Industry Standards - Designated Internet Services and Relevant Electronic Services

Submission by the Alannah & Madeline Foundation

December 2023

For their right to be safe

Contents

Executive summary 3
About us 4
Recommendations 4
Definition of childhood 5
Default privacy protections for children 5
Reporting of child sexual exploitation 6
Identifying the right industry standard for a service 7
Investment in systems, processes and technologies to improve children's safety 7
Complaints mechanisms for end-users 7
Consultation process 8
Leadership of standard development for industry 8

Executive summary

The Alannah & Madeline Foundation (the Foundation) applauds the ongoing work of the eSafety Commissioner to build a better digital environment for children. We appreciate this opportunity to respond to the draft Designated Internet Services Standard and Relevant Electronic Services Standard for Class 1A and 1B material. Our response focuses on the category of child sexual exploitation material.

We are a national not-for-profit organisation dedicated to keeping children and young people free from violence and trauma wherever they live, learn and play. Our strategic priorities include empowering children and young people as positive digital citizens and upholding the rights of children and young people in the digital environment.

The Foundation voiced our support for the eSafety Commissioner's decision to take over drafting these two industry standards, which cover:

- Relevant Electronic Services, which enable people to communicate directly with each other online, including by email, instant messaging, MMS and chat, dating services, and games with communication functionality.

- Designated Internet Services, which enable people to access material using an internet carriage service, or which deliver material to a person by means of an internet carriage service. They include online file storage services.

The digital environment presents unprecedented opportunities and risks to children's development; as such, it is imperative that regulatory frameworks prioritise measures to uphold children's rights. The best interests of the child must be a primary consideration in the creation of industry standards. We welcome eSafety's reference in the discussion paper to the rights and best interests of children as a key consideration.

This submission responds to **Question 2** of the discussion paper: 'Do the obligations on each relevant electronic service and designated internet service category appropriately reflect the above considerations?' The considerations include: 'the rights and best interests of children'.

The draft standards represent a shift towards greater protections for children. For example, they address the highly significant relationship between generative AI and child sexual exploitation material – a vital and timely step. They also articulate improved expectations about services' complaints and reporting obligations in relation to child sexual exploitation material.

However, we believe additional steps could be taken to strengthen protections for children's rights. These should include defining a child as anyone under 18 and lifting default privacy settings to align with this; ensuring children have access to safe, easy, age-appropriate mechanisms to raise a concern; and engaging children, young people, parents / carers, and experts in child safety and development fully in the drafting of the standards.

The draft standards set new expectations about detection, removal, disruption and deterrence of known and new child sexual abuse material and investment in new approaches to enable this.

Use of technological tools by private industry to proactively detect child sexual abuse material is a complex topic for legal, technological, and ethical reasons. Within the brief consultation period, we do not feel well placed to comment in detail on this matter. But we support the overall direction articulated, recognising the scale and urgency of the issue.

We trust any such measures will align with guidance from the United Nations Convention on the Rights of the Child, General Comment 25: that any measures to enable the detection of child sexual exploitation material in a context of encryption must be 'strictly limited according to the principles of legality, necessity and proportionality'.[1] As UNICEF has also stated 'Means and methods of proactive detection of child sexual

abuse materials ... must be legal, necessary and proportionate, the least intrusive option available and not impair the essence of the right to privacy.'[2]

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 27 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. Very much 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, education and care settings and places of work.

- Safe and Strong: building positive digital citizens. The Foundation works with schools, families and communities nationally to help children build the digital intelligence, skills and competencies they need to stay safe online and to be active, positive digital citizens. With over 10 years' experience working in online bullying and wellbeing, as technology has become ubiquitous, our work has developed into building digital intelligence, digital ethics and media literacy for all children aged 3-18.

- 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 Officer 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. Include a definition of 'child' in line with the Online Safety Act and the United Nations Convention on the Rights of the Child: 'an individual who has not reached 18 years'.

2. Raise the age for high default privacy settings to 18, not 16 (see Tier 1 Relevant Electronic Services and open communication relevant electronic services) in line with child rights guidance and relevant codes in other jurisdictions.

3. Ensure confirmation by the National Children's Commissioner that the requirements for service providers to report child exploitation material to the authorities align with the highest standards for reporting child sexual abuse across Australian jurisdictions.

4. Determine that where a service could fall within the scope of more than one industry code or industry standard, the applicable code or standard will be the one that provides the highest level of protection against identified risks.

