RSIS COMMENTARY

24 March 2026

Australia's Social Media Minimum Age Act – Has It Addressed the Issue?

Sean Tan

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 057 – 24 March 2026

Australia's Social Media Minimum Age Act – Has It Addressed the Issue?

By Sean Tan

SYNOPSIS

Australia's Social Media Minimum Age Act has been portrayed as a resolute ban on minors' access to social media. However, its design has significant gaps that could affect other jurisdictions considering similar measures.

COMMENTARY

Last December, Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024 transitioned from legislative proposal to actual enforcement. Ostensibly a bold initiative to protect minors from online harms, the Australian government has been eager to portray its new minimum age rules as a leading step in child online safety.

Announced with considerable political confidence, the policy has been praised as both protective and long overdue. It has been widely reported in both domestic and international media as a decisive *ban* on social media access for under-16s.

As enforcement begins, a more fundamental debate arises: Does the law truly restrict access, or does it merely shift responsibility while maintaining structural conditions that allow underage use? The answer to this question matters for domestic legitimacy and for the adoption of similar initiatives elsewhere.

A "Ban" Without Prohibition

Australia has not criminalised under-16s' access to social media, nor has it imposed legal penalties on parents who allow it. On the contrary, the government has

described the law as merely constituting a *social media delay rather than enforcing an outright ban.* In reality, nothing in the framework compels parental enforcement, nor does it give the state the power to intervene if parents choose not to comply. Public polls even suggested that fewer than a third of parents intend to enforce the restriction actively.

Instead, the burden of compliance sits squarely with social media platforms, which are required to take "reasonable steps" to prevent minors from holding accounts, or risk penalties of up to AU$49.5 million (US$34.6 million). Where household-level enforcement is weak or absent, the policy's effectiveness rests almost entirely on platforms' technical willingness and capacity to act.

Accordingly, compliance has largely occurred through platform-level account deactivation and age-assurance processes – perhaps most notably by Meta, which has removed over half a million Australian accounts believed to be held by users under the age of 16 and has incorporated age-prediction models to ascertain user age. Crucially, these measures do not prevent *access* to content which does not require a login. Many sites remain viewable without an account, and minors below 16 can still watch videos or read posts.

In this regard, the law's statutory design avoids criminalising users while imposing compliance duties on platforms to reshape their user base. Instead of directly prohibiting social media engagement by minors, legislators have rhetorically asserted prohibition while neglecting to specify how youth exclusion is to be effectively implemented in practice.

Pushback by Social Media Platforms

Unsurprisingly, the new framework has been met with resistance from major platforms, which have questioned both its feasibility and coherence. Despite publicly emphasising its compliance efforts, Meta has also reiterated long-standing concerns about the limitations of age verification measures, the absence of industry standards for age verification technologies, and the fact that regulators expect outcomes without defining (let alone mandating) acceptable technical means.

Reddit's response has been more robust. The platform indicated that it would comply with the law but also launched a High Court challenge, arguing that the legislation is being applied inaccurately and illogically. Central to its argument is that the law focuses on account-holding rather than access (as logged-out users can still view content); consequently, platforms risk being penalised for a form of engagement that the statute does not meaningfully regulate.

Industry groups and other platforms have echoed these concerns. Some argue that the law's accelerated implementation timeline and its reliance on the undefined standard of "reasonable steps" expose platforms to substantial legal risk, even where good-faith compliance efforts are made. Others have further warned that more intrusive verification requirements risk misidentifying adult users.

Root Causes Remain Unaddressed

As such, policy frameworks that target a symbolic threshold without addressing the underlying online structures of engagement and design incentives may achieve limited results. When enforcement focuses on account eligibility, rather than how content is surfaced (and monetised), the main drivers of harm remain largely intact.

Even if age-gating were accepted as the most operationally feasible enforcement mechanism currently available, "reasonable steps" and enforcement obligations remain somewhat open to subjective interpretation and inconsistency – for instance, where different platforms apply varying standards based on their own incentives, which undermines meaningful accountability.

Additionally, the regulatory guidance itself confirms that platforms are not required to verify the age of all users or to meet any defined accuracy standard. Platforms can plausibly comply (e.g., through self-declaration) while avoiding robust verification. Further fundamental questions are whether such legal frameworks meaningfully address market incentives or serve as administrative delegations to corporate organisations, which are then tasked with managing risk at the margins.

Enforcement at the Point of Use

The Australian framework also encapsulates a broader regulatory pattern: regulation at the point of use rather than at the system or platform-design level. By focusing on user age (rather than, for example, content recommender systems or engagement mechanics), the framework overlooks the commercial incentives that shape minors' online exposure in the first place.

Although minimum age thresholds may appear decisive, they are inherently fragile. Minors are notably adept at bypassing digital restrictions – perhaps even more so than parents, who may lack the capacity or time to intervene (even if willing to do so).

These limitations are not merely speculative. Independent expert assessments commissioned ahead of enforcement have consistently found that existing age-assurance methods (such as behavioural inference and biometric estimation) are prone to error or manipulation and may also be unevenly applied by social media platforms.

Moreover, while the statute rests on an implicit assumption that age thresholds will reduce online harms experienced by minors, a growing body of research suggests that they do not meaningfully reshape the dynamics of exposure or engagement in digital environments, particularly regarding algorithmic content available to logged-out users (or via shared and/or family devices).

Similarly, neither do such thresholds address broader categories of harm (including, but not limited to, cyberbullying, misinformation, and addictive design features), which are, in any case, amplified by recommender systems optimised for engagement rather than age appropriateness.

Implications for Similar Frameworks Abroad

Despite its implementation ambiguities, Australia's move has already become a reference point in other regulatory debates. France and the UK have publicly floated social media age bans for younger cohorts, explicitly citing the Australian example as precedent. Regulatory interest is also rising in the Asia-Pacific, with proposals from Indonesia, Malaysia, New Zealand, and the Philippines reflecting an age-restricted approach.

Adopting the Australian model as a blueprint may introduce significant enforcement gaps without appropriate mechanisms for system-level governance. At the user level, the outright criminalisation of unauthorised social media usage is likely to be as unfeasible as it is heavy-handed. Enforcement agencies would also be structurally constrained from verifying compliance at scale without triggering new privacy and data protection concerns.

Conversely, legislators also have an opportunity to broaden the policy lens by integrating education and infrastructure-level safeguards into a more holistic framework for children's digital rights. For now, Australia's framework may continue to signal intent and influence global debates.

However, early evidence suggests that the underlying dynamics of online harms remain largely unchallenged and that regulatory authority has shifted from the state to corporate platforms. The result is a measure that rhetorically claims control without fully exercising it. Therefore, the question is not whether Australia has banned children from social media, but whether it has merely shifted responsibility elsewhere.

Sean Tan is a Senior Analyst at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.