alannah & madeline foundation

Phase 2 online safety codes for industry

Submission by the Alannah & Madeline Foundation

November 2024

Contents

Executive summary

The Alannah & Madeline Foundation (the Foundation) welcomes the opportunity to comment on the Phase 2 draft codes for industry under the Online Safety Act 2021. eSafety envisaged that these codes would help prevent and reduce children's risk of exposure to adult content – notably pornography, self-harm content and simulated gambling, as well as R18+ content.

We welcome the shift towards systems-based solutions to online risks and harms, including through industry codes. For too long, responsibility for avoiding harm online was left to parents, schools and children themselves, an inadequate and unjust approach.

There is deep concern in the community about children's exposure to adult material online and a strong public appetite for effective action to prevent and reduce this problem. However, there is also strong concern about new risks to children if measures like age assurance are not handled appropriately. Children should be protected from high-risk material without losing their rights to privacy, protection from exploitation, and freedom to participate in the digital environment.

The Online Safety Act 2021 states that the eSafety Commissioner's decision to register or reject a draft industry code rests partly on whether or not the draft code provides 'appropriate community safeguards'.

If, using their technical and regulatory expertise, eSafety assesses that the draft codes are unlikely to lead to children's rights being upheld meaningfully and in full, we believe eSafety should decline to register the draft codes and should require either redrafting or replacement by regulator-led industry standards.

We argue such an approach would be in line with General Comment 25 of the UN Convention on the Rights of the Child, as well as community sentiment in Australia.

The draft codes contain several positive indicators, including:

- Objectives 1 and 2, which replicate the 'Matters' in eSafety's position paper.
- Definition of a child as 'an Australian end-user under the age of 18 years'.
- Abandonment of Phase 1 categories of 'young Australian child' and 'children's interactive devices'.
- Requirement that social media services, relevant electronic services and designated internet services will estimate the likelihood that a child will access or be exposed to high-impact adult material on their services, as part of their risk assessment process.
- Recognition that appropriate age assurance can help prevent children's exposure to adult material.
- Requirement that age assurance measures show technical accuracy, robustness, reliability and 'fairness', and limit circumvention where reasonably possible.
- Requirement that some services provide tools and default settings to promote safety.

However, to uphold children's rights, we maintain the draft codes need the following:

- A stronger commitment that age assurance measures will be rights-respecting, user-friendly and proportionate to risk, with a data minimisation approach which protects children's privacy.
- Clearer alignment with the understanding of pornography articulated by eSafety, which recognises the impacts of new technologies like generative AI.
- Appropriately robust default safety settings for all digital products and services likely to be used by children, not just those which formally permit high-impact material.
- More in-depth approaches to risk assessment in relation to children's rights.
- Appropriate safety tools and settings offered to families with children under 18, not just under 13.
- A more meaningful commitment to community engagement, especially with young people.

We believe the above issues must be addressed appropriately before the codes are registered by eSafety.

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, 24/7 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

We support the role of the eSafety Commissioner as regulator and the approach outlined in eSafety's position paper. We would support an intervention by eSafety to lift protections for children's rights in the codes, including taking over development of industry standards if necessary.

For now, we urge industry leaders to work with eSafety to strengthen the draft codes in the following ways:

All codes:

1. Clarify that appropriate age assurance measures should be proportionate to risk, user-friendly, and take a data minimisation approach, handling personal information only to the extent necessary to provide the elements of a service with which an end-user is actively and knowingly engaged.

2. Expand the definition of pornography (and measures to address it) to align with eSafety's proposed framing of material which includes 'realistically simulated, generated and animated sexual content; high-impact text-based sexual content, including interactive services such as chatbots and AI models providing pornographic content; and high-impact nudity'.

3. Require appropriately robust default safety settings for all products and services likely to be used by children. (For example, we do not support the approach of the draft code for social media services, which limits high default protections to services which permit high-impact pornography and/or self-harm material officially.)

4. For purposes of assessing risks to children, provide high-quality guidance about how to estimate whether 'a significant number of Australian children' is likely to access a service.

5. Require industry participants to report publicly and accessibly on how they have assessed risks to children that may occur on their products or services and the steps taken to prevent and reduce these risks.

6. Strategise further to prevent and reduce the risks of image-based abuse through 'nudifying apps'.

7. Engage meaningfully with young people eg. through the eSafety Youth Advisory Council.

8. Extend the minimum consultation period for future drafts of revised codes to at least 60 days and extend the current consultation similarly.

9. Commit to a high-quality approach to prevent and reduce children's exposure to R18+ violent content.

Designated internet services:

10. Confirm that the category of 'high impact class 2 generative AI DIS' includes all 'nudifying apps' ie. covering generation of high-impact nudity material as well as high-impact sexual material.

App distribution services:

11. Further clarify that services have a responsibility to help prevent and reduce children's access and exposure to 'high impact class 2 generative AI DIS' eg. 'nudifying apps'.

12. Require a more in-depth approach to assessing risks to children, if advised by eSafety.

Equipment services:

13. Review whether the proposed approach to age assurance aligns with eSafety's emphasis on the importance of an 'ecosystems' approach.

14. Require that options for child accounts on shared devices be offered to families with children under 18, not just under 13.