5. Ensure the requirements for services to invest in development programs to detect, disrupt and deter Class 1A and 1B material align with the 'maturity' measure of innovative solution development by industry articulated in the WeProtect Model National Response to preventing and tackling online child sexual exploitation and abuse.

6. Specify that mechanisms for end-user reporting of Class 1A or 1B material should include mechanisms which children can use to report a concern directly. These should be age-appropriate, easy to use, clear and honest, displayed prominently, with information about the response process and guidance about support available to children.

7. Extend the consultation to include targeted, funded, proactive engagement with a wide range of relevant not-for-profit community services, experts in child safety and development, parents and carers, and young Australians themselves. For example, we would welcome an opportunity to hear from the eSafety Youth Council.

8. As part of the pending statutory review of the Online Safety Act, advocate for the development of codes or standards for industry under the Act to be led by an independent, expert, trusted regulator, not by industry associations.

Definition of childhood

Despite a welcome statement that Tier 1 Designated Internet Services – eg. 'gore' sites and pornography sites – are expected to take appropriate action to prevent access by under-18s (Section 25), we cannot find that the draft standards specify an overall definition of a 'child'.

We believe this absence should be addressed. If a child is defined according to existing legislation eg. the Online Safety Act – it would make sense to clarify this.

Codes to regulate industry's handling of children's data in the United Kingdom, Sweden, the Netherlands, Ireland, and France define childhood as including all under-18s, in line with the United Nations Convention on the Rights of the Child.[3]

Default privacy protections for children

We are concerned about the proposed requirement that Tier 1 Relevant Electronic Services and open communication relevant electronic services must ensure the accounts of children aged under 16 are private by default (Section 19). This will likely mean that the accounts of 16- and 17-year-olds will remain public by default.

It is perplexing that the default age has been set so low, especially as Tier 1 Relevant Electronic Services are assessed as high-risk for Class 1A and 1B materials, and as open communication relevant electronic services enable their users to search, view and communicate with other people without needing their contact details first and may recommend new contacts.

We maintain high default privacy settings for children under 18 are important for several reasons:

- It's their right. General Comment 25 of the United Nations Convention on the Rights of the Child, which defines children as all under-18s, specifies 'States parties should require all businesses that affect children's rights in relation to the digital environment to implement … industry codes … that adhere to the highest standards of ethics, privacy and safety'.[4]

- It's in keeping with international practice. For example, the U.K. Children's Code requires all services likely to be accessed by under-18s to have high privacy settings by default, including for geolocation data, unless the service can demonstrate a compelling reason to do otherwise, taking into account the best interests of the child.[5] Codes to regulate the handling of children's data in Sweden, the

Netherlands, Ireland and France all articulate expectations that under-18s are entitled to minimal handling of their personal data and protection from harmful design features. Default high privacy settings are highlighted.[6]

- It's in line with community values. 92% of Australian parents support default privacy settings for children being set to high and 85% support geo-location tracking being turned off by default for children.[7] (Two-thirds of Australians dislike low-privacy default settings for adults.)[8]

- It's likely to have an impact. Options presented as default are more likely to be chosen, either actively due to consumer bias or passively due to consumers making no choice.[9] The UK Information Commissioner concluded 'Many children just accept whatever privacy settings they are given and never change them.'[10]

- It may well set a precedent. A Children's Online Privacy Code is pending for Australia, which has broad ramifications for the design and operation of online services. We are concerned that codes and standards under the Online Safety Act may serve to normalise a lower age ceiling of protection for children before drafting of a Privacy Code can begin.

- It's unreasonable to expect children and parents to take the lead on safety all the time. The Australian Centre to Counter Child Exploitation found that parents commonly feel they have less digital literacy than their children; most have poor awareness of online child sexual exploitation; and around four-fifths assume it would not happen to their children. (The ACCCE cites messaging apps and interactive games as risky spaces.)[11] Meanwhile, eSafety found that 69% of Australian teens aged 14-17 had been in contact with someone they first met online. In a quarter of cases, the person was an adult with no prior connection to the child. 47% of Australian teens had received a sexual message, while 15% had sent a photo or video of themselves to someone they had never met in person.[12] Many children assume certain spaces, such as private messaging services and gaming platforms, are safer than they really are.[13]

The discussion paper invites respondents to reflect on how the draft standards take into account the 'best interests of children'. We can see no strong argument for children's best interests being served better by low default privacy settings than by high ones, or for 16- and 17-year-old Australians having weaker in-built protections than their peers overseas.

