



Review of Online Safety Review 2021

Submission by the Alannah & Madeline
Foundation

June 2024

Contents

Executive summary	3
About us	4
Recommendations	4
The Office of the eSafety Commissioner	5
Voices of children and young people	6
Industry code development	6
Consultation on industry codes.....	8
Best interests of the child	8
Child rights impact assessments	9
Basic Online Safety Expectations Determination	10
Access to data.....	11
Age assurance	11

Executive summary

The Alannah & Madeline Foundation (the Foundation) welcomes the opportunity to contribute to the review of the Online Safety Act 2021 (the Act). When it was introduced, the Act represented a major step forward in legislating to address serious cyber bullying, image-based abuse, illegal content and adult content. It provided for the determination of Basic Online Safety Expectations for industry and the creation of codes to address industry's handling of illegal and restricted material.

All these directions remain important, but we believe several key reforms to the Act would strengthen Australia's approach to addressing new, emerging and persistent threats to children's safety online.

Firstly, the Foundation maintains **that industry safety codes created under the Act should be led by the Office of the eSafety Commissioner** in preference to the current 'co-regulatory' approach. The current approach has not delivered optimal outcomes for children; the processes have been lengthy and the final products inferior in several ways to overseas regulatory regimes. We have particular concerns about the next round of industry safety codes, focusing on 18+ material. Leadership of **code development by industry is inappropriate**, given how central such material is to the commercial models of some industry stakeholders. We strongly support the unique role of the eSafety Commissioner in upholding children's rights online.

Secondly, an updated Online Safety Act would be significantly enhanced by a stronger focus on the rights of the child across the board. This approach should include a requirement for industry to treat the best interests of **the child as a primary consideration** and to undertake child rights impact assessments in line with **international best practice**.

A **child rights approach** should also include stronger provision for engagement with children and young people, including in consultations like this one, to ensure they have a **meaningful voice** in the decisions that affect them.

Thirdly, we recognise the value of the (recently updated) Basic Online Safety Expectations Determination. This could be strengthened significantly if there were **enforceable requirements placed on industry** to implement the child safety expectations of the BOSE Determination.

Fourthly, the issues paper raises the topic of age assurance. Technological solutions to **age assurance can play a positive role in the wider picture of children's safety online** eg. by preventing children's access to products and services illegal for them to use or own. However, we emphasise that age assurance is not a 'magic wand' and does not, in itself, make the online world safe for children. Age assurance technologies are currently immature, but they are evolving rapidly and may escalate faster as overseas jurisdictions put various age-gating requirements into law. As such, we think it is crucial that Australia gets on the 'front foot' in regulating these new and emerging technologies, as recommended by eSafety, to prevent the further mishandling and exploitation of children's personal data.

Several additional steps could also be taken to deepen public engagement with the Online Safety Act and its outcomes – specifically, by **extending the public consultation periods for industry safety codes and by providing researchers and eSafety with broader access to data**.

Finally, while the Online Safety Act remains very valuable, it **does not address broader threats to children's safety which are inherent in the commercial models of many digital platforms** ie. the **monetising of children and their personal information**. The push to deepen user engagement and increase handling of personal information leads to many practices that can cause harm, eg. accounts set to 'public' by default; the personal, biometric and geolocation profiling of children; and the feeding of recommender systems which can connect children to age-inappropriate content and contacts.

To address such concerns effectively, any reforms to the **Online Safety Act must align with the promised Children's Online Privacy Code**. We strongly support the introduction of such a code and trust it will be led by an expert, independent regulator and backed by appropriate resourcing.

About us

The Foundation was established the year after the Port Arthur tragedy, by Walter Mikac AM in memory of his two young daughters, Alannah and Madeline. Our vision is that all children and young people are safe, inspired and have freedom to flourish.

Over the last 25 years our work has grown and evolved but our purpose remains the same. We have three program streams:

- **Safe and Strong: recovering and healing from trauma.** Linked to our origin story, we have a specialist trauma recovery and therapy service for children who have experienced significant trauma. This has grown in recent years to include working with early childcare providers, kindergartens, and now primary schools to help them build their trauma informed capability and practices. Most of our work in trauma healing and recovery is Victorian based, with our therapists and consultants working from our client's homes and places of work.
- **Safe and Strong: building positive digital citizens.** The Foundation supports schools, educators, families and communities nationally to build digital skills and competencies to develop a generation of safe and strong digital citizens. For over 12 years the Foundation has delivered eSmart, an initiative designed to empower children (3 - 18 years) to be safe and responsible online. It encompasses a range of learning tools and resources to help students build essential digital and media literacy skills, so they can thrive online.
- **Safe and Strong: bringing children's rights to life.** As a rights-based organisation, this is our policy and advocacy work. Since inception, we have advocated for firearms safety, and we convene the Australian Gun Safety Alliance. In other key policy matters related to our programs, we work closely with the Office of the eSafety Commissioner, the Prime Minister's National Office for Child Safety and other major agencies such as the Australian Federal Police.

In 2018, we partnered with Kate and Tick Everett, after the tragic suicide of their daughter, Dolly. With them we worked to establish Dolly's Dream.