15. Require a more risk- and outcomes-based approach to assessing risks to children, if advised by eSafety.

16. If the Tier 1-3 risk assessment process is retained, clarify the risk level of desktop computers.

Hosting services and internet carriage services:

17. Require a more in-depth approach to assessing risks to children, if advised by eSafety.

Internet search engine services:

18. Require that optional parental controls be offered to families with children under 18, not just under 13.

The need to prevent and reduce children's exposure to adult material

eSafety articulated that the Phase 2 codes should focus on the following matters:

- Protect and prevent children in Australia from accessing or being exposed to class 1C and class 2 material* [X18+ material, R18+ material including simulated gambling in video games, and fetish pornography material]; and –
- Provide end-users in Australia with effective information, tools and options to limit access and exposure to class 1C and class 2 material.[1]

We were pleased to see these matters articulated as Objectives 1 and 2 of the draft industry codes.[2]

Children are vulnerable to various harms in the digital environment. There is strong community concern about children's exposure to age-inappropriate content and adult sites.[3]

Concerns about pornography include the modelling of violent and degrading sexual behaviour; negative impacts on adolescents' mental health, development, body image and relationships; harm to the social fabric of school communities; and risks of compulsive use.[4]

Other age-inappropriate content also raises concerns. Studies from the UK have illuminated how engaging with self-harm material can become an immersive and destructive 'cycle' for some adolescents, while viewing violent content has become frighteningly normalised even among primary school students.[5]

Immediate harm to individuals is not the only issue. We are also concerned about exploitation of children in the long term eg. when recommender systems feed children age-inappropriate content in a commercial push to capture their attention and data; when child viewership helps to enrich the pornography industry which is at the centre of serious concerns about abuse and trafficking;[6] and when children's simulated gambling online is linked plausibly to higher rates of real gambling later in adult life.[7]

Adult content and spaces pose particular risks to children with higher-than-average vulnerabilities – e.g. those with a child protection history, disability, eating disorder and/or chronic illness. Research from the UK found these children were far more likely than their peers to visit adult sites and view content depicting disordered eating, violence, self-harm and/or suicide. These vulnerable children were more likely than their peers to have negative responses to digital technology such as anxiety, compulsion and harm to relationships – but they were also more likely to rely on technology for social connection and a sense of escape. Compared to their peers, they received less parental support to stay safe online and less online safety education.[8]

Where such protective factors are absent, inbuilt systems-level protections become even more important.

A mandate to prevent and reduce children's exposure to adult material

Children have a right to appropriate protections. General Comment 25 of the Convention on the Rights of the Child recognises the need for states to protect children from harmful online content, including pornographic and violent content, while balancing children's rights to information and freedom of expression. It specifies: '[States] should legislate to ensure that children are protected from harmful goods, such as weapons or drugs, or services, such as gambling. Robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use.'[9]

Australian legislation and regulation have laid the groundwork for such measures. The Online Safety Act provides for the creation of industry codes to cover procedures for dealing with class 2 material, while the Basic Online Safety Expectations (BOSE) determination includes a core expectation: 'The provider of the service will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service'.[10]

* For purposes of brevity, this paper will include class 1C material within 'class 2'.

Having appropriate systems in place to prevent children's exposure to class 2 materials could also help to align expectations in the digital environment with those in the offline world. In the offline world, businesses are prohibited on pain of fines and/or custodial sentences from selling or screening R18+ films, games or publications to children under 18; selling adult products like alcohol, tobacco, vapes / e-cigarettes and controlled weapons to children under 18; failing to prevent children under 18 from gambling in gambling venues; and allowing children under 18 onto premises used for commercial sexual purposes, including as clients.[11] (The final example is a useful analogy in relation to online pornography sites.)

It seems reasonable to expect equivalent standards of protection in the digital environment, albeit with appropriate protections for children's privacy and other rights. There is a public appetite for systems change – for example, 8 out of 10 Australian adults believe tech companies hold some responsibility for their online safety, and three-quarters of Australian adults support the implementation of age assurance to prevent children's exposure to pornography.[12] When Australian teens aged 16-18 were asked which stakeholders held some responsibility for preventing children from accessing pornography, 87% said the pornography industry, 82% said social media or gaming platforms, and 75% said the government.[13]

The role of the regulator

Under the Online Safety Act 2021, if codes drafted by industry do not contain appropriate community safeguards, the eSafety Commissioner may decline to register them and may take over development of industry standards instead.

If eSafety were to assess that the Phase 2 draft codes fail to uphold children's rights adequately, we would support any such decision.

We look to General Comment 25 of the U.N. Convention on the Rights of the Child, which specifies:

> '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. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child.'[14]

A strong line by the regulator could also reflect community sentiment. Australians show quite high levels of mistrust of social media and other digital technology companies – for example, around 4 in 10 Australians believe tech companies do not do enough to build safety features into their services and products. Only 15% of Australians believe businesses do enough to protect individuals' privacy.[15]

Most Australians see a major role for government and regulators here. For example, 8 out of 10 Australians agree that regulators should have the power to require businesses to pause or test data practices that may lead to harmful outcomes for people.[16] Almost 9 out of 10 Australians agree that government should keep businesses accountable for how they collect, share and use people's personal information.[17]

Classification of material

The type of materials eSafety envisaged as covered by the codes align with the approach of the National Classification Scheme: X18+, R18+, category 1 and 2 restricted, and class 1C.[18] We support the push to address children's exposure to these materials.

However, the draft codes focus predominantly on the most 'high impact' material: pornography (class 2A and 1C), self-harm† material, and simulated gambling. Other types of adult content (e.g. violence, crime) are positioned as less immediate priorities unless they fall into the serious, illegal categories covered by the Phase 1 codes.

This approach may resonate with eSafety's own priorities,[19] and we appreciate the urgency of addressing pornographic, self-harm and simulated gambling content.

