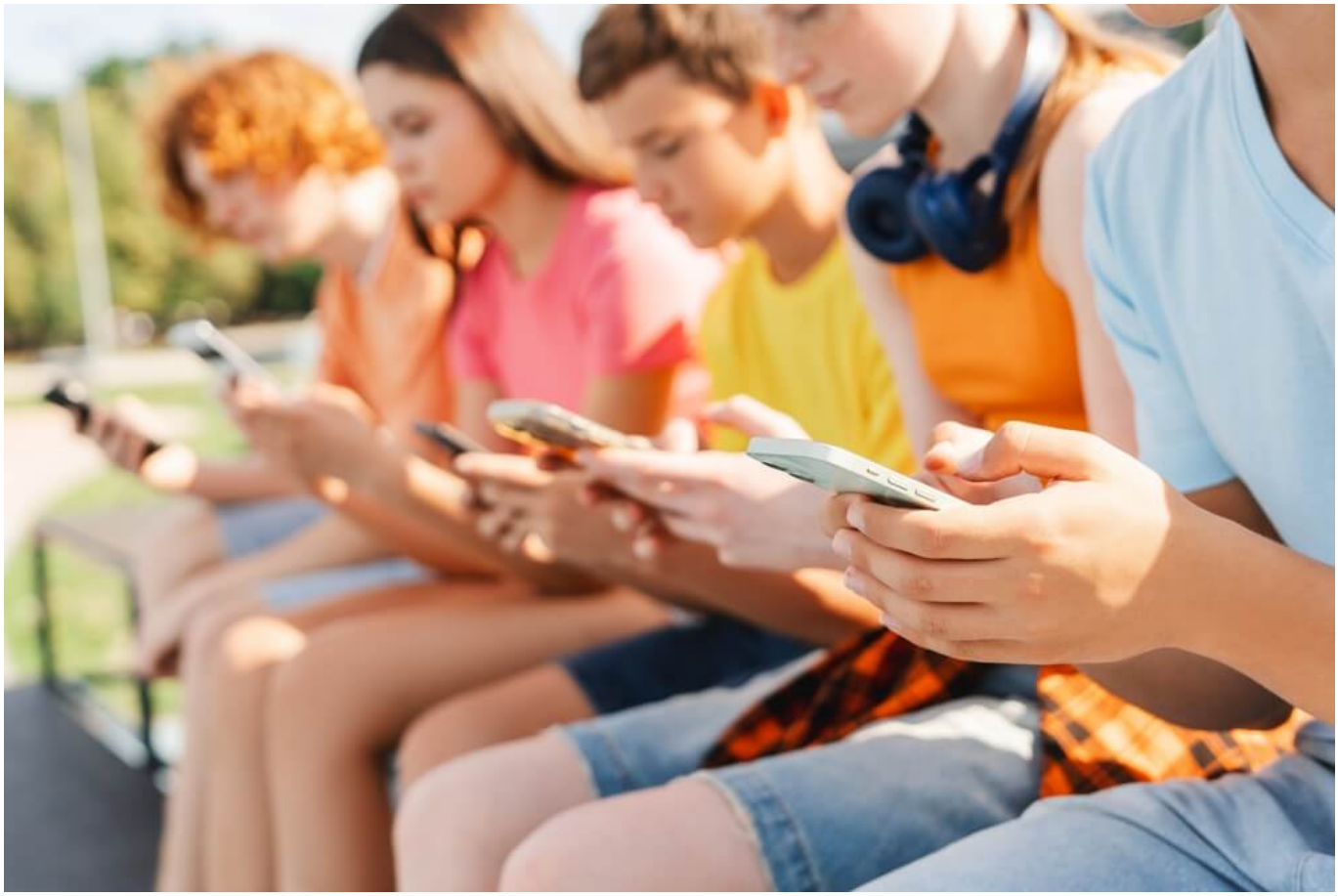
Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Australia vs Big Tech – who decides how old a user is?



Australia's decision to double the maximum penalties for platforms that fail to prevent children under 16 from having social media accounts raises a much bigger issue than simply protecting minors online.

It is the first serious test of the state's ability to compel global digital companies to implement a rule that directly impinges on their most valuable asset: access to users, their data, and the time those users spend on the platform.

Prime Minister Anthony Albanese's government has announced that the maximum fine for systematic violations of the rules will be increased from 49.5 million Australian dollars to 99 million Australian dollars, or about 68 million US dollars.

At the same time, the eSafety Commissioner, Australia's independent internet safety regulator, should be granted stronger powers to require platforms to provide evidence of what they have actually done to prevent users under 16 from opening or maintaining accounts.