- **Safe and Strong: Dolly's Dream, changing the culture of bullying.** The purpose is the same, but the programs and services (Parent Hub, telephone help line, school, and community workshops etc.) are specifically designed for remote, rural, and regional families and communities, to meet their unique needs and contexts.

Recommendations

1. Recognise the importance of the Office of the eSafety Commissioner in **upholding children's rights in the digital world** in line with the U.N. Convention on the Rights of the Child, General Comment 25.
2. Resource opportunities for **children and young people to engage meaningfully in this review**. This might involve eSafety's Youth Council, the Office for Youth's Youth Advisory Groups, or the Youth Advisory Group of the Victorian Information Commissioner. Relevant research into the views of children and young people has also been conducted through University of Sydney, UNICEF, Reset Australia, Western Sydney University, headspace, and eSafety.
3. **Reject the co-regulatory approach and empower the eSafety Commissioner** to lead the development of industry safety standards, including for Phase 2 of code development which concerns 18+ material.
4. Amend the Online Safety Act to require that the development of standards for industry must include a period of **public consultation of at least 60 days**.

5. Incorporate an **enforceable requirement for industry to treat the best interests of the child as a primary consideration** in any decisions which affect children. This requirement could sit within a formalised duty of care framework, as supported by the Parliamentary Committee on Social Media and Online Safety (2022).
6. Require industry to undertake **child rights impact assessments** to identify actual and potential adverse impacts on children's rights in relation to the digital environment and take appropriate steps to prevent, monitor, investigate and address these. These assessments should be shared publicly.
7. **Make enforceable the expectations of the Basic Online Safety Expectations Determination** which relate to children's rights in the digital environment, eg. expectations that relevant digital providers will ensure the best interests of the child are a primary consideration in the design and operation of any service likely to be accessed by children, and that providers will take reasonable steps to minimise harms and enable reporting of child cyber bullying, image-based abuse, child sexual abuse and exploitation material, and children's exposure to illegal material and 18+ material.
8. Put mechanisms in place to provide researchers and eSafety with access to industry **data relating to children's safety online**.
9. Pursue a **regulatory scheme for the accreditation and oversight of age assurance providers** to promote privacy, security, strong governance, transparency, trustworthiness, fairness, and respect for human rights, the need for which was identified by eSafety.
10. Pursue eSafety's recommendations for the Online Safety Act review in their **roadmap to age verification for online pornography**. This should include considering whether to extend various provisions of the Act to additional industry participants and whether existing legislation and regulation are sufficient to address children's exposure to pornography via emerging technologies such as generative AI and extended reality.

The Office of the eSafety Commissioner

The issues paper asks '*What features of the Act are working well, or should be expanded?*' One key feature of the Act is that it legislates the role of the eSafety Commissioner. The Foundation sees many of eSafety's functions as crucial to Australia's successful realisation of General Comment 25 of the U.N. Convention on the Rights of the Child ('On children's rights in relation to the digital environment'). For example:

- General Comment 25 urges states to ensure digital literacy is taught in schools and that parents and caregivers have opportunities to gain digital literacy in relation to children's safety online. This is progressed by eSafety's Trusted eSafety Provider Program, parent resources, Toolkit for Schools, and Best Practice Framework for Online Safety Education.
- General Comment 25 urges states to make available safe, free, confidential and responsive reporting mechanisms for violations of children's rights. This is progressed by eSafety's reporting schemes for child cyber bullying, image-based abuse, and online child sexual abuse material.
- General Comment 25 states that regularly updated data and research are crucial to understanding the implications of the digital environment for children's lives. This is progressed by eSafety's research into the online safety experiences of children, young people and parents.
- General Comment 25 urges that robust age verification systems be used to prevent children from accessing products and services that are illegal for them to own or use. This will be progressed by eSafety's planned pilot to prevent children's exposure to pornography via age assurance.

- General Comment 25 urges states to ensure businesses meet their obligations to prevent and remedy abuses of children's rights. This was progressed by eSafety's pressure on industry to lift child safety standards in codes developed under the Online Safety Act.
- General Comment 25 urges states to require a high standard of safety-by-design in the services and products children use, to minimise the risk of crimes against children. This is progressed by eSafety's Safety by Design initiative for digital providers.
- General Comment 25 urges states to involve children, listen to their needs and give due weight to their views when developing legislation, policies, programs, services and training on children's rights. This is progressed by the eSafety Youth Council, who share their insights on online safety issues with eSafety and Government.

No other regulatory body provides such support for the rights of children in the digital world.

Voices of children and young people

Children have a right to express their views freely on matters that affect them. General Comment No.25 of the U.N. Convention on the Rights of the Child states 'When developing legislation, policies, programmes, services and training on children's rights in relation to the digital environment, States parties should involve all children, listen to their needs and give due weight to their views.'¹

We trust this review will include engagement with eSafety's Youth Council and perhaps other bodies like the Office for Youth's Youth Advisory Groups (eg. 'Civic Engagement', 'Safe and Supported', 'Prevention of Gender-Based Violence') and the Youth Advisory Group of the Victorian Information Commissioner.

