Minors' online safety: The options beyond Australia's social media ban
By Lim Sun Sun

The Straits Times, Singapore, Page 3, Section: OPINION I
Wednesday 8 April 2026
1850 words, 1749cm² in size
386,100 circulation

Minors' online safety: The options beyond Australia's social media ban

In the efforts to keep minors safe online, there are lessons to be drawn from Australia's ban, Brazil's tighter rules and Singapore's Codes of Practice for Online Safety.

Lim Sun Sun

In a trial watched closely by online safety advocates, a Los Angeles jury recently found Meta and Google negligent for designing Instagram and YouTube in ways that harm young people. Whereas US law protects social media companies from liability for the content on their platforms, this case focused squarely on platform design rather than content and the companies' failure to warn users of their products' potential dangers. This "bellwether" verdict is likely to influence thousands of similar cases consolidated in California.

The case was brought by a 20-year-old woman who claimed to have become addicted to social media as a minor due to attention-capturing features like infinite scroll. Meta was found liable for US$4.2 million (S$5.4 million) in damages and Google (which owns YouTube) US$1.8 million. TikTok and Snapchat were also defendants in the trial but reached a settlement with the plaintiff without disclosing details.

With the ruling hinging on evidence that the tech companies had knowingly introduced features to make the platforms deliberately addictive to teens, some may argue that it strengthens the case for social media bans for young people. But this would be the wrong conclusion to draw and Australia's fraught experience with its social media ban will shed useful light.

AUSTRALIA'S EXPERIENCE WITH BANS

Passed in late 2024, Australia's Online Safety (Social Media Minimum Age) Act effectively prohibited children under 16 from having social media accounts and covered platforms such as TikTok, Instagram, Snapchat, YouTube, Reddit, Twitch and X. The legislation has drawn close attention worldwide, spurring a wave of similar regulatory efforts. From Indonesia, Malaysia, Austria, France, Denmark to the UAE, at least 42 countries are working through or have already passed age-restriction measures for social media.

But here are critical lessons we can draw from the consequences of Australia's social media ban. First, months after the imposition of the ban, many youths are reportedly still able to access these platforms via workarounds. Children have thus not withdrawn from the online world but have instead adapted their behaviours. Although access has seemingly been curtailed with millions of under-16 accounts removed or restricted, demand remains strong, and usage persists via VPNs and subverting age verification tools.

Circumvention is a notable reality, underlining the technical and practical limits of enforcement. Current age verification systems operate on a spectrum of reliability: government ID–based checks remain the most accurate (with low error rates), AI-driven facial age estimation is improving but still carries a margin of error, while self-declaration and payment-based methods are easily bypassed and therefore weakest.

To get around these limitations, regulators often introduce "grey zone" buffers, yet even stronger systems are vulnerable to spoofing through deepfakes, borrowed IDs, and other workarounds used by tech-savvy minors. At the same time, these systems face structural challenges including demographic bias in facial analysis and significant privacy risks from storing sensitive biometric and identity data which necessarily raise concerns about fairness, security, and public trust.

Second, rather than eschewing the online world entirely, children have migrated to less regulated environments such as gaming, messaging and chatbot platforms where oversight is weaker and harms may be less visible. Interviews with young people reinforce this mixed picture, suggesting that daily digital habits remain largely intact and that bypassing restrictions is often straightforward. Given such platform migration, the online risks children face are not diminishing but are merely shifting.

Third, as young Australians keep up such active circumvention, critics assert that they are being socialised into thinking that laws can be easily violated without ramifications. At their formative age, such experiences of acting with impunity will distort their understanding of citizenship and legal obligations for the long haul.

Above all, keeping young people off social media also denies them online spaces that can be edifying and beneficial if used with the right safeguards. In totality, these challenges —including workarounds, platform migration, loss of beneficial online spaces, and imperfect age assurance technologies — underscore the limits of access-focused approaches. Crucially, there remains limited robust evidence that blanket bans actually improve wellbeing.

BRAZIL'S STRICTER RULES

If bans are difficult to implement effectively, and there is evidence of tech companies' designs inducing unhealthy dependence, how can regulations be tightened to hold technology companies to account? Most recently, Brazil passed in record time its ECA Digital Law (named after the country's foundational Estatuto da Criança e do Adolescente child protection statute) with stricter rules to protect children online.

As regulations go, Brazil's ECA Digital Law imposes a comprehensive duty of care on platforms, mandating robust age verification and tiered access restrictions for inappropriate, prohibited, and illegal content, with enforcement extending to app stores and operating systems at the account-creation level.

It also requires platforms, especially those targeting minors, to curb addictive design practices by strengthening privacy protections and limiting techniques such as profiling, emotional analysis, and manipulative reward systems. Complementing this, the law introduces an expedited notice-and-takedown regime and a strengthened enforcement architecture led by Brazil's federal regulatory agency on data protection, supported by a new screening unit within the police force. Platforms found to be in violation could face warnings and fines of up to US$10 million and for extreme cases, suspensions and outright bans from the country imposed by Brazilian courts.

