Singapore reins in app stores to protect the young

Osmond Chia, Sarah Koh
The Straits Times, 25 January 2025

SINGAPORE - Just as age verification is mandatory for pub entry, app stores will soon need to check the age of young users before allowing them to download apps for grown-ups.

Come March 31, Singapore's media regulator will roll out a new code requiring, among many things, that app stores screen and prevent users aged below 18 from downloading apps meant for adults, such as dating apps or those with sexual content. App stores have one year until March 2026 to roll out the measures.

All other obligations spelt out by the Infocomm Media Development Authority (IMDA) in the Code of Practice for Online Safety for App Distribution Services will kick in on March 31, 2025.

For one thing, app stores must have community standards in place and enforce it among app developers, and also respond promptly to reports of violations flagged by its users.

The new code aims to set guard rails at the gateway to apps, which have come under fire for exposing children to all sorts of harmful content, including sexual and violent material and content linked to self-harm or cyber bullying.

The requirements of the code will apply to Apple, Google, Huawei, Samsung and Microsoft as they operate stores or online portals for downloading applications.

With the responsibility pinned on app stores to manage app developers, the authorities have a single point of contact to crack down on problematic apps that also contain, among other things, terrorism-related or child abuse material that could be exposed to children.

The new measures are an attempt to rein in app stores in a similar way to how social media platforms are required to provide restricted account settings and tools for parents to manage their children's safety under Singapore's Code of Practice for Online Safety, which took effect in 2023.

Rule flouters risk being fined up to $1 million or blocked under the Broadcasting Act, which was amended in 2023 to rein in social media platforms and app stores.

Pros of the new code

A key feature of the upcoming Code of Practice for Online Safety for App Distribution Services is age screening.

The logic is simple: If young users are not allowed to download apps not meant for them, the harm stops at the gate.

Institute of Policy Studies (IPS) adjunct senior research fellow Chew Han Ei said that app stores act as "gatekeepers".

"By targeting the app stores, the code tackles a critical access point and introduces clearer responsibilities for regulating content," he said.

The success of the law banks on the effectiveness of age verification methods.

App stores have until March 2026 to roll out the tools to screen the approximate age of users to prevent children from installing dating apps like Tinder, which is rated for ages 18 and above, and those under 12 from downloading TikTok or Instagram.

Today, few app stores enforce age-appropriate downloads. Many simply ask users to state a birth date before downloading a mature-rated app.

Lax age verification has been a headache for parents, said Madam Salizawati Abdul Aziz, 41, who has caught her own children trying to fake their age to download apps for grown-ups.

“I realised how inappropriate some of the apps can be so I started to control their access with family mode settings,” said Madam Saliza, a teacher with six children.

“By having this code,” she added, “app stores can help to restrict and block young users from downloading inappropriate apps and that would prevent unnecessary exposure to these content in the first place.”

The law also broadens the authorities’ powers to crack down on harmful user-generated content within apps, such as inappropriate conversations in games with strangers on chat functions or content posted on social media platforms.

The authorities can now knock on the doors of app stores, which are required to take action against app developers who fail to address users’ complaints about harmful content, or implement measures to spot and address harms. These actions include a ban or removal of the app from the store.

User-generated content has long been a pain point for parents who fret about what appears on their children’s feed.

Popular games like Minecraft and Roblox that are available on app stores have become hunting grounds for predators and bad company, who can target children through in-game chats.

Notably, a radicalised 16-year-old in Singapore had joined several Roblox servers, with maps depicting conflict zones occupied by real-world extremist groups.

The code of practice for app stores will work in tandem with 2023’s Code of Practice for Online Safety, which mandates social media platforms to address harmful content affecting children.

Similarly, app developers are required to monitor their platforms for online harms, provide tools for parents to manage their child’s safety, and respond promptly to user reports of harmful content.

Associate Professor Carol Soon of NUS’ Department of Communications and New Media said that by imposing similar duties on app stores, the authorities will add an extra layer of protection to shield children from harmful content on top of existing regulations.

Social media services were targeted under the Code of Practice for Online Safety, whereas the code for app stores targets all sorts of apps, she added.

Prof Soon, who is also the vice-chairwoman of the Media Literacy Council, said: “This new code enables another layer of mitigation at the system level as it targets app stores that act as users’ entry points to a wide range of services and products, many of which are not covered by existing regulations.”

Hurdles

One of the biggest hurdles to reining in harms online is how to tell if a user is a child.

IMDA has suggested two ways: The use of government-sanctioned identification or credit cards, or technology such as artificial intelligence (AI) and facial screening.

The jury is still out on how these will be implemented. Samsung and Google, for instance, said they are considering their options and in discussions with the authorities, which has given app stores till March 31, 2026, to roll out the measures.

Experts said government ID ranks among the most precise ways to check a person’s age but that it can be seen as heavy-handed as it would require significant changes and raise privacy concerns.