It is also valuable to refer to recent insights from Australian children and young people already provided to online safety researchers – see for example research from University of Sydney, UNICEF, Reset Australia, Western Sydney University and headspace, as well as the eSafety Commissioner.²

The Foundation is compiling Student Voice Insights Reports from workshops held at schools involved in our eSmart suite of offerings. For example, we recently consulted with 118 Years 1-3 students at a primary school in a Victorian city. The students expressed mixed feelings about the digital environment, seeing the internet as fun and useful but also involving dangers. They mentioned contact with strangers, scary content, hackers and scams, nasty comments, eye strain, and being online for too long. Social media was not a big theme, but many children were enthusiastic gamers, communicating with friends and strangers in gaming environments from a very young age. Using digital devices alone without adult supervision was common and older siblings were mentioned as role models. Their comments drew our attention to children's ability to learn safety tactics but also their vulnerability when navigating spaces not designed with their best interests in mind. For example, children spoke of looking up ratings in the app store, having backup accounts, 'being careful' when playing with strangers, not giving out phone numbers, and blocking people or leaving a digital environment if they felt unhappy. With more time, we would be glad to share further insights.

Industry code development

The issues paper asks '*Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the codes drafting process be improved?*' It also asks '*Does the Commissioner have the right powers to address access to violent pornography?*'

At present, Division 7 of the Online Safety Act states that bodies or associations representing the online industry should develop codes in relation to their online activities. The eSafety Commissioner can register a code if it provides appropriate community standards; if not, eSafety may determine an industry standard.

We do not support this 'co-regulatory' approach. It is our view that leadership by an independent, expert, trusted regulator would be preferable for several reasons:

- It is more likely to prioritise the rights of the child. A regulator accountable to the public is better placed than industry to create codes with the highest standards of ethics, privacy and safety for children. General Comment 16 of the U.N. Convention on the Rights of the Child ('On State obligations regarding the impact of the business sector on children's rights') recommends 'Strengthening regulatory agencies responsible for the oversight of standards relevant to children's rights ... so that they have sufficient powers and resources to monitor and to investigate complaints and to provide and enforce remedies for abuses of children's rights'.³
- It would align better with international good practice. For example, codes of practice and guidance for child-specific duties under the UK's Online Safety Act are being drafted by their communications regulator, Ofcom. Codes to address the use of children's personal information in the UK, Ireland, France, Sweden and the Netherlands were developed by state agencies or commissions.⁴
- It aligns with the approach to regulating other products and services that carry risks to children's safety. For example, mandatory safety standards for certain consumer products like children's toys and clothing are set by the Commonwealth under Australian Consumer Law.⁵ Safety standards for early childhood services are regulated under the National Quality Framework, set by all Australian governments and monitored by national and state regulators.⁶ Child Safe Standards for providers of services to children were developed by the Children's Commissioners and are regulated by public agencies. In some states like Victoria, the standards also apply to businesses which engage children in potentially high-risk ways, such as children's gym, play and sporting facilities; entertainment and party services; and photography, talent and beauty services.⁷
- eSafety has already demonstrated a commitment to lifting child safety standards in industry codes. For example, in 2023 eSafety sent several draft codes back to industry for redrafting. As a result, the final versions did more to address the risks of generative AI and contained slightly higher expectations about social media risk assessment, reporting of child sexual abuse material (CSAM) to law enforcement, and industry investments to address CSAM. eSafety also took over the development of industry standards for designated internet services and relevant electronic services. It seems likely these standards will lift expectations about generative AI and CSAM, industry complaints systems, and industry investments to address CSAM.

We recognise the Online Safety Act currently contains provision for eSafety to intervene if industry-drafted codes do not do enough to meet community safety standards. However, we do not believe this arrangement has been sufficient to deliver the best possible results for children. We have several concerns:

- Processes have been lengthy and complex. Initially it was anticipated that all codes would be registered by December 2022. As of June 2024, two Phase 1 standards are still pending and Phase 2 consultations have not yet commenced.⁸ We do not suggest inefficiency by eSafety; rather, it seems co-regulation has proven more laborious and conflicted than anticipated.
- The changes negotiated by eSafety, while positive, have still not brought Australia to the highest level of child protection. For example, eSafety's draft standards replicate industry's approach of setting high-privacy settings by default only for under-16s, rather than aligning with the definition of children as under-18s in the Online Safety Act and in children's data codes overseas.⁹ Unlike many overseas children's codes, Australia's codes are still not grounded in principles like 'the best interests of the child' or 'privacy and safety by design and default' across the board.¹⁰
- Phase 2 of code development will focus on limiting children's exposure to X18+ and R18+ material and to violent and fetish pornography. Under the current setup, code development will be led by industry representatives, including those digital providers whose services are most likely to contain 18+ material ie. pornography websites.¹¹

We have serious concerns about code development for 18+ material being led by industry. It was challenging to get adequate safety measures in place in the first round of codes, which focused on material like CSAM which is illegal and not part of industry participants' business models. We fear that building high

child safety standards into industry codes to address pornography will be a much harder ask, as these materials are fundamental to the business model of some legal and wealthy providers.

