suitable, legal documentation is not meant for online verification as it forces the user to share an excessive amount of highly sensitive, secondary personal information, including their full name, exact date of birth, photo, and home address, thus going against the principle of data minimisation (Livingstone et al., 2024). Notably, the French data protection authority has ruled that the systematic collection of official identity documents for age verification violates data protection rules due to the serious risks of identity theft, misappropriation, and disclosure (Humain-Lescop, 2025). This method would also exclude marginalised groups like asylum seekers or undocumented children who could find themselves completely shut out of the internet (EDRi, 2023). Additionally, Goldman (2025) stresses how storing a centralised database of thousands of passports, credit cards and driver's licences creates an incredibly high-value target, a 'honeypot', for cybercriminals and poses a major information security threat to both minors and adults. Numerous cases have been registered; following a security breach, AU10TIX, used by major platforms like TikTok and X, exposed the actual uploaded government IDs and driver's licences of users. Outabox, used for mandatory ID checks in Australian clubs, leaked over 1 million customer records after a cyber-attack (Goldman, 2025, p. 205). Moreover, the latter argues this method triggers a direct clash between the privacy requirement to delete data after confirmation and platforms' incentive to keep the records out of fear of massive regulatory fines. Finally, due to a lack of resources, platforms outsource verification processes to third-party vendors, such as Yoti or Jumio, that have access to many different websites. As a result, private, profit-driven entities can track users' navigation histories, violating purpose limitation boundaries (Woodley et al., 2025).

An alternative method proposed is based on age estimation techniques. An example of these is biometric facial analysis, which relies on Artificial Intelligence and machine learning models to determine a user's age based on facial features or other physical attributes in a photo or video recording (Humain-Lescop, 2025). Routine collection and processing of this kind of sensitive biometric data, especially from children, could conflict with the provisions of Article 9 of the GDPR, as this technology can be unequivo-

cally used to identify a natural person (Díaz Díaz, 2016). Moreover, under Art. 8 of the GDPR, processing a child's personal data based on consent is lawful only if the child has reached the age of 16, although Member States may lower this threshold to 13; alternatively, it must be authorised by a parent (Humain-Lescop, 2025). However, platforms cannot determine whether the user has reached this age threshold without first scanning their facial features. Thus, they cannot legally rely on user consent to estimate their age in the first place (Shaffique & van der Hof, 2026). Regardless, it's highly questionable whether children's consent would have been informed or freely given, given their lack of awareness of the potential privacy risks and the major role digital networks play in youth social participation today (EDRi, 2023).

The final technique abandons the single verification moment entirely; instead, behavioural (or digital profiling) uses AI and machine learning to predict a user's age from the quiet accumulation of their everyday online activity. Shaffique and van der Hof (2026) offer a few examples of such prediction: engaging patterns like content liked, shared, or viewed; browsing and purchase history, social connections, public posts, and private messages (i.e., platforms could scan online interactions as simple as wishing someone happy birthday); and behavioural biometrics, including typing speed and users' activity logs. The same authors reveal that major technology platforms such as Meta, Google, and TikTok are already deploying this technique for age assurance. While digital profiling doesn't require screening 'walls' or legal documentation to allow access, it still raises several privacy concerns. Examples include mass data harvesting and data mining of both children and adults, which involve scanning private chat histories and tracking personal interactions (Goldman, 2025). Additionally, given platforms' interest in commercial profiling, these methods seem ill-suited to consistently comply with Art. 28b(3) of the Audiovisual Media Services Directive and with Art. 28 of the Digital Services Act, as it risks legitimising surveillance under the pretext of child safety (Shaffique & van der Hof, 2026).

Policy recommendations: from verification to empowerment

First, age assurance should be subject to a strict necessity and proportionality test. Consistent with the EDPB (2025), verification should only be required when a specific risk is recognised and where less intrusive measures cannot achieve the same objective. If age assurance is necessary, policymakers should favour privacy-preserving technologies, including localised processing and zero-knowledge proofs, which can establish whether a user satisfies an age threshold without unnecessarily disclosing their identity or other personal information.

Second, regulation should prioritise privacy and safety by design rather than relying primarily on exclusion. Platforms should be required to pre-

emptively assess the impact of their services on children; in this regard, the enforcement of existing frameworks such as the GDPR and the Digital Services Act may rely less on introducing increasingly intrusive verification requirements (EDRi, 2023; Jakubowska, 2024).