Tech adviser Josh Lee from legal firm Rajah and Tann said IDs are typically used for high-risk services.

App stores and the authorities will need to address privacy concerns, such as fears that the data collected could be used for other purposes, said Mr Lee, who is also a committee chairman at non-profit organisation Cyber Youth Singapore.

It is yet to be seen how far Singapore can influence app stores because businesses generally prefer consistency in global operations, as variations in their app could rack up costs, said Mr Lee.

Mr Glenn Gore, chief executive of identity solutions provider Affinidi, proposed that app stores and the authorities could utilise zero-knowledge proofs – a digital verification process to confirm that users are who they claim to be without revealing sensitive details – tapping national databases like Singpass.

The alternative to ID is facial screening technology, which typically taps the user’s smartphone front-facing camera or some form of AI, to gauge their age.

Experts said age-screening technology is prone to huge margins of error.

A 2024 study by the US National Institute of Standards and Technology on age estimation and verification methods found that the technology’s accuracy varied. Variations, such as camera quality or the user’s skin condition, colour and facial structure, can all affect the accuracy of readings, it found.

Associate Professor Terence Sim of NUS’ School of Computing said that age screening technology may reliably estimate broad age groups, such as people in their 20s or 30s, or children under 13.

But teenagers undergo significant physical changes, making precise age estimation much more challenging, he added.

“This is not a tech problem, it’s just biology. Some people just look younger or older than they are,” said Prof Sim.

Mr Campbell Cowie, head of policy at biometric solutions firm iProov, said platforms should use a mix of age screening technology and identification.

“Age estimation solutions are okay if it’s voluntary. It would just be a best effort,” said Mr Cowie. “But if we want something accurate to use as part of legislation, age verification is the only accurate option.”

He added that the authorities will need to spell out standards for reasonably assessing users’ ages to avoid inconsistencies between app stores, which could put users at risk of harmful content.

Even with facial scannings, there are ways a determined child can evade age checks.

Rajah and Tann’s Mr Lee said children who have access to their parents’ device could access such content since their device would likely be configured to an adult profile.

Children could get the assistance of an adult to pass the age checks and download an app on their own device, he said, adding that adults also play a key part in the issue.

Prof Sim said platforms need to go one step further and require checks in real time, instead of accepting a one-time approval at the point of registration.

For this to work, app stores should seek biometric authentication – a guarantee of explicit approval – each time a user wants to install a mature-rated app. The user’s account should also be linked to digital identification, so that the app store can be certain of the downloader’s age, Prof Sim added.

“You shouldn’t rely on passwords too. They are simply not secure enough as a child might already know the parent’s password, which might have been given to them during the phone’s set-up,” he said.

Experts and parents highlighted inconsistencies in how content is rated. For instance, some apps include films or user-generated content potentially unsuitable for children, even though the app is rated suitable for children on the app store.

These include streaming services like Netflix, which, despite carrying a 12+ age rating on app stores, hosts shows intended for mature audiences (18+), typically protected with a code to restrict access.

NUS’ Prof Soon said the mismatch boils down to age ratings for apps being submitted by app developers in most cases. But enforcing accuracy by app stores could be tough due to the sheer number of apps available, she added.

App developers can make content updates that might render the initial age rating invalid, which makes user reporting channels to flag inappropriate content crucial if developers have any hopes of keeping up.

Room for more

As five major app stores by the likes of Apple and Google figure out suitable tools to spot children, one of the biggest gaps is the omission of PC gaming marketplace Steam.

With millions of users globally, Steam is the PC gamer's gateway to install games with explicit content such as Grand Theft Auto, and others that have come under scrutiny over user-generated content and forum interactions like Roblox.

Highly sexual titles, often labelled NSFW (not suitable for work), are a mainstay on Steam's menus too – with some even free to play.

Yet, the platform has been criticised for its lax age verification, which simply asks users to declare a birth date before downloading a mature-rated game.

Prof Soon said there is a possibility that other platforms will fall under the code, which targets five dominant services in the market for the time being while the regulators figure out the most suitable age assurance methods.

The role of parents, too, cannot be understated in the quest to keep children away from online harms.

Experts said there is little stopping a parent from approving the installation of adult games, while others might not be aware of how children might try to game the system.

NUS' Prof Sim suggested the use of notifications to parents as a way to deter children from installing applications for adults.

App stores should alert parents through e-mail or a prompt each time their child requests to install a mature-rated app, the same way Instagram alerts the account holder when there is a log-in on a new device, Prof Sim added.

This is feasible, since most young people buy devices with the help of their parents, who can in turn be required to set up the device beside their child and implement notifications and other guard rails, he said.

"It will make children think twice," he said. "Parents also have an opportunity to talk to their children about the content they consume."

Prof Sim added: "If your child had a drinking problem, you'd want to talk to them. It works the same online."