For example, eSafety states that MindGeek (now Aylo), owner of Pornhub, claims to get 115M+ daily visitors across their web properties, serving 3 billion+ advertising impressions. As of November 2022, Pornhub was the 14th most visited website in Australia. There are 13,600,000 monthly Google searches for 'pornhub' in Australia.¹² In 2018, MindGeek's annual revenue was estimated at over \$450 million USD.¹³

Under-18s, especially boys, are part of this market. According to eSafety, three-quarters of young Australians aged 16-18 have seen online pornography. Of these young people, 86% saw it before they turned 16, and 70% of exposure was via pornography sites.¹⁴ More than 10% of adolescent males in Australia view online pornography every day. Between a quarter and a half view it every week.¹⁵

It is hard to believe that any industry would choose willingly to exclude, reduce or dissuade such a valuable consumer base. This seems especially unlikely if one takes seriously research findings of a strong correlation between young age of first viewership and frequent use of pornography later in life.¹⁶

The prospect of industry-led safety codes here is unacceptable. There are high levels of community concern about the impact of online pornography on children. Concerns include the modelling of violent and degrading sexual behaviour; negative impacts on adolescents' mental health, body image and relationships; and the risk of compulsive use.¹⁷ (One study found 1 in 6 young Australian men believed they were 'addicted' to pornography.¹⁸) Other concerns exist about children's exploitation – e.g. the commercial handling of children's data and the role of child viewership in helping to drive an industry at the centre of serious concerns about image-based abuse, child sexual exploitation and trafficking.¹⁹

In their 'Roadmap to Age Verification', eSafety listed elements which should be considered in the review of the Online Safety Act to better prevent children's exposure to pornography.²⁰ We trust reviewers will follow up on these.

Consultation on industry codes

Sections 140 and 148 of the Online Safety Act state that the development of industry codes and standards must include a period of public consultation of at least 30 days.

We believe this time period is inadequate to enable meaningful participation by community members and not-for-profit providers, which often operate on very limited resourcing. The first round of industry code consultation was very challenging, as it involved reviewing and critiquing nine complex draft codes.

A longer required consultation period would align better with the U.N. Convention on the Rights of the Child, General Comment 12 ('The right of the child to be heard'), which states that all processes in which children are heard and participate must include 'Adequate time and resources ... to ensure children are adequately prepared and have the confidence and opportunity to contribute their views'.²¹

Best interests of the child

The issues paper asks '*Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?*' and '*Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?*' The Terms of Reference considers whether there should be a duty of care requirement towards users and/or requirements to ensure industry acts in the best interests of the child.

We strongly support the introduction of a requirement that industry should treat the best interests of the child as a primary consideration. At present, this is an expectation of the BOSE Determination but is not mandatory or enforceable in any consistent, serious way. This review provides an opportunity to go further.

The 'best interests of the child' principle is aimed at ensuring both the full and effective enjoyment of all rights and the holistic development of children. General Comment 14 of the UNCRC ('On the right of the child to have his or her best interests taken as a primary consideration') states that the following elements are to be taken into account: the child's views; the child's identity; preservation of the family environment and maintaining relations; care, protection and safety of the child; the child's situation of vulnerability; the child's right to health; and the child's right to education.²²

Treating the best interests of the child as a primary consideration means decision-makers recognise children's particular vulnerabilities and the need to give high priority to children's best interests, not treating them as just one of several considerations.²³

The best interests of the child is a guiding principle of the UK's Children's Code, Ireland's Fundamentals for a Child Oriented Approach to Data Protection, Sweden's 'Rights of Children and Young People On Digital Platforms', and the Netherlands' Code for Children's Rights, amongst others.²⁴

Potentially, a 'best interests of the child' obligation might sit within a broader duty of care requirement.

This approach would speak to the position of the Parliamentary Select Committee on Social Media and Online Safety (2022). The Select Committee expressed their support for a formalised framework for a duty of care, believing it would enhance the existing regulatory framework of the BOSE and give industry an incentive to ensure the safety of all users, notably children. The Select Committee anticipated that a formalised duty of care would include penalties for non-compliance and would incorporate the best interests of the child principle to 'ensure online platforms place this concept at the forefront when designing new products and updating existing services.'²⁵

Any duty of care framework should include requirements to assess and mitigate risks, appropriate powers and resourcing to ensure enforcement, and appropriate transparency and accountability measures.

Child rights impact assessments

A key step to ensuring the best interests of the child is treated as a genuinely meaningful guiding principle is to require industry to undertake child rights impact assessments (CRIAs).