The regulator will be able to request information not only from the platforms themselves but also from third parties, including companies that provide age-verification technologies or app-distribution intermediaries.

Australia is now attempting to do what many states have postponed for years: turn rules written into law into obligations that platforms must implement in their own systems. The law came into force on 10 December 2025.

Platforms covered by the rules must take reasonable steps to prevent Australians under the age of 16 from opening or maintaining an account. Children and parents are not punished. Responsibility has been shifted to where the data, algorithms, account opening procedures and access control actually reside: the platforms themselves.

This distribution of responsibilities is precisely where a political novelty lies. Canberra is not asking families to solve a problem that arises from the design of digital systems themselves.

It argues that companies that manage access, recommendations, accounts and data must be held accountable for the users they admit into the system. It marks a shift in attitude towards Big Tech.

Platforms are no longer regarded solely as services that citizens use voluntarily, but as infrastructure whose consequences the state has begun to measure and sanction.

Weak point of the law

The Australian model became globally visible precisely because it was ambitious enough for others to follow closely. However, six months of implementation exposed its greatest weakness.

The government claims that more than five million accounts belonging to users under the age of 16 have been removed, deactivated or restricted. At the same time, research shows that many adolescents still use social networks.

According to a study published in the British Medical Journal, more than 85% of Australians aged 12 to 15 were still using social media three months after the rules took effect. Those data show where the real problem with the Australian model lies.

If the law is formally valid, yet most users whose access is restricted still remain on the platforms, then the weakness lies not in the ban itself, but in its implementation, in age-verification methods, and in companies' willingness to genuinely change the way users enter the system.

The announced change in the law is therefore not only a matter of harsher penalties. Canberra is trying to remove the platforms' ability to comply formally without making real changes to the system.

So far, it has been sufficient to show that there

is an age-verification procedure, a category of deleted accounts, and an internal rulebook confirming compliance with the law.

> Australia's communications minister, has accused the platforms of doing only what is necessary to avoid punishment, rather than what is needed to make the law work

The regulator's new powers are intended to reveal something more specific: how platforms verify users' ages, how quickly they react when they discover a younger user's account, where the verification system fails, and whether measures are in place to prevent access or provide the company with proof that it has at least attempted to do so.

Anika Wells, Australia's communications minister, has accused the platforms of doing only what is necessary to avoid punishment, rather than what is needed to make the law work.

That is the crux of the dispute with Big Tech. Companies that track user behaviour in minute detail, measure dwell time, recognise interest patterns and target content to each profile now claim that reliable age verification is a technically and legally complex issue.

This is precisely where the Australian government sees hypocrisy: systems accurate enough to sell the attention of minors suddenly become powerless when it comes to keeping them off the platform.

This is where the most politically sensitive part of the case emerges. Australia now requires platforms to prove that they genuinely control who enters their system, rather than merely maintaining a formal procedure to protect themselves from punishment.

Governments find it increasingly difficult to accept the claim that companies have enough data to accurately convert children's attention into revenue yet lack a reliable way to determine who is allowed to be a user in the first place. That is why Australian law has become the first major legal test of Big Tech's responsibility for its own entry system.

The responsibility lies with the platforms

Canberra has therefore carefully defined this responsibility: children under the age of 16 will not be fined if they try to use social media, nor will parents be fined.

In practice, the rule means that platforms must prevent users under 16 from opening a new account or keeping an existing one. Politically, it is important that responsibility is not shifted to families but placed on the companies that control access to the platforms.

This wording is important because the fate of the Australian model will depend on three factors: child protection, privacy protection, and the state's ability to compel platforms to actually enforce the rule.

A state may require stricter age verification, but any tighter checks raise the question of how much personal information users must disclose. If age verification is reduced to entering a date of birth or simply confirming that the user is old enough, the law remains weak.

If the state requires much stricter identity verification, another question arises: how much data users have to hand over, and who will be able to use it in future.

> For now, Canberra is trying to focus pressure on companies rather than citizens

Australia is therefore not only addressing children's access to social networks, but also entering a much wider debate about where the protection of minors ends and the infrastructure of digital control begins.

This makes the Australian case far more serious than the usual debate about screens, children and parental controls. It tests how a liberal state can restrict digital platforms without creating a dangerously intrusive identification system. It is a fine line.

Platforms will stress user privacy when stricter vetting does not suit them. States will stress child protection when they need tighter oversight of platforms. The public will simultaneously want less harm, less dependence on screens and less data collection.