However, we would be concerned if no meaningful attention were given to reducing children's exposure to R18+ violent content. More than a third of Australian teens aged 14-17 were exposed to violent imagery online in the past year.[20] Repeated exposure to violent media content is one risk factor that appears to contribute to emotional dysregulation and aggressive behaviours by children.[21] A study conducted in the UK found that even primary school children tended to see violent content as 'unavoidable', with viewership peaking between ages 13 and 15. Despite many negative consequences to viewing such content, children mistrusted reporting functions and rarely used them.[22]

Definition of pornography

We support eSafety's message to industry about the need to address risks and harms to children associated with synthetic and animated pornographic content at a time of major technological innovation eg. generative AI. To this end, eSafety urged industry to adopt a definition of online pornography which includes 'realistically simulated, generated and animated sexual content; high-impact text-based sexual content, including interactive services such as chatbots and AI models providing pornographic content; and high-impact nudity, ensuring protections are clear.'[23]

Serious concerns exist in the community about the proliferation of technologies such as:

- 'Nudifying' apps, many free and easy to use, which enable deepfake nude and pornographic images of real individuals, facilitating image-based abuse. These have already led to serious incidents in Australian schools. One analysis identified 24 million unique global visitors to 34 'undressing' websites in September 2023 alone, plus a huge rise in promotion of the apps on social media.[24]
- 'Non-photographic' pornographic entertainment (e.g. animated or drawn). The British Board of Film Classification scanned 100 popular pornographic sites in 2022 and found that 65% carried non-photographic content that appeared to promote abusive relationships and/or child sexual abuse, while 48% of sites carried non-photographic content based on popular characters likely to appeal to children eg. cartoon or superhero characters. It appeared that children who accessed the sites were more likely than adult users to view such content.[25] Meanwhile, a 2023 study found that Pornhub hosted approx. 109,000 hentai videos and named 'hentai' as their most popular search term for 2022. This style of animation, famous for portraying childlike figures engaged in sexual violence, also has a presence on mainstream sites like YouTube and TikTok.[26]
- AI-powered chatbots. In July 2024, over 100 AI powered applications were known to offer romantic and sexual interactions, and the Google Play store showed 30 million downloads of the 'friend' chatbot Replika and its two main competitors. Many concerns exist about possible effects on individuals' mental health, social skills, relationships and beliefs about consent.[27]

We are not sure that the draft codes' framing of 'pornography' captures such concerns adequately.

The draft Head Terms seems to have maintained a historical definition of class 2A material as that which is, or would likely be, classified as X18+ because it depicts actual sexual activity between consenting adults.[28]

The draft codes do introduce a new category of 'high impact class 2 generative AI DIS': a designated internet service which 'uses machine learning models to enable an end-user to produce material' and which 'has the sole or predominant purpose of being used to generate high impact online pornography'.[29] The inclusion of

† Note: for brevity and in line with the draft codes, we use the term 'self-harm material' to cover material that encourages, promotes or provides instruction for suicide, deliberate self-injury, and/or an eating disorder.

this category is welcome. However, we have some concerns that its scope may not be wide enough to address all the relevant concerns raised by eSafety. We seek to clarify the following:

- Whether or not this category covers all types of artificial and synthetic pornographic material flagged by eSafety in their position paper.
- Whether or not this category includes all 'nudifying apps', including those that produce what might be considered class 2B material (high impact nudity), which can cause great harm in the context of image-based abuse, but which might not be technically classified as 'high impact pornography'.
- Whether or not app distribution services are expected to take responsibilities in relation to 'nudifying apps', as part of their wider responsibilities in relation to 'high impact apps' which have the sole or predominant purpose of enabling end-users to access high-impact pornography. (The draft code for designated internet services signals that high impact generative AI services may be included in the overall category of high impact services, but the app distribution services draft code is less clear.)[30]

More broadly, we are not convinced by the overall approach to 'nudifying apps' in the draft codes, which seems to focus on limiting access to adults only and providing tools to reduce unwanted exposure and enable complaints.[31] The sharing of deepfake sexual material without consent will soon be treated as a criminal offence according to Australia's Criminal Code Amendment (Deepfake Sexual Material) Bill 2024. Surely image-based abuse is inherent to these digital products; they function as tools for relational abuse.[32] Were eSafety to push for stronger measures against these products, we would see merit in such a position.

Definition of a child

We welcome the draft Head Terms' recognition of an Australian child as 'an Australian end-user under the age of 18 years'.[33] This aligns with the definitions in the Online Safety Act 2021, the Classification Act 1995, the U.N. Convention on the rights of the Child, and the proposed insertion into the Privacy Act 1988.[34]

It is positive that the draft codes have not replicated the Phase 1 category of a 'young Australian child' (under 16), which effectively restricted various minimum default protections to under-16s instead of under-18s.[35]

We also welcome the fact that the draft equipment code has abandoned the Phase 1 distinction between 'children's interactive devices' and general devices, recognising that children often use general devices and face risks when doing so.[36] By the ages of 10-13, more than half of Australian children have their own phones and/or their own laptops, tablets or PCs.[37] We think it likely most of these were not designed or marketed as 'children's devices'.

However, we are concerned that a new category for mandatory minimum protections has been introduced: children under 13, described as 'the most vulnerable, young Australian child end-users'.[38] The equipment services code would require providers of Tier 1 devices to have in place measures to enable adults who share their devices with children to set up separate child accounts for under-13s with high default safety settings.[39] Similarly, the draft code for internet search engine services would require providers to make parental controls available to the parent or carer of a child under 13.[40]

Offering optional safety tools like parental controls is an imperfect way of addressing the risks children face online. Many parents cannot or do not use these tools, and many children still encounter adult content even with parental controls in place.[41]

Still, such safety tools would assist some families, and it is unclear to us why they should only be offered to families with younger children. We cannot find that eSafety recommended limiting minimum protections to this younger cohort. And such measures would do nothing to address the high exposure to age-inappropriate content experienced by adolescents aged 13 and over, who are still underage and developmentally vulnerable. For example, eSafety found that in the past year 25% of teens aged 14-17 had seen self-harm material online and 20% had seen suicidal material.[42]

Risk assessment

We encourage measures to assess, identify, and respond to the likely impacts of digital technologies on children's ability to enjoy all their rights. General Comment 25 of the UN Convention on the Rights of the Child specifies:

> '[States] should mandate the use of child rights impact assessments to embed children's rights into legislation, budgetary allocations and other administrative decisions relating to the digital environment and promote their use among public bodies and businesses relating to the digital environment.
> …
> 'States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public'.[43]

Assessing 'risk' alone is a narrower undertaking. Nonetheless, we encourage assessment of risks to children as an important step in the right direction.