A child rights approach recognises that, in light of children's vulnerabilities, their best interests should be given high priority, not treated as merely one of many considerations. As the UK Children's Code states 'it is unlikely … that the commercial interests of an organisation will outweigh a child's right to privacy'.[14]

The only argument in favour of limiting high default privacy settings to under-16s would be consistency with the existing industry-led codes under the Online Safety Act. However, we do not see this as a more compelling argument than those listed above.

Reporting of child sexual exploitation

The draft standards for Relevant Electronic Services (Section 15) and Designated Internet Services (Section 15) state that if the provider of a service identifies child sexual exploitation material and believes in good faith it is not 'known' (ie. not previously identified by relevant authorities), then the provider must as soon as practicable notify a governmental or recognised authoritative non-governmental organisation which combats child sexual abuse or child sexual exploitation.

The draft standards add that this requirement is 'in addition to any other applicable law'.

We welcome this direction and trust that eSafety has engaged with the National Children's Commissioner to confirm this requirement aligns with the highest standards for reporting of child sexual abuse in Australian jurisdictions – see for example those of Victoria, New South Wales, and the Northern Territory.[15]

The reporting requirement above does not seem to apply to Tier 3 Relevant Electronic Services or Tiers 2 and 3 Designated Internet Services. However low their risk of encountering child sexual exploitation material, we feel these services should still be expected to report any that might come to their attention.

Ultimately, we would like to see both known and new CSEM identified and actioned via appropriate, effective technology and appropriately qualified, skilled and resourced personnel, supported by adequate infrastructure. Such interventions should be deployed, or at least regulated, by a trusted public entity working in line with international best practice and Australian law. These interventions should be resourced through partnerships between government and private industry.

Identifying the right industry standard for a service

The draft standards state that where a Relevant Electronic Service (Section 5) or Designated Internet Service (Section 5) could fall within the scope of more than one industry code or standard, the applicable code or standard will be the one with which the service's predominant functionality most closely aligns.

We submit that 'predominant functionality' may be rather subjective and does not necessarily indicate the frequency or severity of risk. Where a single service could fall within the scope of more than one code or standard, we would rather see it categorised under whichever code or standard provides the highest level of protection against the risks identified for that service.

The current proposed approach aligns with that of the industry-led Head Terms document. This points to one reason we do not support the industry-led approach: even when the regulator takes over standard development, there seems to be pressure to align with existing industry-led products.

Investment in systems, processes and technologies to improve children's safety

The draft standards require those Designated Internet Services (Section 24) and Relevant Electronic Services (Section 23) which are deemed to be larger and higher-risk to establish and implement a development program of systems, processes and technologies that enhance providers' ability to detect, deter and disrupt the generation, accessing, distribution or storage of child sexual abuse material.

We welcome this requirement, which has potential to ensure continuous improvement in protections for children. It is important to ensure the regulatory scaffolding is as strong as possible to encourage the best outcomes from industry's efforts. This might perhaps be delivered by more explicit alignment with the 'maturity' measure of innovative solution development by industry articulated in the Model National Response (WeProtect Global Alliance and UNICEF):

'Innovative technological solutions that demonstrably enhance existing approach to preventing and tackling child sexual exploitation and abuse are consistently and effectively developed, scaled up, monitored and updated. Industry actively finances and prioritises tech solutions that are compatible with children's rights and safety online.'[16]

Complaints mechanisms for end-users

We welcome the requirement that certain Designated Internet Services (Section 29) and Relevant Electronic Services (Sections 27, 29) will provide mechanisms for end-users to make complaints about Class 1A or 1B material, and that these mechanisms will be easy to use, with clear instructions, and easily accessible within or through the service.

This measure would be strengthened further by specifying that providers have complaints mechanisms which children can use to report a concern directly. These should be prominent, age-appropriate, easy to use, clear and honest, with information about timeframes for response and guidance about other support available to children eg. Kids Helpline. We believe this approach would align with the advice of General Comment 25 that businesses should ensure they provide effective complaint mechanisms for children.[17]

Consultation process

We have concerns about the community's capacity to engage meaningfully in this consultation, in light of the substance and complexity of the documents and the timeframe involved: a 31-day period immediately before the end-of-year holiday season.

We believe consultations should be longer and should include proactive engagement (backed by appropriate resourcing) with a wide diversity of relevant public bodies, not-for-profit community services, experts in online safety and child health and development, and young Australians themselves. This would ensure the development of industry standards is informed by a full range of stakeholder insights.