As with the Australian experience, implementation and enforcement will determine the tangible effects of this bold and ambitious regulation. Critics are already predicting that it will have more bark than bite, referencing an oft-cited Brazilian saying that "there are laws that stick, and laws that don't". Ensuring that the ECA Digital Law is squarely of the former will be a monumental task.

SINGAPORE'S CODES OF PRACTICE

Brazil is certainly not alone in wanting tech companies to exercise greater accountability but the track record for concretely holding platforms to task has been patchy worldwide. Singapore's experience of imposing Codes of Practice for Online Safety – Social Media Services may provide some middle ground. As the recently released Online Safety Assessment Report 2025 by the Infocomm Media Development Authority indicates, securing big tech's compliance can be effected through means other than legislation and punitive measures.

Promulgated in 2023, these codes require designated social media services (DSMs) to address six categories of harmful content, including violent and sexual material, cyberbullying, self-harm, public health threats, and content that promotes criminal activity. Platforms must also limit users' exposure to such content, especially for those under 18, offer simple reporting tools, inform users of outcomes after reports are reviewed, and publish annual online safety reports to promote transparency and accountability.

This being the second report issued since these codes were introduced, it was encouraging to see year on year improvements in the social media services' performance in ensuring online safety. Using the same methodology as in the 2024 report, IMDA undertook mystery shopper tests to assess their safety measures for children. These involved creating fake child accounts to gauge how easily they could access restricted content and verifying how effectively platforms handled reports of harmful content.

Some areas of improvement were noted from the year before.

Instagram had enhanced safety for Teen Accounts by automatically placing users under 18 into the most restrictive content setting, with parental permission required to adjust to a less restrictive setting.

TikTok has also introduced a new parental control that allows parents to switch their teen's account back to the default private setting if their teen has made their profile public.

Meanwhile, YouTube launched a new Family Center hub where parents can access shared insights into their teen's channel activity, and strengthened enforcement of its policies on "violent or graphic content" and "illegal or regulated goods or services" by age-gating additional types of content in these categories, including fictional violence with graphic scenes and certain types of online gambling content such as online casino promotions.

Crucially too, gross lapses were flagged and action taken by IMDA. These pertained to the egregious harms of child sexual exploitation and abuse material (CSEM) and terrorism content. X and TikTok were issued Letters of Caution for their failure to systematically detect and expunge significant numbers of CSEM and terrorism content respectively.

The two companies have since accepted IMDA's findings and pledged to rectify these oversights. They have concurrently been placed under Enhanced Supervision where they must meet regularly with IMDA to report on their remedial efforts until marked improvements are made.

With greater parental interest to regulate their children's media use, the safest platform could become the most popular and tech firms should move towards viewing trust and safety as a profit centre, says the writer. PHOTO: REUTERS

THE WAY FORWARD

By no means is such a governance approach meant to let tech companies get off lightly. But rather than imposing a burdensome regulatory regime that could force tech companies to seek workarounds, the codes of practice require tech companies to do more for online safety, with assessments and supervision to hold their pledges to account. Such an approach can help steer tech companies to channel their abundance of financial, technological and intellectual resources towards architecting digital infrastructures that enhance safety and advance wellbeing.

Equally therefore, the codes of practice should be refreshed to set a higher bar for tech companies. Regulators should go beyond verifying content moderation and responses to user reports and also demand platform proactiveness on eliminating features that manipulate users to stay online longer, including push notifications, infinite scroll, autoplay and autoscroll, or that undermine wellbeing, including beauty filters and sycophantic chatbots.

These have been the features that have benefited tech companies richly by making their platforms stickier and more alluring, drawing more eyeballs and generating tremendous revenue from advertisers, and eliminating them will tank their current business models. A phased approach that requires all DSMs to begin by eliminating the most harmful features will help level the playing field in the first instance, but also give them time to innovate their business models and distinguish their product offerings in other ways.

With greater parental awareness and interest to regulate their children's media use, the safest platform could well become the most popular and tech companies should reorientate towards viewing trust and safety as a profit rather than cost centre.

Around the same time that the US court delivered its landmark verdict, US First Lady Melania Trump appeared at an AI education summit, walking in with a humanoid robot and proclaiming that robot teachers would soon be key to children's education. Contrived as it was, this event captured the relentless frenzy around technology. With AI acceleration gaining pace, bans simply do not help children adapt well to our rapidly technologising world. But making devices and platforms safer by design will do so.

• Lim Sun Sun is vice-president, partnerships and engagement at the Singapore Management University and Lee Kong Chian professor of communication and technology at its College of Integrative Studies. Her latest book is Humanising Technology: Reflections on Design, Ethics and Inclusion.