Australia's BOSE determination lists child safety risk assessment and mitigation as a reasonable step that industry participants are encouraged to take to fulfil the expectations that they will treat the best interests of the child as a primary consideration, and that they will take reasonable steps to ensure technological or other measures are in effect to prevent access by children to class 2 material provided on the service.[44]

To this end, it seems appropriate that eSafety envisaged a risk-based regulatory approach for the Phase 2 codes,[45] listing the following risk factors as important:

- The purpose of a service, including whether or not class 2 material is part of the service's primary purpose or permitted by the service.
- The likelihood that a service may be used to directly expose children to class 2 material.
- The likelihood that a child will use the service to access class 2 material.[46]

The draft codes for app distribution services, hosting services, and internet carriage services do not outline a process for assessing risks to children, on the grounds that risk profiles within these categories are broadly consistent.[47] We cannot review this position in detail but given the importance of risk assessment to upholding children's rights, we would support any push by eSafety for a more in-depth approach.

The draft code for equipment services outlines an approach to risk assessment which focuses largely on the functionality of different devices. Tier 1 devices – the only ones subject to mandatory minimum compliance measures – are defined as personal and portable. We are concerned this may not cover some devices like desktop computers, which are still user-interactive and enable internet browsing through a screen.[48]

Meanwhile, there seems to be no explicit requirement for equipment services to assess the likelihood that a device may facilitate child access or exposure to class 2 material. We would support any push by eSafety for a more outcomes-focused approach to assessing risks to children in line with eSafety's position paper.

The approach to risk assessment in the draft codes for social media services, relevant electronic services and designated internet services includes welcome requirements to assess the likelihood that a child will access or be exposed to high-impact adult material on the service.[49] This seems to align with eSafety's priorities.

However, more guidance may well be needed in relation to the requirement that these services will assess whether 'a significant number of Australian children will access the service'.[50]

A similar requirement was included in the UK Children's Code, which created a significant problem: lack of clarity about what constituted 'significant numbers'. Many services accessed by children self-excluded from the Code because they claimed the numbers of children on their services were not 'significant'.[51] The Information Commissioner's Office had to explain what a 'significant number' could mean, addressing the accessibility, appeal and riskiness of a service to children and evidence of children using the service.

The ICO concluded '"Significant" in this context does not mean that a large number of children must be using the service or that children form a substantial proportion of your users. It means that there are more than a de minimis or insignificant number of children using the service.'[52]

Default protections for children

We support the use of default safety measures to reduce children's risk of exposure to high-impact adult material across all digital technologies likely to be accessed by children.

This would align with a reasonable step in the BOSE determination: that, in order to treat the best interests of the child as a primary consideration, 'if a service or a component of a service (such as an online app or game) is likely to be accessed by children (the children's service) – ensuring that the default privacy and safety settings of the children's service are robust and set to the most restrictive level'.[53]

To this end, we support the minimum compliance measure proposed by eSafety: 'Implement appropriate protective measures as a default to child end-users to prevent their access or exposure to class 1C and class 2 material.'[54]

The draft code for internet search engine services includes some encouraging requirements: that services must either apply safety tools and settings by default for an account holder which its age assurance systems indicate is likely to be a child; or, if age assurance is not adopted, apply other measures by default such as blurring high-impact pornography or reducing the risk of this material appearing in search results.[55]

Also encouraging is the requirement of the draft equipment services code that Tier 1 devices must have 'appropriate default safety settings applied to such child accounts or profiles that reduce the risk of such accounts or profiles being used to view high impact pornography' and only permit these default settings to be adjusted by the linked adult account/profile.[56] However, we fear this will be undermined by treating 13 as the maximum age for children's accounts.

The social media services draft code requires that default safety settings for child end-users are 'appropriately robust to protect children from being exposed to high impact online pornography and self-harm material' – but it appears this is only required of services which permit such material under their terms of use.[57]

We are concerned this may not be sufficient. eSafety's position paper did not seem to envisage that default protections for children would be limited to the riskiest services only.[58] Of those Australian teens who have seen pornography, 60% saw it on social media on platforms including Instagram, X/Twitter, TikTok and Snapchat.[59] Instagram, TikTok and Snapchat (as well as Facebook, YouTube and Pinterest) all prohibit such content formally – and yet evidently this has not been enough.[60]

In the draft code for relevant electronic services, we cannot see any indication that privacy or safety measures should be 'on' or 'high' by default.[61] This raises concerns, as many children see pornography on these services – for example, of Australian teens who have seen pornography, 17% saw it in a group chat and 11% saw it on a gaming site.[62] We note that the Phase 1 code for relevant electronic services does require accounts for under-16s to be private by default for high-risk services. However, we would like to see these default protections extended to 16- and 17-year-olds and reiterated in the Phase 2 code.[63]

The draft code for designated internet services requires that Tier 1-3 providers take appropriate measures to reduce children's risk of exposure to pornography and/or self-harm material. This 'may' include 'enabling child profiles on the service that are set by default at the highest safety settings available to limit children's exposure to high impact online pornography and/or self-harm materials', and/or implementing other functions such as blurring and halting autoplay.[64] These directions are positive, but we query whether this optional approach is enough.

High default child safety settings are not mentioned in the draft codes for app distribution services, hosting services and internet carriage services, although the latter does require services to provide information on

filtering products.[65] We appreciate the topic may be less relevant to those sections of industry – however, we would support any push by eSafety for more proactive measures.