For example, we would be pleased to learn that resourcing has been made available to enable the eSafety Youth Council to provide their perspectives on these proposed standards.

Children's rights and best interests are flagged in the discussion paper as an important consideration. Typically, the rights and best interests of children are understood to include having a voice on matters that affect them. The United Nations Convention on the Rights of the Child, General Comment No.12, states 'The views expressed by children may add relevant perspectives and experience and should be considered in decision-making, policymaking and preparation of laws and/or measures as well as their evaluation.'[18] We believe this should include a voice in the creation of safety standards for industry.

Leadership of standard development for industry

The Foundation does not support the primary approach of Section 137 of the Online Safety Act: that bodies or associations representing the online industry should develop codes under the Act. Granting industry the autonomy to create its own regulatory codes in relation to children's online safety raises grave concerns about profit being prioritised over the wellbeing of vulnerable individuals. This raises the risk of online services ending up with insufficient safeguards, potentially exposing children to harm. We believe the development of online safety codes should be led by an independent, expert, trusted regulator.

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

Dr Jessie Mitchell, Manager, Advocacy
[redacted]

Sarah Davies AM, CEO
[redacted]

Ariana Kurzeme, Director, Policy & Prevention
[redacted]

[1] United Nations (UN) Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[2] UNICEF, 'Ending Online Child Sexual Exploitation and Abuse,' New York, 2021, https://www.unicef.org/media/113731/file/Ending%20Online%20Sexual%20Exploitation%20and%20Abuse.pdf
[3] 5Rights Foundation, 'Approaches to children's data protection: a comparative international mapping,' 2022, https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf
[4] UN Convention on the Rights of the Child, 'General comment No.25'
[5] UK Information Commissioner's Office, 'Protect children's privacy by default' (Children's code design guidance), accessed Dec 2023, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/protect-children-s-privacy-by-default/#:~:text=Settings%20must%20be%20%27high%20privacy,provide%20and%20never%20change%20them.
[6] 5Rights Foundation, 'Approaches to children's data protection'
[7] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey,' Canberra, 2023, https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf
[8] Consumer Policy Research Centre, 'Not a fair trade: consumer views on how businesses use their data,' 2023, https://cprc.org.au/wp-content/uploads/2023/03/CPRC-working-paper-Not-a-fair-trade-March-2025.pdf
[9] Australian Government, Behavioural Economics Team, 'Harnessing the Power of Defaults,' Governance note, https://behaviouraleconomics.pmc.gov.au/sites/default/files/resources/harnessing-power-defaults.pdf
[10] UK Information Commissioner's Office, 'Protect children's privacy by default'
[11] Australian Centre to Counter Child Sexual Exploitation, 'Understanding community awareness, perceptions, attitudes and preventative behaviours,' Research report, 2020, https://accce.prod.acquia-sites.com/sites/default/files/2021-02/ACCCE_Research-Report_OCE.pdf
[12] eSafety Commissioner, '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%20-%20Parental%20awareness%20of%20children%27s%20exposure%20to%20risks%20online%20-%20FINAL.pdf
[13] WeProtect Global Alliance, 'Global Threat Assessment 2023,' https://www.weprotect.org/global-threat-assessment-23/#full-report
[14] UK Information Commissioner's Office, '1. Best interests of the child,' Age appropriate design code: a code of practice for online services, accessed Dec 23, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/
[15] NSW Health, 'New child abuse related offences - failure to report and failure to protect,' accessed Dec 23, https://www.health.nsw.gov.au/parvan/childprotect/Pages/criminal-justice-changes.aspx ; Northern Territory Office of the Commissioner for Public Employment, 'Make a report,' accessed Dec 23, https://ocpe.nt.gov.au/working-in-the-public-sector/support-and-counselling/domestic-family-and-sexual-violence/make-a-report ; Victorian Government Department of Justice and Community Safety, 'Failure to disclose offence,' accessed Dec 23, https://www.justice.vic.gov.au/safer-communities/protecting-children-and-families/failure-to-disclose-offence
[16] WeProtect Global Alliance and UNICEF, 'The Model National Response Maturity Model,' accessed Dec 23, https://www.weprotect.org/model-national-response/
[17] UN Convention on the Rights of the Child, 'General comment No.25'
[18] UN Convention on the Rights of the Child, 'General comment No.25'