Finally, protection should be accompanied by empowerment. In line with the principle of children's evolving capacities, policies should support age-appropriate participation rather than treating access to digital environments as either permitted or prohibited (Sylwander & Livingstone, 2025). This should include digital media education and the meaningful involvement of adolescents in the design of online safety measures (Champion et al., 2025). In this sense, effective child protection should be measured not only by how successfully children can be excluded from risky digital environments, but also by whether those environments can be tailored to their safety and needs.

References

Champion, K. E., Birrell, L., Smout, S., Teesson, M., & Slade, T. (2025). Debate: Social media in children and young people–time for a ban? Beyond the ban–empowering parents and schools to keep adolescents safe on social media. *Child and adolescent mental health*, *30*(4), 411-413.

Díaz Díaz, E. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions. *Church, Communication and Culture*, *1*(1), 206-239.

eSafety Commissioner. (2026, July 30). *Early insights from eSafety's comprehensive evaluation project*. eSafety Commissioner. https://www.esafety.gov.au/newsroom/media-releases/early-insights-from-esafetys-comprehensive-evaluation-project

European Commission. (2026). Commission Recommendation (EU) 2026/1035 of 29 April 2026 on establishing a common framework for EU wide Age Verification technologies. *Official Journal*, L 1035, ELI: http://data.europa.eu/eli/reco/2026/1035/oj

European Data Protection Board. (2025, February 11). *Statement 1/2025 on age assurance*. European Union. https://www.edpb.europa.eu/documents/statement/statement-12025-on-age-assurance_en

European Digital Rights. (2023, October). *Online age verification and children's rights* [White paper]. https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf

Goldman, E. (2025). The" Segregate-and-Suppress" Approach to Regulating Child Safety Online. *Stan. Tech. L. Rev.*, *28*, i.

Humain-Lescop, A. (2025). *Towards harmonised online age verification ? A comparative study of French and EU legal frameworks*. Digital, Governance and Sovereignty Chair at Sciences Po.

Jakubowska, E. (2024). Exploring Europe's Digital Future: What Does a Safe and Private Internet Look Like?. *Opportunities for All*, 53.

Köhler-Dauner, F., Peter, L., Sitarski, E., Chauviré-Geib, K., Haag, A. C., & Fegert, J. M. (2025). Digital child protection in social networks: age verification and age-tiered regulation in Europe. *Child and adolescent psychiatry and mental health*, *19*(1), 143.

Le Monde, & Agence France-Presse. (2026, August 14). *France's Constitutional Council strikes down social media ban for under-15s*. Le Monde. https://www.lemonde.fr/en/pixels/article/2026/08/14/france-s-constitutional-council-strikes-down-ban-on-social-media-for-under-15s_6756507_13.html?srsltid=AU7gw4X3cBJoca3oJQGRWS1aedbIAuk7jD_j2TMgWmRBozu6DK9xU_L2

Livingstone, S., Nair, A., Stoilova, M., Van Der Hof, S., & Caglar, C. (2024). Children's rights and online age assurance systems: The way forward. *The International Journal of Children's Rights*, *32*(3), 721-747.

Marcu, B.-I., & Hales, D. (2026, May 12). *The EU Commission's Approach to Age Verification: Mobile Apps, DSA Enforcement, and Challenging National Social Media Bans*. Future of Privacy Forum. https://fpf.org/blog/the-eu-commissions-approach-to-age-verification-mobile-apps-dsa-enforcement-and-challenging-national-social-media-bans/

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (2016). Official Journal, L 119, ELI: http://data.europa.eu/eli/reg/2016/679/oj

Shaffique, M. R., & Van Der Hof, S. (2026). Behavioural profiling for age assurance: do the ends justify the means?. *International Data Privacy Law*, *16*(1).

Sylwander, K. R., & Livingstone, S. (2025, November). *The impact of General comment No. 25 in the UNCRC review process* [Policy brief]. Digital Futures for Children centre, London School of Economics and Political Science.

Stott, T. C., MacEachron, A., & Gustavsson, N. (2016). Social media and child welfare: Policy, training, and the risks and benefits from the administrator's perspective. *Advances in Social Work*, *17*(2), 221-234.

United Nations Committee on the Rights of the Child (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. CRC/C/GC/25. United Nations. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Woodley, G., See, H. W., O'neill, B., Green, L., Staksrud, E., & Haskell‐Dowland, P. (2025). Australian teen voices on age verification and age assurance measures. *Policy & Internet*, *17*(4).