Age assurance

In their position paper, eSafety put forward the following minimum compliance measures:

- 'Online services must take reasonable steps to ascertain the age of users by implementing appropriate age assurance measures before providing access to class 1c and class 2 material'
- 'Online services should ensure age assurance measures are user-friendly, privacy-preserving and easy to adopt.'

eSafety proposed that the appropriateness of age assurance measures should be proportionate to risk, and that age assurance measures could be applied, where relevant, through centralised user accounts in 'ecosystems' of products and services.[66]

Importantly, eSafety emphasised that they do not support 'invasive, unreasonable or unfair data collection practices' and that nothing in their position paper should be taken as endorsing additional end-user data collection by service providers beyond what is essential for their operations.[67]

We support eSafety's approach to age assurance, which aligns with one of the reasonable steps cited in the BOSE determination.[68] We also refer to General Comment 25 of the UN Convention on the Rights of the Child, which states:

> 'Age-based or content-based systems designed to protect children from age-inappropriate content should be consistent with the principle of data minimization.
> …
> 'Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention.
> …
> 'States parties should require the integration of privacy by design into digital products and services that affect children.'[69]

There is strong support in the community for age assurance measures to prevent children's exposure to pornography, with nearly 8 in 10 Australian adults supporting age verification by government for this purpose.[70] Almost 6 in 10 Australian teens agree that age assurance should be present on pornography sites.[71] Meanwhile, research conducted with British families returned findings which we believe are likely to match Australian community sentiments: most families support online age assurance for activities associated with adult age limits in the offline world eg. gambling, pornography, alcohol.[72]

However, there is significant public apprehension about risks associated with online age assurance in relation to privacy, data security, reliability, effectiveness, and ease of use.[73]

Protection of children's personal information is especially important. Three-quarters of Australian parents agree they are uncomfortable with businesses tracking a child's location without permission, selling personal information about a child to third parties, inferring sensitive information about a child based on their personal data, and targeting advertising to a child based on information gained by tracking the child online.[74] Nine out of 10 Australian parents agree that profiling and targeted advertising should not happen to children and that organisations should collect only the minimum data about a child necessary to provide the service.[75]

We welcome the draft codes' inclusion of an umbrella definition of age assurance; their acknowledgement of the coming Children's Online Privacy Code; and their recognition of the value of age assurance to protecting children in some high-risk digital spaces.[76] The Head Terms' does recognise the importance of protecting and promoting human rights, including the rights not to be subjected to arbitrary or unlawful interference with privacy.[77]

We also welcome the Head Terms' statement that appropriateness of age assurance measures should be determined by aspects including technical accuracy, robustness, reliability, 'fairness', and limiting circumvention 'where reasonably possible'.[78]

However, we are concerned that the draft codes' guidance about age assurance does not require services to take a data minimisation approach. (Data minimisation is mentioned broadly in the discussion paper as something industry supports,[79] but it is not specified in the codes themselves.) Nor, as far as we can tell, are services required to assess risks to children's privacy or prohibited from using personal information obtained through age assurance for other purposes.[80]

Nor do the draft codes acknowledge the possibility that a generalist provider may dispense with the need for age assurance by making their products and services safe for children by design and default.

Finally, we note that age assurance is not mentioned explicitly in the draft codes for equipment services or internet carriage services. We recognise it may not have been considered relevant, but in light of eSafety's promotion of an 'ecosystems' approach,[81] we would support any push by eSafety to address the matter there.

Consultation with children, young people and the wider community

Industry associations have signalled their willingness to work within the timeframe outlined by eSafety, who requested that draft codes be submitted for final consideration by 19 December 2024.[82]

We sympathise with eSafety's sense of urgency given the serious and growing nature of the problems and the historical delays in this space. Initially, it was anticipated that all Phase 1 and 2 codes would be registered by December 2022.[83]

However, we think it vital that there is proper community consultation. The 31-day public consultation period fits within the terms of the Online Safety Act but is unlikely to enable widespread, meaningful participation by children, young people, families, educators and not-for-profit providers, whose resources are limited.

A public consultation period of at least 60 days would be preferable. This would make it easier to work in line with the UN Convention on the Rights of the Child, General Comment 12, 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'.[84]

Extending the consultation period could also align with eSafety's message to code drafters that they should engage with children, young people, parents and carers, educators and child-rights groups, possibly for longer than the 30-day minimum.[85]

For these reasons, we do not support the proposal in the draft Head Terms that any future drafts of revised codes be subject to a 30-day minimum consultation period.[86]

At a minimum, we trust that the consultation will engage eSafety's own Youth Advisory Council and any youth engagement bodies hosted by industry partners.

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

Sarah Davies AM, CEO
sarah.davies@amf.org.au

Ariana Kurzeme, Director, Policy & Prevention
ariana.kurzeme@amf.org.au

Dr Jessie Mitchell, Manager, Advocacy
jessie.mitchell@amf.org.au

[1] eSafety Commissioner, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' July 2024, https://www.esafety.gov.au/sites/default/files/2024-07/Development-of-Phase-2-Industry-Codes-under-the-Online-Safety-Act-eSafety-position-paper_0.pdf , p.26

[2] Australian Mobile elecommunications Association (AMTA), Communications Alliance (CA), the Consumer Electronics Suppliers Association (CESA), the Digital Industry Group Inc (DIGI), and the Interactive Games and Entertainment Association (IGEA) and contributors, 'Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms,' 2024, https://onlinesafety.org.au/phase-two-codes/, p.13