The United Nations Committee on the Rights of the Child has urged Australia to require companies to undertake and share assessments of the impacts of their business activities on children's rights and their plans to address such impacts.²⁶ The expectation that states will require businesses to undertake child-rights due diligence is outlined in General Comment 16 of the U.N. Convention on the Rights of the Child ('On State obligations regarding the impact of the business sector on children's rights').²⁷

According to the U.N. Guiding Principles on Business and Human Rights and the Children's Rights and Business Principles, the process should involve businesses identifying and addressing actual and potential adverse impacts on children's rights; integrating the findings into their internal functions; taking appropriate action to address, prevent and mitigate impacts; monitoring the effectiveness of their actions; and being prepared to communicate their efforts externally.²⁸

Requirements for CRIAs should apply to the providers of digital products and services too. General Comment 25 of the U.N. Convention on the Rights of the Child reiterates that states should require businesses to undertake child rights impact assessments, disclose them publicly, and take appropriate steps to prevent, monitor, investigate and address child rights abuses – 'with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children.'²⁹

Organisations calling for CRIAs in relation to the digital environment include the U.N. Committee on the Rights of the Child, Council of Europe, UNICEF, LEGO, Millicom, Safaricom and 5Rights Foundation. Others who refer to the importance of CRIAs include International Telecommunication Union, the Broadband Commission for Sustainable Development, the European Network of Ombudspersons for Children, and the European Network of Youth Advisers.³⁰

We understand UNICEF is working to develop global guidance and a toolkit to support the integration of children's rights within the work of businesses to identify their human rights impacts in relation to the digital environment. Their project aims to build CRIA capacity among industry players and to promote the adoption of CRIA processes in relation to the digital environment.³¹

Requiring digital providers to identify and act on threats to children's rights would also align with Australia's National Principles for Child Safe Organisations. The National Principles highlight the importance of organisations having frameworks, strategies, processes and tools to prevent, identify and mitigate risks to children; engaging children and young people in risk identification; and ensuring proactive risk identification and mitigation by staff and volunteers.³² In their 2022 report, the Parliamentary Select Committee on Social Media and Online Safety expressed support for applying the National Principles for Child Safe Organisations explicitly to digital media platforms.³³

There are overseas precedents for requiring businesses to assess and address threats to children's rights in the digital environment. Children's data privacy codes in the UK, Ireland, Sweden and the Netherlands require industry to conduct data protection impact assessments in order to minimise the risks to children that arise from the processing of their personal information.³⁴ This speaks to requirements by the Council of Europe and the EU's Digital Services Act.³⁵

Meanwhile, the UK's Online Safety Act requires services likely to be accessed by children to undertake a children's risk assessment, identifying the possible harms and how these will be mitigated, with a focus on priority content – suicide, self-harm, eating disorders.³⁶ While a narrower approach than a CRIA, this is still an important step.

While child safety impact assessments are now built into the BOSE Determination as reasonable steps to uphold the best interests of the child, they are not yet required or enforceable. We believe they should be.

Basic Online Safety Expectations Determination

The Basic Online Safety Expectations (BOSE) Determination sets out the Government's minimum user safety expectations of social media services, relevant electronic services and designated internet services. The issues paper asks '*Should the Act have strengthened and enforceable Basic Online Safety Expectations?*' We would welcome such an approach with regard to children's safety.

At present, there is no legally enforceable requirement for service providers to implement the expectations of the BOSE Determination, although eSafety can require services to report on what they are doing to comply.

In practice, this reduces the pressure on industry to show that they are taking steps to minimise and enable reporting of child cyber bullying, image-based abuse, child sexual abuse and exploitation material, and children's exposure to illegal material and 18+ material.

We welcomed the recent decision by the Australian Government to strengthen the BOSE Determination by inserting a new expectation that digital providers will take reasonable steps to ensure the best interests of the child are a primary consideration in the design and operation of any service likely to be accessed by children. The updated Determination also includes welcome new expectations that digital providers will take steps to protect their users' safety in relation to generative AI and recommender systems.

These changes are welcome but under the current system their impact is likely to be uneven. Greater accountability for industry would help deliver stronger outcomes and would align better with General Comment 25 of the U.N. Convention on the Rights of the Child, which urges 'States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services.' [our emphases]³⁷

Access to data

The issues paper asks *'Should there be a mechanism in place to provide researchers and eSafety with access to data? Are there other things they should be allowed access to?'*

We believe researcher access is essential to improving accountability and transparency of the digital industry. We also urge that services be required to report on how they have assessed and acted to uphold the best interests of the child.

This approach would enable Australia to demonstrate strong alignment with the following standards:

- Principle 1 of the National Principles for Child Safe Organisations ('Child safety and wellbeing is embedded in organisational leadership, governance and culture').³⁸ One indicator is an organisation's ability to demonstrate that it has publicly available and current documents, including risk management strategies.³⁸
- General Comment No.25 of the U.N. Convention on the Rights of the Child, which urges states to require the business sector to disclose their child rights impact assessments to the public.³⁹
- The U.N. Committee on the Rights of the Child's observations on Australia, which urged Australia to require companies to make full public disclosure of the child rights impacts of their business activities and their plans to address such impacts.⁴⁰

Such an approach is being adopted in the UK, where the Online Safety Act requires large digital platforms likely to be accessed by children to make public summaries of their children's risk assessments. Some services must also summarise in a publicly available statement their approach to age assurance in relation to preventing children's access to pornography.⁴¹

Age assurance

The issues paper asks *'What role should the Act play in helping to restrict children's access to age inappropriate content (including through the application of age assurance)?'*

Age assurance could play a valuable role in the bigger picture of children's online safety. For example, General Comment 25 of the U.N. Convention on the Rights of the Child 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.⁴² The Foundation welcomed the news that the eSafety Commissioner would be funded to pilot an approach to trial age-assurance to prevent children's exposure to pornography. eSafety's proposed approach (tokenized, double-blind, informed by the euCONSENT) sounds ethical and sound.⁴³

However, age assurance does not, in itself, make children safe online; it only identifies that a child is present.⁴⁴ Age assurance does not make digital platforms child-safe, nor does it fix the risks to children's safety inherent to the commercial models of many digital platforms, which focus on maximising user engagement and data handling. To change this picture, a Children's Online Privacy Code is needed, led by an expert independent regulator and underpinned by appropriate resourcing.

