December 2025

Australia's Social Media Minimum Age Act Undermines U.S. Digital Competitiveness

Executive Summary

Australia's **Social Media Minimum Age Act (SMMA or "the Act")**,[1] which takes effect **December 10, 2025**, substantially amends the **Online Safety Act 2021** by requiring certain online services to take "reasonable steps" to prevent Australians under 16 years of age from holding accounts (§ 63D). The measure is presented as a child-protection law, but its structure and scope—heavily reliant on ministerial designation, broad definitions, and severe civil penalties— severely disadvantage U.S.-based companies in the Australian market.

This brief outlines the Act's statutory mechanics and analyzes its broader implications for digital innovation, global trade, and user privacy. It examines the new framework's inherent operational complexities and recommends policies for keeping the digital ecosystem competitive while protecting youth safety online.

Key Provisions

Scope

The Act's definition of an **"age-restricted social media platform"** (§ 63C) is broad, covering services whose "*sole* purpose," or "*significant* purpose," is to enable online social interaction between two or more end-users. Eight of the ten services currently considered by the regulator to be "in scope" are owned by U.S. companies, including Facebook, Instagram, Reddit, Snapchat, Threads, Twitch, X, and YouTube,[2] with the Act granting the Australian government substantial interpretive flexibility.

The Act includes exemptions for services primarily used for business, messaging, gaming, enterprise collaboration and education.[3] The Minister for Communications may also designate or exempt additional services as age-restricted through legislative rules when **"reasonably necessary"** to minimize harm (§ 63C(1)(b)). While the Minister must first seek advice from the eSafety Commissioner, there is no requirement to adopt that advice, nor mandates for transparent criteria, public evidence, or independent expert review. This gives Australia's executive branch **unfettered power** to expand or contract the scope of regulation quickly, without the accountability of parliamentary debate.

Australian officials have already indicated an intent to scope in the "most popular" services,[4] almost all U.S.-based, rather than applying a neutral, function-based risk assessment. This

[1] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7284
[2] https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions
[3] https://www.legislation.gov.au/F2025L00889/latest/text
[4] https://www.infrastructure.gov.au/sites/default/files/documents/esafety-commissioner-advice-on-draft-online-safety-rules-19-june-2025.pdf

approach reinforces concerns that political visibility, rather than harm-based evidence, may ultimately determine which entities the bill covers.

"Reasonable Steps" Requirement

Section **63D** introduces a sweeping duty requiring covered services to take **"reasonable steps"** to block access for all Australians under 16. This duty applies to both new and existing accounts, effectively requiring providers to reassess their entire user base and close accounts where age cannot be verified.

The Act **does not define** what constitutes "reasonable steps," nor does it mandate specific risk thresholds. In a context of heavy penalties, covered entities are likely to err toward **stricter forms of age assurance**, potentially involving facial analysis, documentation review, or behavioral inference. Such measures significantly increase operational burdens, raise privacy risks, and—because of their fallibility—may still fail to prevent account creation by minors.

Enforcement Powers

The Act grants the eSafety Commissioner expansive investigative powers, including the ability to compel information relevant to service designation and compliance (**§ 194**).
Non-compliance with information requests triggers a civil penalty of **500 penalty units** (AUD $165,000 or approximately **USD $109,000**), whereas major violations, such as failing to prevent age-restricted users from holding accounts, incur a substantially larger fine of **150,000 penalty units** (AUD $49,500,000 or approximately **USD $32.2 million**).

The Commissioner may also publish public statements about alleged violations (**§ 120(2)**), creating reputational risk even before adjudication. The lack of rapid or automatic judicial review increases the disproportionate leverage the Commissioner holds over U.S. companies.

Privacy Provisions

The Act prohibits covered entities from only accepting government ID or accredited digital identity services as the exclusive means of age assurance (§ 63DB), requiring that they also offer at least one alternative method. It also imposes limits on retention and treats misuse of age-assurance data as an interference with privacy (§ 63DA). While these provisions add some guardrails, they do **not eliminate the underlying privacy risks**. Mandated age verification creates large repositories of sensitive user data for hackers and other malicious actors to exploit, since such data must be collected, processed, and stored for compliance purposes.[5]

Implications for U.S. Companies

Disproportionate Market Impact

The law's broad scope and regulatory discretion will likely burden U.S.-based services disproportionately. Such asymmetry risks **violating nondiscrimination and fair competition**

[5] https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586

principles that underpin digital trade, potentially creating a *de facto* barrier to market access for U.S. service providers. Industry bodies within Australia have warned[6] that this approach forces covered services to act as 'internet police,' limiting the market to only those companies with enough resources to absorb significant compliance liability.