[3] Australian Centre to Counter Child Exploitation, 'Online Child Sexual Exploitation: understanding community awareness, perceptions, attitudes and preventative behaviours,' 2020, https://www.accce.gov.au/sites/default/files/2021-02/ACCCE_Research-Report_OCE.pdf ; House of Representatives Standing Committee on Social Policy and Legal Affairs, 'Protecting the age of innocence: Report of the inquiry into age verification for online wagering and online pornography,' 2020, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024436/toc_pdf/Protectingtheageofinnocence.pdf;fileType=application%2Fpdf; ReachOut, 'Parenting in the digital age: navigating concerns about the online world of young people,' 2023, https://d1robvhmkdqpun.cloudfront.net/6443e8c2623028a2222d030f8d7ea6f2.pdf

[4] 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; Maggie Dent and Collective Shout, 'Sexual Harassment of Teachers Report,' 2024, https://www.collectiveshout.org/shot-report; eSafety Commissioner, '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 ; 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; WeProtect Global Alliance, 'Global Threat Assessment 2023,' 2023, https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf

[5] Family Kids & Youth, 'Understanding Pathways to Online Violent Content Among Children,' 2024, https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/experiences-of-children/understanding-pathways-to-online-violent-content-among-children.pdf?v=368021 ; Ipsos UK and TONIC Research, 'Online Content: Qualitative Research - Experiences of children encountering online content relating to eating disorders, self-harm and suicide,' 2024, https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/experiences-of-children/experiences-of-children-encountering-online-content-relating-to-eating-disorders-self-harm-and-suicide.pdf?v=368019

[6] See eSafety, 'Roadmap for age verification'; 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,' 2024, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2024/pipeda-2024-001/; 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

[7] Kei Sakata, Rebecca Jenkinson, 'What is the link between video gaming and gambling?', Snapshot Series - Issue 7, 2022, https://growingupinaustralia.gov.au/research-findings/snapshots/what-link-between-video-gaming-and-gambling. See also Nancy Greer, Cailem Murray Boyle and Rebecca Jenkinson, 'Harms

associated with loot boxes, simulated gambling and other in-game purchases in video games: a review of the evidence,' Australian Gambling Research Centre, Australian Institute of Family Studies, June 2022 https://www.classification.gov.au/sites/default/files/documents/agrc_literature_review_final_20220906_accessible.pdf

[8] Adrienne Katz and Aiman El Asam, 'Look at me: teens, sexting and risks,' Internet Matters, 2020, https://www.internetmatters.org/wp-content/uploads/2020/06/Internet-Matters-Look-At-Me-Report-1.pdf ; Adrienne Katz and Aiman El Asam, 'Refuge and Risk: Life Online for Vulnerable Young People,' Internet Matters, 2021, https://www.internetmatters.org/wp-content/uploads/2021/01/Internet-Matters-Refuge-And-Risk-Report.pdf ; Adrienne Katz and Aiman El Asam, 'Vulnerable Children in a Digital World,' Internet Matters, 2019, https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf

[9] United Nations (U.N.) 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

[10] Commonwealth of Australia, 'Online Safety (Basic Online Safety Expectations) Determination 2022,' amended 31 May 2024, https://www.legislation.gov.au/

[11] Classification (Publications, Films and Computer Games) (Enforcement) Act 1995, amended 1 March 2019, items 13, 18, 31, 42 https://content.legislation.vic.gov.au/sites/default/files/ca97c6c2-8c84-3b11-8adf-55a9298d6f01_95-90aa042%20authorised.pdf; Sydney Morning Herald, 'Tabcorp fined after failing to stop teen from punting 30 times,' 13 June 2024, https://www.smh.com.au/business/companies/tabcorp-fined-after-failing-to-stop-teen-from-punting-30-times-20240613-p5jljo.html ; Victorian Gambling and Casino Control Commission, 'Compliance resources for gaming venues,' 2024, https://www.vgccc.vic.gov.au/gambling/gaming-venue-operator/understand-your-gaming-licence/compliance-resources-gaming-venues ; Victorian Government, 'Giving Police More Power To Crackdown On Crime,' 2024, https://www.premier.vic.gov.au/giving-police-more-power-crackdown-crime ; Victorian Government, 'Liquor fees and fines,' 2024, https://www.vic.gov.au/liquor-fees-and-fines ; Victorian Government, 'Sex Work Decriminalisation Act 2022,' items 42, 45, 47 https://content.legislation.vic.gov.au/sites/default/files/2022-02/591279bs1.pdf ; Victorian Government, 'Tobacco retailer guide,' 2024, https://www.health.vic.gov.au/publications/tobacco-retailer-guide ; Victorian Government, 'Under-18 patrons on licensed premises,' 2024, https://www.vic.gov.au/under-18-patrons-licensed-premises ; Victorian Government, 'Weapons definitions,' 2024, https://www.police.vic.gov.au/weapons-definitions

[12] eSafety, 'Australians' negative online experiences 2022,' https://www.esafety.gov.au/research/australians-negative-online-experiences-2022; eSafety, 'Roadmap for age verification'

[13] eSafety, 'Young people's attitudes towards online pornography and age assurance', 2023, https://www.esafety.gov.au/research/young-peoples-attitudes-towards-online-pornography-and-age-assurance

[14] U.N. Convention on the Rights of the Child, 'General comment No. 25'

[15] Consumer Policy Research Centre (CPRC), 'Not a fair trade: consumer views on how businesses use their data', 2023, https://cprc.org.au/report/not-a-fair-trade-consumer-views-on-how-businesses-use-their-data/ ; eSafety, 'Australians' negative online experiences 2022. See also Office of the Australian Information Commissioner (OAIC), 'Australian Community Attitudes to Privacy Survey,' 2023, https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023

[16] CPRC, 'Not a fair trade'

[17] CPRC, 'Not a fair trade'

[18] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' p.47

[19] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' pp.49-53

[20] eSafety, 'Mind the Gap: Parental awareness of children's exposure to risks online, 2023, https://www.esafety.gov.au/sites/default/files/2022-02/Mind%20the%20Gap%20%20-%20Parental%20awareness%20of%20children%27s%20exposure%20to%20risks%20online%20-%20FINAL.pdf