Meanwhile, it is important that Australia prepares for the future challenges posed by the evolution of age assurance technologies. Technological solutions to age assurance – while new and immature – are evolving rapidly. 5Rights Foundation described age assurance as 'a fast-changing area with a growing market', predicting that research and investment in new solutions is likely to accelerate.⁴⁵ A report commissioned for the UK Information Commissioner found there has been significant recent growth in age assurance products

* While not mandatory, the National Principles enable organisations, including businesses, to show their commitment to child safety.

and services: 'age assurance technologies are still in their relative infancy and evolving rapidly'.⁴⁶ Examples of approaches under development include voice estimation technologies and biometrics using fingerprints, palmprints, hand-geometry and digit prints.⁴⁷ The eSafety Commissioner notes that industry players like Roblox, Google, Yubo and Meta have trialled, or announced their intention to trial, various approaches for specific products, via ID scans, selfies, and facial age estimation technology. eSafety concludes 'the age assurance market is immature but developing. Each technology has benefits and trade-offs'.⁴⁸

Overseas developments may put some digital providers under pressure to present more effective age assurance 'solutions'. For example, in the U.S. various state bills have been passed or proposed which include requirements for age assurance for social media use.⁴⁹ Meanwhile, the UK's Online Safety Act requires online services to use effective age verification and/or estimation to prevent children from encountering pornography and high-risk content.⁵⁰ In Germany, the Youth Protection Act mandates the use of age verification systems for age-restricted content like pornography.⁵¹

Such developments could create the conditions for new age assurance 'solutions' to be developed and brought to market. However, at present age assurance is poorly regulated. This creates its own set of risks to children's rights eg. that new technologies will be used by companies to maximise data collection, including in invasive areas like biometrics. 5Rights Foundation urges that age assurance needs clear guidance, standards and effective regulation to ensure efficacy, accuracy, security and privacy, backed by a regulatory framework with robust oversight and accountability.⁵² A report on age assurance commissioned for the UK Information Commissioner found that further standards development is needed: 'These products have emerged largely in a standards lacuna.'⁵³

Meanwhile, eSafety has stated that Australia will need a regulatory scheme for the accreditation and oversight of age assurance providers, to promote privacy, security, strong governance, transparency, trustworthiness, fairness, and respect for human rights.⁵⁴

It is important Australia gets on the 'front foot' in regulating new and emerging technologies – for example, to avoid a repeat of the widespread mishandling of children's personal data that has occurred in the 'edtech' sector.

We would welcome the opportunity to discuss any of these matters further. Please contact:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

¹ United Nations Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment,' 2021, <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

² eSafety, 'Mind the Gap: Parental awareness of children's exposure to risks online,' 2022, <https://www.esafety.gov.au/sites/default/files/2022-02/Mind%20the%20Gap%20-%20Parental%20awareness%20of%20children%27s%20exposure%20to%20risks%20online%20-%20FINAL.pdf> ; headspace, 'Youth Mental Health Statistics', especially '2022 Insights: social media' and