For now, Canberra is trying to focus pressure on companies rather than citizens. That is why strengthening the authority of the eSafety Commissioner carries particular weight.

The regulator will not be able to rely solely on the platforms' statements. They will need to see the procedures, results, omissions and technical flows that sit behind formal compliance. In digital regulation, this is often the difference between a law that exists on paper and a law that changes companies' behaviour.

Why is the world closely monitoring Australia?

Australia does not have the scale of the US market, the regulatory weight of the European Union, or the technological power of China.

Yet this is precisely why its experiment has particular value. It shows what a medium-sized country can do when it comes into direct conflict with the largest digital platforms.

Facebook, Instagram, YouTube, Snapchat and TikTok are all under active investigation for potential violations. The broader list of platforms that eSafety considers covered by the rules includes X, Reddit, Threads, Twitch and other services.

The sheer breadth of this list shows that it is not a narrow measure aimed at one company or one type of content. It is an attempt to bring the entire model of social platforms up to a minimum standard of responsibility towards minors.

The UK is already closely monitoring the Australian model and introducing restrictions that could go even further, including in parts of the gaming and live-streaming space. France, Denmark, Spain, Poland, Slovenia and Malaysia are considering or developing similar approaches, while Norway, Greece, Sweden, Türkiye, Indonesia and certain Indian states are moving in the same direction.

The differences between these models are important: in some cases they propose a complete ban before the age of 15 or 16, in others they require parental consent, and in others they impose an obligation on platforms to verify the user's age themselves.

> The platforms will try to demonstrate that the law is too broad, technically difficult to implement, and risky for freedom of expression

However, the broader trend is clear. Governments are increasingly rejecting the idea that children's presence on social media is solely a family matter. Australia has therefore become a useful testing ground for a much wider change: an attempt to shift responsibility for minors' access from parents to the companies that control digital access.

The most serious legal challenge so far comes from Reddit, which is contesting the law in Australia's highest court on the grounds of freedom of political communication. As a result, the dispute is no longer solely about the protection of children, but also about the status of social networks in modern public life.

If platforms have become spaces where part of the political conversation takes place, then the state must carefully explain how it restricts access for minors without infringing the freedom of public speech itself.

Yet this very public role of platforms also strengthens another argument: systems that have become an important part of social communication cannot remain outside robust rules on access, user protection and responsibility towards minors.

This is why this dispute will matter beyond Australia. The platforms will try to demonstrate that the law is too broad, technically difficult to implement, and risky for freedom of expression.

The government will argue that the public importance of social networks does not reduce companies' responsibility but increases it. The outcome of this conflict will be closely watched by every country considering similar restrictions.

Canberra is looking for proof, not an explanation

The 99 million Australian dollars fine is attracting attention, but the fate of this bill will not be decided by the amount of the fine alone. For the biggest platforms, it is a serious blow to their reputation and business, but not a sum that changes their underlying economic logic.

What will be crucial is whether eSafety can verify companies' claims: how they determine a user's age, how reliable their checks are, and what they actually do when they discover an underage account.

This is where the most difficult part of the Australian test begins. Platforms will no longer be able to rely solely on terms of use, general explanations, and the number of accounts removed.

If Canberra succeeds in turning the minimum-age rule into a genuine corporate commitment, other democracies will have a model they can emulate - Anthony Albanese

The regulator will want to see how users' ages are verified, how reliable those checks are, what happens when the system detects an account belonging to a minor, and how quickly the company responds. The benchmark will no longer be the platform's claim to obey the law, but the effectiveness of its system in preventing what the law prohibits.

Australia will not win that battle easily. Young users will look for ways to stay on the platforms. Companies will offer technical solutions that reduce the risk of fines while preserving as much of the existing model as possible.

Courts will have to draw a line between the protection of minors, privacy and freedom of communication. At the same time, the government will have to deliver results, because it has itself raised the political price of failure.

The direction is set. It will become increasingly difficult for large platforms to argue that they have done enough if minor users continue to remain in the system. States will look for evidence, data and measurable results.

That is far more embarrassing for Big Tech than the fine itself, because it cuts into the part of the business that companies have kept under wraps for the longest time: how they control accounts, user profiles, access to data, and the distribution of content.

That is why the Australian case has a

significance that extends beyond the ban itself for under-16s. It will show where state power ends when confronted with platforms that control attention, identity and access to digital public space.

If Canberra succeeds in turning the minimum-age rule into a genuine corporate commitment, other democracies will have a model they can emulate. If it fails, the conclusion will be just as serious: states do not yet possess sufficiently robust instruments for the systems they are trying to regulate.