[21] Children & Media Australia, 'Submission to the inquiry into the issue of increasing disruption in Australian school classrooms,' 2023, https://childrenandmedia.org.au/assets/files/taking-action/cma-submission-on-increasing-disruption-in-australian-school-classrooms-april-2023.pdf

[22] Ofcom, 'Encountering violent online content starts at primary school,' March 2024, https://www.ofcom.org.uk/online-safety/protecting-children/encountering-violent-online-content-starts-at-primary-school/
[23] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' pp.23, 50-51
[24] Graphika, 'A Revealing Picture,' 2023, https://graphika.com/reports/a-revealing-picture Also eSafety, 'Senate Standing Committee Opening Statement: Criminal Code Amendment (Deepfake Sexual Material) Bill 2024,' 23 July 2024, https://www.esafety.gov.au/newsroom/media-releases/senate-standing-committee-opening-statement-criminal-code-amendment-deepfake-sexual-material-bill-2024
[25] British Board of Film Classification, 'New BBFC research reveals children are more exposed to sites specialising in non-photographic pornography, compared to adults,' 2022, https://www.bbfc.co.uk/about-us/news/new-bbfc-research-reveals-children-are-more-exposed-to-sites-specialising-in-non-photographic-pornography-compared-to-adults
[26] Gail Dines and Mandy Sanchez, 'Hentai and the Pornification of Childhood: How the Porn Industry Just Made the Case of Regulation,' *Dignity: A journal of analysis of exploitation and violence*, vol. 8, no.1, 2023, https://www.researchgate.net/publication/368899868_Hentai_and_the_Pornification_of_Childhood_How_the_Porn_Industry_Just_Made_the_Case_of_Regulation
[27] Rob Brooks, 'I tried the Replika AI companion and can see why users are falling hard. The app raises serious ethical questions,' *The Conversation*, 21 February 2023, https://theconversation.com/i-tried-the-replika-ai-companion-and-can-see-why-users-are-falling-hard-the-app-raises-serious-ethical-questions-200257; Raffaele F Ciriello, 'The AI sexbot industry is just getting started. It brings strange new questions – and risks,' *The Conversation*, 15 October 2024, https://theconversation.com/the-ai-sexbot-industry-is-just-getting-started-it-brings-strange-new-questions-and-risks-238998 ; Valerie A. Lapointe, David Lafortune, Simon Dubé, 'Computer love: AI-powered chatbots are changing how we understand romantic and sexual well-being,' *The Conversation*, 7 July 2024, https://theconversation.com/computer-love-ai-powered-chatbots-are-changing-how-we-understand-romantic-and-sexual-well-being-234054 ; Dan Weijers and Nick Munn, 'AI companions can relieve loneliness – but here are 4 red flags to watch for in your chatbot 'friend',' *The Conversation*, 9 May 2024, https://theconversation.com/ai-companions-can-relieve-loneliness-but-here-are-4-red-flags-to-watch-for-in-your-chatbot-friend-227338
[28] AMTA et al, 'Head Terms', p.9
[29] AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 3 – Designated Internet Services Online Safety Code (Class 1C and Class 2 Material) DRAFT 3,' October 2024, 2024, https://onlinesafety.org.au/phase-two-codes/ p.4; AMTA, CA, CESA, DIGI, IGEA, 'Discussion Paper: Draft Phase 2 online safety codes,' 2024, https://onlinesafety.org.au/phase-two-codes/ p.39
[30] AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 4 – App Distribution Services Online Safety Code (Class 1C and Class 2 Material)' 3 October 2024, https://onlinesafety.org.au/phase-two-codes/ , p.3; AMTA et al, 'Discussion Paper', p.59. Also AMTA et al, 'Schedule 3 – Designated Internet Services Online Safety Code,' pp.4-5
[31] AMTA et al, 'Schedule 3 – Designated Internet Services Online Safety Code,' pp.25-26. Also AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 4 - App Distribution Services Online Safety Code,' pp.5, 8
[32] eSafety, 'Senate Standing Committee Opening Statement: Criminal Code Amendment (Deepfake Sexual Material) Bill 2024'
[33] AMTA et al, 'Head Terms', p.8
[34] Australian Government, Privacy and Other Legislation Amendment Bill 2024, part 4, 12 September 2024, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7249
[35] Onlinesafety.org.au, 'Consolidated Industry Codes of Practice for the Online Industry, Phase 1,' https://onlinesafety.org.au/codes/
[36] AMTA et al, 'Discussion Paper', p.74
[37] OAIC, 'Australian Community Attitudes to Privacy Survey,' 2023
[38] AMTA et al, 'Discussion Paper', p.75; AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 7 – Equipment Online Safety Code (Class 1C and Class 2 Material),' October 2024, p.2;
[39] AMTA et al, 'Discussion Paper', pp.75-76; AMTA et al, 'Schedule 7 – Equipment Online Safety Code,' p.7
[40] AMTA et al, 'Discussion Paper', p.54 Also AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 8 – Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material),' October 2024, p.6

