AUSTRALIAN RESEARCH COUNCIL
Centre of Excellence for the Digital Child.

22 September 2025

Submission to Environment and Communications References Committee

Internet Search Engine Services Online Safety Code

By the Australian Research Council Centre of Excellence for the Digital Child

With contributions from Amanda Cipriani, Dr Xinyu (Andy) Zhao, Dr Audrey Cooke, Dr Chris Zomer, Dr Giselle Woodley, Dr Kristy Corser, Professor Michael Dezuanni, Professor Tama Leaver.

About the Digital Child

The ARC Centre of Excellence for the Digital Child ('Digital Child') is charged with leading national and global research, policy and practice to ensure that all Australian children are healthy, educated and connected in a rapidly expanding digital world.

The Digital Child is shaping an environment with children, families, and communities so they can navigate their own digital worlds. We know that children's lived experiences are rapidly changing, and that every childhood is now fundamentally digital. Our mission is to create positive digital childhoods for every child in Australia.

We do this by focusing on:

- Healthy digital lives, understanding how digital technology intersects children's lived experiences and providing guidance to families, educators, and policymakers as they navigate this space.
- Educational empowerment, equipping children with the skills they need to live their best digital lives.
- Safe digital spaces, making online engagement safer while promoting healthy digital relationships.

This submission provides a brief response to the inquiry. We would be pleased to provide further information, including an oral submission.

Contact information

Dr Tara Roberson, tara.roberson@qut.edu.au

Response to specific areas

a. Privacy and data protection implications of age verification

Prominent child rights researchers have explored the implementation and challenges of age assurance systems to protect children online, focusing on the European context. They investigated the legal requirements for age assurance and examined the effectiveness of these systems in practice. Professor Sonia Livingstone from the London School of Economics and colleagues argue that current age assurance methods often fail to protect children adequately and may infringe on their other rights, such as privacy and non-discrimination.

Further, the Organisation for Economic Co-operation and Development (OECD)'s recent report reviewing the age assurance practices of 50 online services used by children indicated that many online age assurance practices are poorly enforced or easily circumvented.

The use of age assurance tools raises ethical and legal considerations around consent as they may contravene UNCRC principles relating to the collection of data or metadata from children. While some effort has been put in place to position the Online Safety Amendment (Social Media Minimum Age) Act 2024 as compatible with young people's rights, including privacy, the overall impact of age assurance has to be considered in light of the Phase 1 and Phase 2 codes, which add additional layers of age gating later in December 2025, and then in March 2026. Reassurances offered in relation to the first do not automatically apply to the Phase 2 codes in particular, which add additional requirements to age-verify adults to access restricted content such as legal pornography. The overall impact of all of these changes is very likely to impact on the privacy of all Australians, young and old.

The importance of privacy to young people is apparent. In the UK, 45.7% of young people surveyed used VPNS or anonymised browsers such as Tor, to overcome age gates, with another 22.9% aware of these technologies. Research conducted by eSafety found that Australian young people also felt proposed measures posed a serious threat to privacy. In forthcoming research (publication currently under review), privacy formed young people's primary concern, with 63% of those surveyed (total sample n=1004) apprehensive around the privacy of personal information. For those too young to consent, rights to digital privacy must also be respected.

Most assurance measures require the handing over of personal data to third party companies. Previous research has explored the significant risk this poses to privacy and interests of consensual and legal adult consumers too. This research cites scepticism over the reliability and efficacy of the proposed arrangements around third-party age verification services or governments preserving privacy and anonymity of its users when storing personal data securely. In an age where data is monetised and considered a valuable commodity; allowing third-parties to host such intimate and personal data raises justified security and privacy concerns for all Australian users.

b. The expansion of corporate data collection and user profiling capabilities enabled by code compliance requirements

The introduction of these technologies compounds pre-existing privacy concerns for children and young people with some platforms "over-anticipating" needs of regulators and keeping too much personal data on users. Encrypting data (whether in the form of temporary digital tokens or digital ID), still poses dangers around data retention or data leaks due to internal incompetence and malicious intent.

Data surveillance of children begins before they are born, and mobile applications aimed at parents (to be) play a key role in these processes. Children's data is collected from their earliest life-stages and "even before birth", as asserted by Australian Children's Commissioner Anne Hollonds– echoing arguments made by many academics researching children and technology (e.g. Barassi, 2020; Holloway, 2019; Mascheroni & Siibak, 2021) and by children's rights advocates (e.g. Children's Commissioner, 2018; Cannataci, 2021).