- '2020 insights: experiences of cyber bullying over time,' <https://headspace.org.au/our-impact/evaluation-research-reports/youth-mental-health-statistics/>; J. Humphry, O. Boichak, J. Hutchinson, 'Emerging Online Safety Issues – Co-creating Social Media with Young People – Research Report,' University of Sydney, 2023, https://ses.library.usyd.edu.au/bitstream/handle/2123/31689/USyd_Emerging%20Online%20Safety%20Issues_Report_WEB.pdf?sequence=3&isAllowed=y; L. Moody, L. Marsden, B. Nguyen and A. Third, 'Consultations with young people to inform the eSafety Commissioner's Engagement Strategy for Young People', Young and Resilient Research Centre, Western Sydney University, 2021, https://www.esafety.gov.au/sites/default/files/2022-01/YRRC%20Research%20Report%20eSafety%202021_web%20V06%20-%20publishing_1.pdf; Reset Australia, 'Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions,' 2023, <https://au.reset.tech/news/young-people-s-submission-to-the-inquiry-into-international-platforms/>; Reset Australia, 'Young People and Online Privacy,' 2023, <https://au.reset.tech/news/report-realising-young-peoples-rights-in-the-digital-environment/>; UNICEF Australia, 'Protecting children in the online world: reshaping the digital world for Aussie kids,' 2024, https://assets-us-01.kc-usercontent.com/99f113b4-e5f7-00d2-23c0-c83ca2e4cfa2/6cde226b-23d1-413a-bac3-7f0eafe524d4/UA_Digital-Wellbeing-Position-Paper-2024_LR_FINAL.pdf
- ³ United Nations Convention on the Rights of the Child, 'General comment No. 16 (2013) 'On State obligations regarding the impact of the business sector on children's rights,' 2013 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=5&DocTypeID=11
- ⁴ 5Rights Foundation, 'Approaches to children's data protection: a comparative international mapping,' 2022 <https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf>; UK Government, 'Online Safety Act: explainer,' 2024, <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>
- ⁵ Australian Competition & Consumer Commission, 'Product safety,' 2024, <https://www.accc.gov.au/consumers/protecting-yourself/product-safety>; Commonwealth of Australia, 'Consumer products safety: a guide for businesses and legal practitioner,' 2022, <https://consumer.gov.au/sites/consumer/files/inline-files/acl-guidance-consumer-product-safety.pdf>; Product Safety Australia, 'Australian Consumer Law,' accessed 2024, <https://www.productsafety.gov.au/product-safety-laws/legislation/australian-consumer-law>
- ⁶ Australian Children's Education and Care Quality Authority, 'Guide to the NQF,' <https://www.acecqa.gov.au/national-quality-framework/guide-nqf>
- ⁷ For example, Victorian Commission for Children and Young People, 'Regulating the Standards,' <https://ccyp.vic.gov.au/child-safe-standards/regulating-the-standards/> and 'Who do the Standards apply to?' <https://ccyp.vic.gov.au/child-safe-standards/who-do-the-standards-apply-to-page/>
- ⁸ eSafety, 'Development of industry codes under the Online Safety Act: position paper,' September 2021, <https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf>
- ⁹ 5Rights Foundation, 'Approaches to children's data protection: a comparative international mapping'
- ¹⁰ 5Rights Foundation, 'Approaches to children's data protection: a comparative international mapping'
- ¹¹ eSafety, 'Development of industry codes under the Online Safety Act: position paper'
- ¹² eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography,' March 2023, https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf
- ¹³ Office of the Privacy Commissioner of Canada, 'Investigation into Aylo (formerly MindGeek)'s Compliance with PIPEDA,' 2024, <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2024/pipeda-2024-001/>
- ¹⁴ eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography'
- ¹⁵ Shireen Bernstein, Wayne Warburton, Kay Bussey & Naomi Sweller, 'Mind the Gap: Internet Pornography Exposure, Influence and Problematic Viewing Amongst Emerging Adults,' *Sexuality Research and Social Policy*, March 2022, <https://link.springer.com/article/10.1007/s13178-022-00698-8>; Maree Crabbe, Michael Flood, Kelsey Adams, 'Pornography exposure and access among young Australians: a cross-sectional

- study,' *Australian and New Zealand Journal of Public Health*, 2024, <https://www.sciencedirect.com/science/article/pii/S1326020024000104#:~:text=The%20median%20age%20or%20first,daily%20and%20weekly%20use%20respectively.> ; Longitudinal Study of Australian Children, 'Teenagers and Sex,' 2019 <https://growingupinaustralia.gov.au/research-findings/annual-statistical-reports-2018/teenagers-and-sex>
- ¹⁶ Bernstein et al, 'Mind the Gap: Internet Pornography Exposure, Influence and Problematic Viewing Amongst Emerging Adults'; eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography' ; UK Children's Commissioner, 'A lot of it is actually just abuse' Young people and pornography,' 2023, <https://assets.childrenscommissioner.gov.uk/wpuploads/2023/02/cc-a-lot-of-it-is-actually-just-abuse-young-people-and-pornography-updated.pdf>
- ¹⁷ eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography' ; UK Children's Commissioner, 'A lot of it is actually just abuse' Young people and pornography'
- ¹⁸ Bernstein et al, 'Mind the Gap: Internet Pornography Exposure, Influence and Problematic Viewing Amongst Emerging Adults'
- ¹⁹ Nicholas Kristof, 'The Children of Pornhub', *New York Times*, 2020, <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>; Nina Lakhani, 'Internet porn executives resign after revelations the company's sites hosted underage videos,' *The Guardian*, 22 June 2022, <https://www.theguardian.com/society/2022/jun/22/pornhub-executives-resign-mindgeek-underage-videos>; Office of the Privacy Commissioner of Canada, 'Investigation into Aylo (formerly MindGeek)'s Compliance with PIPEDA'; United States Attorney's Office Eastern District of New York, 'Pornhub Parent Company Admits to Receiving Proceeds of Sex Trafficking and Agrees to Three-Year Monitor,' 2023, <https://www.justice.gov/usao-edny/pr/pornhub-parent-company-admits-receiving-proceeds-sex-trafficking-and-agrees-three-year>
- ²⁰ eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography'
- ²¹ United Nations Committee on the Rights of the Child, General Comment No. 12, 'The right of the child to be heard', 2009, <https://www.ohchr.org/en/treaty-bodies/crc/general-comments>
- ²² United Nations Committee on the Rights of the Child, 'General comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration,' 2013, pp.9, 13-17 https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf
- ²³ United Nations Committee on the Rights of the Child, 'General comment No. 14', p.10
- ²⁴ Reset Australia, 'Best interests & targeting: implementing the Privacy Act Review to advance children's rights,' policy briefing, 2024, <https://au.reset.tech/uploads/Best-Interests-Report-240128-digital.pdf>
- ²⁵ Select Committee on Social Media and Online Safety, 'Social Media and Online Safety,' March 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report
- ²⁶ United Nations Convention on the Rights of the Child, Committee on the Rights of the Child, 'Concluding observations on the combined fifth and sixth periodic reports of Australia,' 2019, <https://www.ohchr.org/en/documents/concluding-observations/committee-rights-child-concluding-observations-combined-fifth-and>
- ²⁷ United Nations Convention on the Rights of the Child, 'General comment No. 16 (2013) 'On State obligations regarding the impact of the business sector on children's rights,' 2013 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=5&DocTypeID=11
- ²⁸ UNICEF, the Global Compact and Save the Children, 'Children's Rights and Business Principles,' 2012, <https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf>; UNICEF, 'Child Rights Impact Assessments in Relation to the Digital Environment: Developing global guidance,' 2024, <https://www.unicef.org/reports/CRIA-responsibletech>
- ²⁹ United Nations Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment'
- ³⁰ Sudeshna Mukherjee, Kruakae Pothong and Sonia Livingstone, Digital Futures Commission, 'Child Rights Impact Assessment: A tool to realise child rights in the digital environment,' 2021, <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf>