[41] Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts, '2022 National Online Safety Survey,' 2022, https://www.infrastructure.gov.au/department/media/news/2022-national-online-safety-survey ; eSafety, 'Mind the Gap'
[42] eSafety, 'Mind the Gap';
[43] U.N. Convention on the Rights of the Child, 'General comment No. 25'
[44] Australian Parliament, 'Online Safety (Basic Online Safety Expectations) Determination 2022' section 6 items 2A and 3e; section 11 items 12(2b)
[45] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' p.9
[46] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' p.63
[47] AMTA et al, 'Discussion Paper', p.60, 71; AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 5 – Hosting Services Online Safety Code (Class 1C and Class 2 Material) Draft 3,' October 2024, p.2
[48] AMTA et al, 'Schedule 7 – Equipment Online Safety Code,' pp.3-4, 6
[49] AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 1 – Social Media Services Online Safety Code (Class 1C and Class 2 Material),' 2024, p.5; AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material),' October 2024, pp.5-6; AMTA, CA, CESA, DIGI, IGEA and contributors, 'Schedule 3 – Designated Internet Services Online Safety Code (Class 1C and Class 2 Material),' October 2024, p.8
[50] AMTA et al, 'Schedule 2 – Relevant Electronic Services Online Safety Code,' p.5; AMTA et al, 'Schedule 3 – Designated Internet Services Online Safety Code,' p.8
[51] UK Information Commissioner's Office (ICO), 'Likely to be accessed: impact assessment,' July 2023, https://ico.org.uk/media/4025881/ltba-guidance-impact-assessment.pdf
[52] UK ICO, ' 'Likely to be accessed' by children – FAQs, list of factors and case studies,' accessed 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/#threshold
[53] Australian Parliament, 'Online Safety (Basic Online Safety Expectations) Determination 2022'
[54] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' p.84
[55] AMTA et al, 'Schedule 8 – Internet Search Engine Services Online Safety Code', pp.5-6
[56] AMTA et al, 'Schedule 7 – Equipment Online Safety Code,' p.7
[57] AMTA et al, 'Schedule 1 – Social Media Services Online Safety Code,' p.7; AMTA et al, 'Discussion Paper', p.18
[58] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' pp.84-85
[59] eSafety, 'Accidental, unsolicited and in your face - young people's encounters with online pornography: a matter of platform responsibility, education and choice,' 2023, https://www.esafety.gov.au/research/young-peoples-attitudes-towards-online-pornography-and-age-assurance
[60] Instagram, 'Community guidelines,' accessed 2024, https://help.instagram.com/477434105621119?ref=igtos&helpref=faq_content ; Snapchat, 'Community guidelines,' 2024, https://values.snap.com/privacy/transparency/community-guidelines ; TikTok, 'Sensitive or mature themes,' 2024, https://www.tiktok.com/community-guidelines/en/sensitive-mature-themes#1; X, 'Adult content,' 2024, https://help.x.com/en/rules-and-policies/adult-content . Also Facebook, 'Community guidelines,' 2024, https://www.facebook.com/help/477434105621119 ; Pinterest, 'Content Safety, https://policy.pinterest.com/en/community-guidelines#section-content-safety ; YouTube, 'Nudity & Sexual Content Policy,' 2024, https://support.google.com/youtube/answer/2802002?hl=en&ref_topic=9282679
[61] AMTA et al, 'Schedule 2 – Relevant Electronic Services Online Safety Code,' pp.9, 10, 11, 21, 23
[62] eSafety, 'Accidental, unsolicited and in your face'
[63] Onlinesafety.org.au, 'Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material),' 2024, https://onlinesafety.org.au/codes/ p.17
[64] AMTA et al, 'Schedule 3 – Designated Internet Services Online Safety Code,' October 2024, p.16
[65] CA, CESA, DIGI, IGEA and contributors, 'Schedule 6 – Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material),' October 2024, p.4
[66] eSafety, 'Development of Phase 2 Industry Codes under the Online Safety Act,' pp.82-84
[67] eSafety, 'Development of Phase 2 Industry Codes under the Online Safety Act,' p.70
[68] Online Safety (Basic Online Safety Expectations) Determination 2022, with amendments, registered 27 June 2024, items 6, 12, https://www.legislation.gov.au/F2022L00062/latest/text

[69] U.N. Convention on the Rights of the Child, 'General comment No. 25'
[70] eSafety Commissioner, 'Public perceptions of age verification for limiting access to pornography', 2021, https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography
[71] eSafety, 'Young people's attitudes towards online pornography and age assurance'
[72] ICO and Ofcom (UK), 'Families' attitudes towards age assurance: research commissioned by the ICO and Ofcom,' 2022, https://www.gov.uk/government/publications/families-attitudes-towards-age-assurance-research-commissioned-by-the-ico-and-ofcom
[73] eSafety, 'Public perceptions of age verification for limiting access to pornography'; eSafety, 'Young people's attitudes towards online pornography and age assurance'; ICO and Ofcom (UK), 'Families' attitudes towards age assurance'
[74] OAIC, 'Australian Community Attitudes to Privacy Survey,' 2023
[75] OAIC, 'Australian Community Attitudes to Privacy Survey,' 2023
[76] AMTA et al, 'Schedule 1 – Social Media Services Online Safety Code,' p.7; AMTA et al, 'Schedule 2 – Relevant Electronic Services Online Safety Code,' p.7; AMTA et al, 'Schedule 3 – Designated Internet Services Online Safety Code,' pp.11, 24, 25; AMTA et al, 'Schedule 4 – App Distribution Services', p.5; AMTA et al, 'Schedule 8 – Internet Search Engine Services Online Safety Code,' p.5
[77] AMTA et al, 'Head Terms', pp.8, 13; AMTA et al, 'Discussion Paper', p.15
[78] AMTA et al, 'Head Terms', p.14
[79] AMTA et al, 'Discussion Paper: Draft Phase 2 online safety codes,' p.8
[80] AMTA et al, 'Head Terms', p.15
[81] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' p.77
[82] AMTA et al, 'Discussion Paper: Draft Phase 2 online safety codes,' p.7. See also eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper'
[83] eSafety, 'Development of industry codes under the Online Safety Act: position paper,' 2021 , https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf
[84] U.N. 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
[85] eSafety, 'Development of Phase 2 Industry codes under the Online Safety Act: position paper,' pp.10, 22, 91
[86] AMTA et al, 'Head Terms', p.20