

20 June 2024

Committee Secretary
Joint Select Committee on Social Media and Australian Society
Via email: socialmedia.joint@aph.gov.au

Joint Select Committee on Social Media and Australian Society

The Alannah & Madeline Foundation (the Foundation) welcomes the opportunity to take part in the consultation of the Joint Select Committee. For too long, social media platforms and other digital platforms have been designed and functioned in ways which are inappropriate and even unsafe for children. System-level changes are needed to put children's best interests ahead of commercial gain.

The Foundation is a leading national not-for-profit charity dedicated to keeping children and young people free from violence and trauma. We support young Australians to recover and heal from trauma; we empower them to become positive digital citizens and change the culture of bullying; and we advocate for their rights, with particular attention to the issues of firearms safety and digital technologies.

The Committee's terms of reference invite comment on 'the use of age verification to protect Australian children from social media' and 'the algorithms, recommender systems and corporate decision making of digital platforms in influencing what Australians see, and the impacts of this on mental health'.

Given the consultation's tight timeframes and co-occurrence with the review of the Online Safety Act, we cannot respond in detail. However, we offer three directions which would help to lift the standard of protection for children's rights in the digital environment, including on social media platforms.

1. Support the planned provision for a Children's Online Privacy Code in the legislation to reform the Privacy Act 1988 anticipated for August 2024.
2. Support an enforceable requirement for digital platforms to treat the best interests of the child as a primary consideration in any decisions affecting children and to demonstrate this through child rights impact assessments. This requirement could sit within a wider 'duty of care' framework – see the current review of the Online Safety Act 2021.
3. Support the development of a regulatory scheme for the accreditation and oversight of age assurance providers, the need for which has been highlighted by eSafety.

Unsafe by design

Many of the risks to children's safety on social media platforms and other digital platforms stem from the platforms' underlying commercial models, which aim to maximise the handling of individuals' personal data in an 'attention economy'. This leads to design features intended to maximise the amount of time individuals spend on a service, their interactions on that service, and the reach of the service.

This is why social media platforms (and others) are highly engaging and difficult to stop using, connect people with ever-expanding networks, and reward content creation, interaction and popularity. Design features which serve these ends include notifications, popularity measures, affirmations (eg. likes), the 'infinite scroll', low-



privacy default settings, recommender systems, anticipation mechanisms (eg. dots to show someone is messaging you), ephemeral content, activity measures (eg. read receipts), cross-platform contact sharing, video autoplay, 'parasocial' relationships with famous influencers, and disguised advertising. Such features lead to children (and adults) spending excessive time on platforms, losing control of private information, connecting with strangers, and encountering extreme, inappropriate or 'echo-chamber' content. (5Rights, [2021](#) and [2023](#))

The need for systems-level change

In our [submission](#) to the review of the Online Safety Act 2021, we called for an enforceable requirement for providers of digital products and services to treat the best interests of the child as a primary consideration in any decisions affecting children. This commitment should be demonstrated through child rights impact assessments to identify, prevent and address threats to children's rights. Such a requirement could sit within a formalised 'duty of care' framework, as supported by the Parliamentary Committee on Social Media and Online Safety (2022). Safety standards could also be lifted by embedding a 'safety by design' approach within digital platforms and by making industry data about online safety available to regulators and researchers.

Meanwhile, we await the introduction of legislation in August 2024 to reform the Privacy Act 1988. We understand it will include planned provision for a Children's Online Privacy Code for all online services likely to be accessed by children under the age of 18, as proposed in the Privacy Act Review Report and agreed to by the Australian Government.

A high-quality Children's Online Privacy Code could force positive changes to social media platforms and other digital platforms in relation to children under 18. For example, a Code might require platforms to set children's accounts to private by default, switch off geolocation and profiling options by default, and not 'nudge' children to provide personal information, unless these things are in the best interests of the child. A Code could also require platforms to have age-appropriate mechanisms for children to report problems and seek help.

