Age assurance: a perspective by Colm Gannon

The calls for stricter age verification mechanisms are growing louder. Driven in part by the frightening risks of online grooming, sexual extortion, exposure to pornography, nudify apps, cyberbullying, and a whole host of other digital harms that many of us in this space know all too well. In recent weeks, stakeholders and the media have asked me to share my thoughts on age assurance, as the topic is gaining significant interest.

As I write this, I realise that the carefree childhood I had, like many of us, without digital devices, feels like a golden age. I know from my own experience growing up that bullying ended at the front door of my house. Today, however, bullying and 24-hour online access can follow our children into their bedrooms and lives at any time, on any device, with no off switch.

Age verification concerns are valid, and at ICMEC Australia, we share the goal of protecting children from technology-enabled harm. However, when one in three internet users worldwide is under 18, we can't rely on age assurance as a default or standalone solution. It's not a silver bullet.

Everyone is watching Australia, and we have an opportunity to establish best practice. We have been pioneers in the past, having been early adopters of DNA profiling in criminal investigations. We have an opportunity to lead in this area by developing digital solutions that are both effective and respectful of children's rights.

It is my firm belief that age assurance is just one part of the puzzle and can't guarantee children's safety on its own. Consider the parents or carers, whether intentionally or not, who enable their children to bypass measures like this by sharing mobile devices, overlooking safety settings, or allowing unsupervised access. If you're a parent or carer, you're likely familiar with the panic of "Can you reset my phone for me?" or handing over your device to keep them entertained during a wait or car ride, without realising the full extent of what they can access.

In today's digital world, children can be both victims and active participants in harmful behaviour. The risks are diverse and growing. These include exposure to adult content on mainstream platforms, unsolicited explicit material such as nudify apps and airdrop abuse, and the algorithmic amplification of harmful trends on social media. They can be exposed to cyberbullying and coercion within peer networks. Increasingly, children are also being targeted for sexual extortion, and child sexual abuse material (CSAM) is being created, shared, or manipulated with AI-driven tools often without their knowledge or consent.

The scale is terrifying. In 2024, NCMEC (The National Centre for Missing & Exploited Children) received over 546,000 reports of online enticement, representing a 192% increase from the previous year. Reports involving AI-generated CSAM, surged by 1,325%, highlighting the growing misuse of generative AI technologies in exploiting children.

Age assurance technology can't resolve this complex landscape alone. Recent events in France, where VPN usage spiked after Pornhub suspended operations due to age verification laws, demonstrate how easily these technical barriers can be circumvented. What is needed is a coordinated, system-wide response that includes strong governance, digital literacy education, platform accountability, and built-in safety features, all working together to support the well-being of children and young people.

Poorly designed or rushed age assurance technologies could cause more problems than they aim to solve. They could undermine children's privacy, exclude vulnerable youth who lack connections to their peer networks, and create a false sense of security. We can't view children as passive users. They are rights-holders, digital citizens, with valuable insights into their own online experiences. To create a safer online environment, we must incorporate their voices into the development process.

It can't be left to tech companies alone

Technology can play a crucial role in child protection. However, we must protect children online based on what is best for the public. Governments, regulators, civil groups, and young people themselves should collaborate to design, implement, and oversee these systems.

Informed consent must be inclusive, especially for neurodivergent children

We need to create mechanisms that genuinely represent informed, child-friendly consent. This means acknowledging that neurodivergent children may understand or participate in consent processes in unique ways. Simplified or standardised interfaces can lead to confusion and restrict agency, especially for children with varying cognitive, sensory, or communication needs.

Biometric data and data sovereignty matter

I've emphasised in many stakeholder discussions that we need clear, transparent protocols around how biometric data is processed, retained, and protected. More broadly, where and how children's data is sourced, stored, and governed, especially in a cross-border context, is a fundamental question of data sovereignty. If data leaves Australian jurisdiction, what legal safeguards apply? Who owns it? Who can access it?

How does this align with the Children's Online Privacy Code?

Any age assurance technologies must be aligned with established frameworks, such as the Australian Children's Online Privacy Code. This involves evaluating whether data minimisation principles are being followed, ensuring that consent is obtained appropriately, and confirming that platforms are accountable for the use of children's data in compliance with Australian law.

Hardware integration and identity protocols require scrutiny

We need to assess if government-issued ID, device-level integration, and protocol exchanges are necessary, proportionate, and respectful of privacy. Robust doesn't have to mean invasive, and any solutions should minimise the burden on children and families while maximising safety and transparency.

Invest in digital literacy and education

Digital literacy should start early and adapt with children's growth. Technology is moving fast. It's not only about knowing how to use technology but also about understanding how to navigate risk, recognise manipulation, question content, and speak up when something feels unsafe. Education should cover the fundamentals: how algorithms shape what we see, what constitutes personal data and when to share it, how online consent works, and the clear steps to take when encountering inappropriate content. This is particularly important during key transition stages, or as I like to say 'education moments', like starting high school or joining new social platforms, when children are more likely to face unfamiliar digital risks. Investing in education helps children use digital spaces wisely. This is all about prevention.

Calls to ban children from social media or to restrict access based on strict age limits often ignore the fact that, for many young people, these platforms are essential for connection, identity, and support. Overly strict measures can have the opposite effect, increasing feelings of isolation and could push children toward less regulated and darker areas of the internet. Prohibition can lead to the evolution of harmful, unregulated behaviours. History shows us that blanket prohibitions often drive activities underground rather than achieving the intended harm protection.

To keep children safe online, we must remember that they're active participants in a digital world that influences many aspects of their lives. From school to social interactions, entertainment, and so on, technology is an integral part. When technology is created with people's needs in mind from the get-go, it can only have a positive impact on them. Together, we can build systems that promote safety, respect, and education.

Let's make sure that every digital space is one where children feel safe, valued, and supported.

But let's include them in the conversation.

Colm Gannon, CEO, ICMEC Australia

PS. I recently had a powerful conversation with Yasmin London on the Qoria platform about pornography's impact in schools. You can listen to the full discussion here