These digital practices contribute significantly to the vast amount of data being routinely collected about children, adding up to around "72 million data points before a child reaches the age of 13". Parents are often relied upon to make decisions that protect their children's data privacy. However, parents are often unable to provide meaningful consent regarding the sharing of their own and their children's personal data.

c. The technical implementation and efficacy of age verification and content filtering mechanisms

Existing age assurance software that enables age estimation (an approximation) or age verification (greater certainty) software is not close to successfully distinguishing between people who are under and over 16 years old. While it remains a common refrain in computer science that such systems simply require better training data, more sophisticated algorithms or other incremental improvement, research analysis has shown that age estimation solutions from facial scans demonstrate that automated processes such as these cannot ever be expected to achieve acceptable levels of accuracy. The recent report on the age assurance technologies trial demonstrates that these technologies continue to struggle when asked to distinguish the age of young people. The trial results indicate that ultimately the only way age can be clearly and efficiently determined by technology companies is to use government issued ID. This leads to privacy and security risks.

The Australian trial of technology for age assurance showed that these technologies are flawed. The tools are more likely to make errors in age estimation when users are in the target age range of 16 years and under and/or if they have an Indigenous or south-east Asian background. As the QUT Digital Media Research Centre highlights in their submission to this inquiry, studies consistently show high error rates, with significant racial, gender, and age biases. A Guardian analysis of the age assurance technology trial

data also shows the impact of introducing age checks will fall hardest on already-marginalised groups.

Age verification technologies will disproportionately affect children who are already marginalised. For instance, children without documentation or ID will be unable to verify their age once they reach 16. Children in rural areas will be further limited in their ability to connect with their peers. In other words, already marginalised groups will be disproportionately affected when this legislation comes into effect.

Age verification should be proportionate, privacy-respecting, rights-respecting and not intrusive. The IEEE 2089.1-2024 Standard for Online Age Verification establishes a framework for rights-respecting age verification systems, building on 5Rights' resource 'But how do they know it's a child?'. Systems should be designed in anticipation of their impact on family life as research has shown parents and children often find alternatives to, and can circumvent, verification systems. A balanced approach that prioritises children's rights, blending both the need to protect and enable access to digital opportunities is needed.

d. Alternative technical approaches to online safety for all users, including young people

Research shows that children can circumnavigate poorly enforced age testing mechanisms.

There is no ideal technical approach to age verification. Of the options discussed in the Australian report on age verification, the parental controls mechanism does at least allow a degree of autonomy for families who can determine when a child is ready for different content online.

An alternative to age verification is improving online spaces, equipping young people with digital skills, and providing support for families and communities. In addition, adopting a 'safety-by-design' approach can shape technical decisions in ways that support child-appropriate features, allowing them to continue accessing digital experiences without pushing children toward adult versions of the services.

There are four pillars we can focus on, as a society, to improve children's online experiences. First, we must set standards for high-quality digital experiences for children. Second, we need to engage in slow design and decision-making processes driven by consultation with children. Third, we must create child-centred regulation and policy, and, fourth, deploy media literacy policy and programs that help young people develop necessary skills to critique and explore the various media they consume. There are also concerns that such a movement will render Australian young people as less digitally literate than children in other countries. Australian young people themselves preference educational measures over age assurance and age verification technologies.

Services likely to be accessed by children should be expected to demonstrate how they have considered the best interests of the child. They should demonstrate what they have

done to ensure the best interests of the child informed the design, deployment and operation of their services.

e. Appropriate oversight mechanisms for online safety codes

The requirement for independent review of the operation of the social media minimum age legislation is built in. We suggest that similar reviews should also occur for upcoming industry codes. These reviews should include opportunities for community consultation and feedback. Evaluation of the Social Media Age Changes and the Phase 2 Industry codes should be done in tandem, looking at the overall impact of various forms of online age gating for Australians, weighing both technical aspects (does it work) and social impact (does it actually improve the experiences and wellbeing of young people).

Legislation in this area should be accompanied by a strong government investment in digital media literacy for children and families. Just as we teach children to swim, or stay safe in society more generally, children need to 'bridged into' adult social media, not dropped in it at age 16. The Australian Curriculum supports both Media Arts and Digital Technologies from Foundation to Year 10, providing appropriate opportunities for media and digital technology education for children and young people.

In particular, Media Arts plays an important role in developing the critical media literacies that young Australians need to thrive in digital media environments. As such, Media Arts within the Australian curriculum presents an opportunity for innovation in how we can support young people navigate social media use effectively.

It is important to ensure the codes do not prevent access to content that may be beneficial or educational for young people.

f. Global experience and best practice; and

Globally, other countries have attempted to restrict access to content deemed harmful with mixed results. In the United Kingdom, online platforms have implemented age verification methods to prevent children from accessing specific types of content. The new rules resulted in a significant surge (1400% for new sign-ups for one service) in the use of VPNs as people work to bypass the age checks. VPNs are proficient AT protecting online privacy, yet the surge in use in the UK has resulted in a crackdown on VPNs through further age verification checks. Users should be able to protect their privacy if desired.