The Australian Government signalled that such an approach was possible in their response to the Privacy Act Review Report, where they gave in-principle support to proposals to prohibit trading in children's data and prohibit targeting and direct marketing to children unless it is in the child's best interests. The Government anticipated that a Children's Online Privacy Code would provide guidance on these matters. This is very welcome, as many risks to children online are driven or intensified by practices like targeting, where information relating to an individual is collected, used or disclosed in order to tailor services, content, information, advertisements or offers. Addressing such practices would speak to the strong public appetite in Australia for better privacy protections for children (OAIC, [2023](#)) and would have positive flow-on effects for safety.

To ensure children's best interests are put ahead of commercial gain, development of a Children's Online Privacy Code should be led by a trusted, expert, independent regulator such as the Privacy Commissioner, not by industry. The regulator must have capacity to meet the demands of this task, which would involve securing compliance from immensely wealthy international platforms – a major task. The experience of the UK, whose highly-regarded Children's Code may serve as a model for Australia, showed that many platforms made positive changes upon the Code's introduction but that adherence and transparency have been uneven in the long term. Guidance, monitoring and compliance mechanisms are essential. (5Rights/LSE [2024](#))

Regulating technological 'solutions' to age assurance

It is important Australia gets on the front foot in understanding and appropriately regulating new and emerging technologies, including those for age assurance. Age assurance is an umbrella term referring to a range of approaches that establish age to varying levels of certainty. It encompasses age verification, which uses 'hard' identifiers to establish age to a high level of certainty, and age estimation, which uses various approaches to establish that a user is likely to fall within a certain age category.



Age assurance can play a valuable role in relation to children's online safety. For example, General Comment 25 of the UN Convention on the Rights of the Child ('On children's rights in relation to the digital environment') articulates that states should use robust, safe and privacy-preserving age verification systems to prevent children from accessing products and services illegal for them to own or use eg. gambling. The Foundation welcomed the news that the eSafety Commissioner would pilot an age assurance trial aimed at preventing children's exposure to pornography. eSafety's proposed approach – tokenized, double-blind, informed by the euCONSENT model – sounds ethical and proportionate to the risks pornography poses to children.

However, age assurance is not a magic wand. It only identifies that a child is present; it does not make digital products or services safe or appropriate for children. Many digital platforms could bypass the need for age assurance by designing their products and services to be safe for children in the first place. In contrast, a social media platform whose main safety measure was age-gating to exclude under-16s might still be very unsafe for 16- and 17-year-olds to use. Social media age limits are no substitute for the wider changes necessary to build a better digital environment for all children under 18 – see the previous section.

That said, age assurance technologies might well have a significant future in Australia and it is vital to prepare for the associated challenges. Age assurance products and services are new and immature but evolving rapidly (5Rights, [2022](#); eSafety, [2023](#); ICO, [2022](#); ICO & Ofcom [2023](#)). Their development may well accelerate in response to various pieces of legislation overseas which require age assurance or verification in certain contexts eg. the UK's Online Safety Act, Germany's Youth Protection Act, multiple US state bills about online safety.

Regulation of age assurance has been poor. A report commissioned by the UK Information Commissioner observed 'These products have emerged largely in a standards lacuna.' (ICO & Ofcom [2023](#)) This creates a new set of risks to children eg. that companies will use age assurance technologies to maximise collection, sharing and use of children's personal information, including in potentially invasive areas like biometrics.

A comparable example is that of educational technology ('edtech') providers, whose products flooded suddenly into schools and homes during the pandemic with little expert oversight. Deep concerns have since emerged about their inappropriate handling of children's personal information. (Digital Futures Commission, [2022](#) and [2022a](#); Human Rights Watch, [2022](#); UNESCO, [2023](#)) It is important to avoid a repeat of this experience.

We support the position of 5Rights Foundation, a charity devoted to upholding children's rights in the digital environment, that any approach to age assurance needs clear guidance, standards and effective regulation to ensure efficacy, accuracy, security, privacy and accountability. In their roadmap to age verification in relation to pornography, eSafety highlighted the need for a regulatory scheme for the accreditation and oversight of age assurance providers in Australia to promote privacy, security, strong governance, transparency, trustworthiness, fairness, and respect for human rights.

We would be delighted to discuss any of these matters further with your team.

Yours sincerely,

Sarah Davies AM
Chief Executive Officer