Technical Ineffectiveness

A blanket age ban is **unlikely to actually prevent determined minors from accessing covered sites**. VPN use, identity spoofing, and account sharing are simple and readily available workarounds,[7] which means the regulatory burden on covered services is massive while the practical safety benefit is limited. This shift undermines the Act's safety rationale and could increase exposure to harmful content, a concern widely shared by the Australian technical community. In an open letter to the Prime Minister,[8] over 140 Australian technology and child welfare experts argued that the ban is "too blunt an instrument" that will drive minors to less regulated, more opaque spaces.

Impacts on Youth: Safety Paradoxes, Community Disruption, and Constitutional Challenges

Account bans for Australians under 16 **create a perverse safety outcome** by overriding parental discretion. Parental tools like time limits, content filters, and activity logs require a linked account to function. By forcing minors to browse anonymously to evade age-gating, the law strips away these safeguards, pushing teens into generic feeds where exposure to mature content may be significantly higher.

Beyond passive consumption, the ban **disrupts active participation in creative and educational ecosystems**. Young creators, many of whom produce educational or other forms of age-appropriate content, stand to lose access to audiences and income. Furthermore, the ban threatens to sever critical lifelines for marginalized youth, disproportionately isolating teenagers in regional areas and LGBTQ+ communities, for whom online forums often provide the only available access to identity-affirming support networks and mental health resources not found in their physical environments.[9]

This restriction on digital participation is the primary basis for a **constitutional challenge** in Australia's highest court brought by several Australian teenagers,[10] which argues that the ban infringes upon the implied freedom of political communication and the rights of young Australians to access information.

[6] https://www.aph.gov.au/DocumentStore.ashx?id=fea53aa3-a3d1-4482-a3ae-d64c03b144dc&subId=759956
[7] https://onlinesafetyexchange.org/social-media-bans-for-young-people-popular-but-pointless/
[8] https://au.reset.tech/news/open-letter-about-social-media-bans/
[9] https://www.abc.net.au/news/2025-10-13/social-media-ban-will-isolate-regional-queer-teens-more/105829530
[10] https://www.theguardian.com/media/2025/nov/27/teens-high-court-injunction-australia-under-16s-social-media-ban

Regulatory Contagion

Australia is actively **promoting its model abroad** in multilateral forums (e.g., UNGA[11]) and through bilateral engagement. New Zealand,[12] Indonesia,[13] Malaysia,[14] Papua New Guinea,[15] and several EU member states are adopting or considering similar frameworks,[16] often with broader scope or more aggressive enforcement. This heightens the risk that "minimum-age bans" become a standard regulatory lever used to target foreign businesses, condition market access, or compel proprietary disclosures under the guise of online safety.

Policy Recommendations

Suspend Implementation Pending Feasibility and Impact Assessment

The December 2025 effective data should be **suspended** to allow for a **comprehensive, public assessment** of technical feasibility, economic impact, and privacy risks. Enforcing a deadline prior to the maturation of secure, standards-based age assurance technologies creates significant security risks for users.

Prioritize Risk-Based, Safety by Design Models

Regulatory frameworks should shift focus away from access prohibitions, which fracture the digital marketplace, toward **"Safety by Design" principles**.[17] Emphasizing safer defaults, voluntary parental controls, and robust online safety measures helps protect younger users online without necessitating the overbroad exclusion of users or the collection of sensitive identity data.

Condition Mandates on Privacy Protections

No age-verification obligation should be imposed until **decentralized, privacy-preserving standards** are fully established. To prevent surveillance risks, regulations must prohibit any requirement that forces private entities to collect government identification or create centralized identity databases.

Conclusion

Australia's Social Media Minimum Age Act reflects genuine, shared concerns about youth safety but employs **structurally overbroad tools** that carry serious consequences for privacy, speech, competition, and global digital trade. Because the Act's model is already spreading

[11] https://www.reuters.com/business/media-telecom/australias-social-media-ban-teens-draws-praise-un-2025-09-25/
[12] https://www.reuters.com/world/asia-pacific/new-zealand-parliament-debate-teen-social-media-ban-2025-10-23/
[13] https://jakartaglobe.id/tech/prabowo-signs-regulation-to-restrict-social-media-use-among-children
[14] https://asianews.network/malaysias-government-to-block-under-13s-from-social-media-says-communications-minister/
[15] https://www.theguardian.com/world/2025/oct/03/papua-new-guinea-considers-age-restrictions-on-social-media-fears-voices-will-be-silenced
[16] https://www.europarl.europa.eu/news/en/press-room/20251120IPR31496/children-should-be-at-least-16-to-access-social-media-say-meps
[17] https://www.esafety.gov.au/industry/safety-by-design

internationally, the U.S. has a strategic interest in shaping implementation and promoting **evidence-based, trade-facilitating alternatives**. Without careful engagement, the SMMA may become a **global precedent** for discriminatory regulation of U.S. digital services.