The 5 Rights Foundation argues that age assurance should not be seen as an end in itself, but as part of a wider programme that allows a child to be a child online. They describe age assurance as a "necessary part of the border action to build the digital world that young people deserve".

The European Data Protection Board (EDPB) in February 2025 adopted principles to reconcile the protection of children's personal data in the context of age assurance, without limiting their access to online experiences. These principles highlight that the

best interests of the child must be prioritised while respecting all their rights, including privacy, access to information, and non-discrimination. Age-assurance measures should be risk-based, proportionate, and use the least intrusive methods with minimal data collection. Further, transparency must be provided so children and parents clearly understand how age assurance works and have ways to challenge faults.

g. Any other related matters

The Internet was not created with children in mind, but children still have a right to be online. Our goal as a society should not be to exclude children from online services rather, it ought to be about creating and facilitating high-quality experiences for children online, which can include social media that provides age-appropriate experiences. The recommendations our researchers provide in our Principles for a better Children's Internet report provide clear guidance on how the government can take realistic and measured steps to improve and support children's experiences online.

The challenges of age verification and/or age gating online spaces include:

Communicating about upcoming changes to parents, carers and communities: we have found that families do not understand what will change in December. Some are shocked to hear about developments. To this end, we are collaborating with eSafety on a project focused on communicating with multicultural communities. A key risk of the upcoming legislation is that it will increase the burden on parents and carers as they contend with an ever increasing number of platforms and services that rely on 'parental controls'. It is likely that as platforms seek to be exempt from the ban, they will develop 'age appropriate' versions of their services that over-rely on parental controls and child and parent negotiation regarding which features they are allowed to use (Principle 14). In regulatory terms, the government's plan to focus on a Digital Duty of Care, which requires platforms to evaluate the potential risks of their tools before they release them, is a much more productive legislative direction, placing the initial burden on platforms, not parents.

Communicating to children through schools and other means: we have found that schools are not currently talking to students about upcoming changes to online access. Children and young people, in general, are under-informed about the changes and how their existing accounts will be dealt with by platforms. In the same way that children and young people are diverse, so are their communication needs, styles, and preferences. Communication methods should be varied, adaptive, and creative to ensure that key messages are amplified, accessible, and best positioned to be understood and embraced by children and young people. This is also helpful in terms of supporting parents and other caring adults (such as teachers) to engage in dialogue with children and young people about these important matters. Methods might include: static multimodal information and live online and in-person discussions for children. Educators require sufficient training and support too.

Impacts on how young people seek health information: The new codes will affect each and every way young people connect to the internet when they seek sexual health

information. The industry codes are intended to protect. However, they risk endangering the ability of Australians to access essential information. This is especially important for the many young people who do not have access to comprehensive sexuality and reproductive health information at home or school. To uphold sexual rights to information, privacy and expression, the codes should ensure non-discriminatory access and require platforms to promote material that supports sexual health, rights and justice. In practice, this necessitates careful consideration of content in context.

Impacts on how parents and carers check-in with their children and young people: Changes to access to social media and search engines may give families the false impression that everything has been handled when it comes to online challenges and harms. The social media age restriction and other measures will not fully prevent those problems, for example messenger apps are excluded from the restriction despite posing a threat of cyberbullying. The government must support efforts to communicate with parents about the ongoing need to check in and support their children and young people. The restrictions may also reduce the individual autonomy and agency of families to discuss what content is removed and why certain content has been chosen to be restricted.

Highlighting risks not currently addressed: A range of those in the community currently aware of the ban and Phase 2 codes appear to believe it will 'solve' the problems of risks to young children, teens and others online. Even if age gating succeeds, many risks still persist. The challenges come with the global roll out of generative artificial intelligence tools can exacerbate many of the risks currently being discussed, including privacy, but also can make other risks (such as the prevalence of mis- and disinformation) considerably worse given their capacity to produce convincing sounding outputs of text, image, audio and now video. Arguably, the ban will also relegate young people to less regulated areas of the internet, where misinformation and other risks are likely to be more apparent. Indeed, previous research has found that adults and some children may be pushed towards VPNs, anonymised browsers to overcome measures, and have a higher likelihood of thus encountering illegal and extreme material that they may not otherwise have been exposed to. Addressing these risks requires a consistent focus on improving media and digital literacies, across formal and informal curriculum and other spaces, which must be deliberately increased to ensure young Australians are equipped to be successful digital citizens.