-
- ³¹ UNICEF, 'Child Rights Impact Assessments in Relation to the Digital Environment: Developing global guidance,' 2024, <https://www.unicef.org/reports/CRIA-responsibletech>
- ³² Australian Human Rights Commission, 'National Principles for Child Safe Organisations,' 2018, https://childsafefoundation.gov.au/sites/default/files/2019-02/National_Principles_for_Child_Safe_Organisations2019.pdf See Principles 1, 2, 5, and 8.
- ³³ Select Committee on Social Media and Online Safety, 'Social Media and Online Safety'
- ³⁴ 5Rights Foundation, 'Approaches to children's data protection'
- ³⁵ 5Rights Foundation, 'Approaches to children's data protection'; Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Terms of Reference,' 2024
- ³⁶ Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Terms of Reference,' 2024
- ³⁷ United Nations Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment'
- ³⁸ Australian Human Rights Commission, 'National Principles for Child Safe Organisations'
- ³⁹ United Nations Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment'
- ⁴⁰ United Nations Convention on the Rights of the Child, Committee on the Rights of the Child, 'Concluding observations on the combined fifth and sixth periodic reports of Australia'
- ⁴¹ 5Rights Foundation & Fieldfisher, 'The Online Safety Act: a comparative legal analysis of the provisions for children,' 2023, <https://5rightsfoundation.com/uploads/5rights-fieldfisher-legal-analysis-osa-final.pdf>
- ⁴² United Nations Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment'
- ⁴³ eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography'
- ⁴⁴ 5Rights Foundation, 'Age Assurance and the new regulatory landscape: 5Rights updated report "But how do they know it is a child?"', <https://5rightsfoundation.com/in-action/age-assurance-and-the-new-regulatory-landscape-5rights-updated-report-but-how-do-they-know-it-is-a-child.html>
- ⁴⁵ 5Rights Foundation, 'Age Assurance and the new regulatory landscape: 5Rights updated report "But how do they know it is a child?"'
- ⁴⁶ Age Check Certification Scheme, commissioned by the Information Commissioner's Office, 'Measurement of Age Assurance Technologies,' 2022, <https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf>
- ⁴⁷ Digital Regulation Cooperation Forum, 'Measurement of Age Assurance Technologies,' 2023, <https://www.drcf.org.uk/publications/papers/measurement-of-age-assurance-technologies>
- ⁴⁸ eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography'
- ⁴⁹ National Conference of State Legislatures, 'Social Media and Children 2023 Legislation,' 2024, <https://www.ncsl.org/technology-and-communication/social-media-and-children-2023-legislation#:~:text=Arkansas%20created%20the%20Social%20Media,for%20illegal%20retention%20of%20ata.>; U.S. Senate Committee on Commerce, Science & Transportation, 'Sens. Cruz, Schatz Lead Colleagues With New Bill To Keep Kids Safe, Healthy, and * * * Off * * * Social Media,' 1 May 2024, <https://www.commerce.senate.gov/2024/5/sens-cruz-schatz-lead-colleagues-with-new-bill-to-keep-kids-safe-healthy-and-off-social-media>
- ⁵⁰ Fieldfisher and 5Rights Foundation, 'The Online Safety Act: a comparative legal analysis of the provisions for children,' 2023, <https://5rightsfoundation.com/uploads/5rights-fieldfisher-legal-analysis-osa-final.pdf>
- ⁵¹ Online Safety Act review consultation paper
- ⁵² 5Rights Foundation, 'Age Assurance and the new regulatory landscape: 5Rights updated report "But how do they know it is a child?"'
- ⁵³ Age Check Certification Scheme, commissioned by the Information Commissioner's Office, 'Measurement of Age Assurance Technologies'
- ⁵⁴ eSafety, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography'