Tech solutions to limit kids' access to social media are fraught with problems, including privacy risks

June 11 2024, by Lisa M. Given

Credit: Karolina Grabowska from Pexels

A campaign to block children's access to social media to limit online harm and unhealthy internet use is picking up momentum in Australian

politics. The current age limit for platforms such as Facebook, Instagram and TikTok is 13, but some state governments are calling for raising this age to 16.

Prime Minister Anthony Albanese has welcomed these efforts, and the federal opposition has committed to introducing laws that will bar under-16-year-olds from social media.

These calls are among the latest attempts to control how young people engage with culture. From banning children's books, to limiting television screen time, and rating music, movies and videogames, society often turns to government regulation to address moral panics.

Yet, critics explain the desire to control children's access is "not really backed by robust science". They raise privacy concerns about uploading personal documents (like passports) and providing details unrelated to age (like credit card numbers) to technology companies. Critics also highlight the social and informational benefits of online engagement, which may be lost if young people are banned.

These criticisms are valid, as age assurance technologies have a long way to go to address these concerns.

Is age verification even possible?

Many online sites currently rely on age gating, where users self-report their age. This can easily fail.

Children under 13 can provide fake birthdates to create social media accounts. And teenagers can simply tap "yes" when asked to verify if they're over the age of 18.

To prevent children from accessing inappropriate and harmful online

content, the federal government is already funding a trial of "age assurance" technologies.

Self-reporting is actually a type of age assurance. Other methods, including more rigorous age verification processes, are also available. However, none of them are foolproof or risk-free.

So how do age verification/assurance technologies work?

Several strategies are being used or tested to identify people's potential age.

- **User-provided age verification.** This asks users to upload "hard identifiers" (such as a passport or driver's license) as proof of age. While this approach is reliable, it excludes anyone who lacks appropriate identification.

- **Verified parental consent.** A parent verifies their age (via a hard identifier) and then confirms the age of a child user, and/or approves access on their behalf. This approach requires the involvement of a responsible adult, but raises concerns about young people's privacy.

- **Age estimation using behavioral data.** Artificial intelligence tools can build users' age profiles based on platform behaviors, such as analyzing the accounts they follow, posts they like and content they post. But these numeric age estimates may not match an individual's stage of development or literacy level, or even their actual age.

- **Age estimation using biometrics.** A user's age is estimated

based on biometric data (for example, facial scanning). This is a challenging approach, as facial recognition technologies are known to be biased and prone to errors.

Unfortunately, many of these approaches raise significant privacy concerns for users, not least because a third party (such as the social media company) would be handling their ID documents and other personal data.

While government-issued digital IDs may offer secure alternatives for age verification, many people may not hold passports, driver's licenses, or other types of "hard" documentation required for these services.

What do we lose by automating age verification?

While these technologies will improve over time, now is the time to decide whether age-based bans are what we need or want.

Society may agree that online adult content—such as pornography, gambling and alcohol sites—should be restricted by age. However, banning children from all social media may cause more harm than good.

Social media platforms provide vital pathways for young people to engage with peers and seek information for school, work and personal needs. For example, YouTube and LinkedIn are critical professional development and networking tools, often used in education. Would a social media ban only target specific tools, or apply to all platforms, regardless of purpose?

By enacting age-related bans and other restrictions across the board, without discretion or consideration for individual maturity, children's right to access information will also be curtailed.

From climate change to the housing crisis, health concerns and career goals, young people need access to reliable information and community networks. Yes, they will also watch cat videos and learn about the latest fashions. And they may, inevitably, encounter inappropriate content, trolls and bullies.

Social media—as with television, the internet and other media content—are best explored by children with the support of parents, teachers and other caregivers to guide their use.

While age assurance technologies may limit access to some adult content, these tools also restrict parental discretion to determine what is best for their children.

Appropriate social media use requires critical thinking and digital literacy skills—not only for children, but for parents and other caregivers. Government investment in educating parents and other caregivers on social media tools and safety practices would ensure families are well equipped to navigate our ever-changing social media landscape.

Provided by The Conversation