SQUIRE PATTON BOGGS

New Report Tests Digital Age Checks in Australia – Here Is What it Found

Australia – September 2025

As digital platforms come under scrutiny to create safer online spaces – particularly for children – the use of age assurance technologies is emerging as a key tool. A recent Age Assurance Technology Trial (the Trial), commissioned by the Australian government, provides critical insights into the effectiveness of such technologies and the different benefits and shortcomings of specific methods. We review the final report (Report) into the Trial below.

The Legal Context

The Trial has taken place in a regulatory environment where the Australian government is exploring tighter controls on access to online services. While Australia has not yet introduced a comprehensive age verification regime akin to the UK's, we are heading in a similar direction. Not only has the eSafety Commissioner implemented codes that require access to age-inappropriate content to be restricted, but the social media "pause" will come into effect in November, requiring age-restricted platforms to take reasonable steps to prevent under 16s from registering accounts.

The government has told us that the results of the Trial will "complement [industry] codes" and that they will build an "implementation plan" based on its findings. Although the Report states that it does not offer "policy recommendations or endorsements", the Trial is clearly more than a technical feasibility test – it will likely be used as a precursor to future regulation and guidance.

Key Findings and Takeaways

The Report spans 1,150 pages. Close to 50 suppliers were tested, with methodologies extending from vendor interviews to mystery shopping scenarios and school-based field testing. Technologies were tested across a range of requirements, including practical effectiveness, usability, privacy compliance, fairness and bias, and security. Practically, this involved testing the technologies against emerging international standards, such as ISO FDIS 27566-1, IEEE 2089.1 and ISO 25000.

This is what stood out to us in the Report – and what it might mean for you:

No Silver Bullet for Age Assurance

The Report tells us, front and centre, that age assurance can be done in Australia privately, efficiently and effectively. However, there is no one-size-fits all solution. Age assurance itself is an umbrella term, whose scope covers age verification, age estimation, age inference, and parental controls and consent. Those methods that offer the greatest accuracy (e.g. age verification) may be the most privacy intrusive, while age estimation – commonly deployed on social media today, including as a background process (for example, Meta uses it when users change their date of birth) – can take place with minimal user and privacy friction, but may not be appropriate for a high-stakes context.

The best way forward seems to be what the Report calls "successive validation" – requiring age assurance to be "proportionate to risk" and "enabling layered approaches where no single method alone is sufficient or contextually appropriate". Many social media platforms already enable this approach. For example, if a user wants to appeal an age finding (which is typically made through age inference) on TikTok, they can do so through selfie with ID (age verification), asking their parent or guardian (parental consent) or photo with parent/guardian (parental consent). In some regions, this can extend to facial age estimation (age estimation).

> **Tip** – Proportionality is critical. In keeping with the Privacy Act, any age assurance solution must only collect the personal information that is reasonably necessary to achieve the stated aim.

Privacy Is (Mostly) Baked In

According to the Report, most providers have in place robust, appropriate and secure data handling practices. But the Trial found some "concerning evidence" that providers were "over-anticipating the eventual needs of regulators" and retaining personal information to respond to such (unmade) requests. This included building tools to retrace actions taken by individuals to verify their age, which would counteract some of the stated benefits of facial estimation (including that personal data is often not retained).

The Report agrees that this practice carries both privacy and cyber risk and considers that providers "[require] clearer regulatory guidance to ensure proportionality". While Section 63F(3) of the Online Safety Act requires the destruction of personal information once it is no longer necessary to prevent under 16s from registering a social media account, this leaves several questions unanswered.

For example, if a platform successfully uses age-related information to deny a 14-year-old from registering an account, is it permitted to retain that information in case of future attempts, or is this limited to one-time use only? Equally, can platforms retain age-related information to show only appropriate content to 16-to-17-year-old users after they have registered? Guidance on these – and other – aspects of the legislation would be extremely helpful ahead of November.

> **Tip** – Evidence (and notify your users of) different authorised uses of age-related information and craft a retention policy that supports them, without keeping personal data "just in case".

Better Data Reduces the Risk of Bias

Data is not only a regulatory risk – it is an opportunity. Nothing proves this better than the Report's finding that age estimation models often produced increased false positives for users with darker skin tones, or users aged 16 to 20. To counter this, the Report recommended that providers "expand [their] testing data sets", including through the use of synthetic data augmentation and "consent-based data gathering" in collaboration with local, underrepresented communities.

> **Tip** – If deploying a third-party solution, ask questions about how the tool was tested and, importantly, the data on which it was built. The Report raised the possibility of nonfacial, privacy-preserving age estimation (such as hand geometry), but recognised that this is not yet developed to the same level as biometric age estimation. Still, this is an option to watch as technology becomes more sophisticated.

Watch Out for Third-party Risk

Many of the providers tested do not supply services themselves but instead provide services directly to impacted platforms. Logically, it remains the platform's responsibility to assess where and how a tool should be used, but responsibility for violations is not always clear. Social media platforms prioritise "real-time, in-app" age estimation, meaning that they especially may be seen to be responsible for material errors made by their suppliers, or those suppliers' misuse of personal information.

> **Tip** – Robust contractual arrangements – which include warranties, appropriate liability limits and a clear delineation of responsibilities – will be essential for platforms outsourcing age assurance to vendors. This mirrors broader trends in privacy law around controller-processor relationships.

Security Measures Evolve

According to the Report, most providers showed alignment with today's security expectations, but vigilance is required. This is especially critical given the risk of deepfake manipulation and injection attacks (which the Report acknowledges are "inherent threats" to age assurance), but, also, due to the kinds of data that age assurance providers are expected to hold – and may in fact retain if they do not abide by deletion protocols.

> **Tip** – Any contract with an age assurance provider should include, insofar as possible, security audit rights and a continuous improvement regime. Where necessary (and specifically in the context of age verification), time-limited retention policies and technical deletion controls are key.

Author

Tanvi Mehta Krensel
Partner, Sydney
T +61 2 8248 7810
E tanvi.mehtakrensel@squirepb.com

69125/09/25