alannah & madeline foundation

South Australia Children (Social Media Safety) Bill 2024

Submission by the Alannah & Madeline Foundation

September 2024

Contents

Executive summary 3
About us 4
Recommendations 4
Risks inherent to the design and function of digital services 5
Aligning with a Children's Online Privacy Code 6
Strengthening the 'duty of care' framing 7
An approach to age assurance that upholds children's rights 8
Regulation of social media services in relation to children 9

Executive summary

The Alannah & Madeline Foundation (the Foundation) welcomes the opportunity to take part in the Government of South Australia's public consultation on the draft Children (Social Media Safety) Bill 2024.

Our response is high-level due to the consultation's tight timeframes and our commitment to focus on national reforms.

The object of the draft bill is commendable: 'to prevent or mitigate the risk of psychological and other harms to children flowing from unrestricted access to social media platforms and services'. We welcome the Government's concern for children's safety and commitment to address threats at a systems level.

For too long, many digital technologies have been designed and functioned in ways which are inappropriate or unsafe for children, with responsibility for managing risk pushed back onto parents, teachers and children themselves. That approach is unethical and unacceptable. It is positive that the Government has recognised this and is committed to change the picture.

The draft bill includes a provision to create an enforceable 'duty of care' for social media services, with options for legal redress for children who have suffered harm as a result of a breach of a service's duty of care. It also makes provision for a Children's Online Safety Fund to support 'research into the provision of safe and beneficial social media services for children', 'education programs relating to social media safety for children', and 'discretionary payments for the benefit of children who have, in the opinion of the Regulator, suffered mental or physical harm as a result of a breach of duty of care under this Act.'

It is very interesting to see a shift towards a 'duty of care' framing for social media services and levying of funds from services to address systemic failings. This signals a positive move towards holding industry responsible in a tangible way for the safety of their services.

However, we have significant concerns about the primary focus of the draft bill: to prevent children under 14 from accessing social media services and to require parental consent for access by 14- and 15-year-olds. This approach does not address the commercial model of many digital platforms (not just social media services) which pose risks to all children under 18.

The basis of many digital technologies, including social media services, is the handling of individuals' personal information in a competitive 'attention economy'. Services are designed and run in ways which are intended to maximise the reach of the service, the time individuals spend there, and individuals' interactions on the service. As a result, services are highly engaging, difficult to stop using, and enable or encourage risky behaviours such as contact with strangers and engagement with inappropriate content. Services handle vast amounts of personal information, including about children, which is shared with third parties and used for direct marketing and targeting of content and contacts to users.

An enforced age limit for social media, while well-intentioned, does not address those issues. It may even give a false impression that children's online safety risks have been 'fixed'. This impression would be especially concerning given the imperfect nature of age assurance solutions at present.

We urge the Government of South Australia to ensure any reforms align with relevant national regulation and legislation. Especially significant are the reforms to the Privacy Act 1988 and the review of the Online Safety Act 2021. The privacy reforms have led to plans to create a Children's Online Privacy Code to transform the way industry treats children's personal information. Meanwhile, it is possible the Online Safety Act will be reformed to include a 'duty of care' requirement more comprehensive than that in this draft bill.

Finally, it is vital that any adoption of age assurance measures prioritises upholding children's rights and adheres to a high standard of safety, security, privacy and accessibility.

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. 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. Commit to align workably with the national regulatory framework established under the Online Safety Act 2021 and take into account the review of the Act underway at present.

2. Widen the framing of 'duty of care' to require social media services to assess, identify, prevent and mitigate threats to the rights of children under 18 on and through their services.

3. In the event of a statutory 'duty of care' for digital services being introduced into the Online Safety Act 2021, ensure South Australian systems align workably with it.

4. Support the creation, implementation and enforcement of a national Children's Online Privacy Code, as announced by the Australian Government in line with proposal 16.5 of the report of Privacy Act Review. Commit to full alignment with the Code, including in relation to age assurance and exemption of certain services from age-gating.

5. In the interim, commit that any age assurance measures encouraged or required by the Government of South Australia will:

    a. align with the 'Joint statement on a common international approach to age assurance,' led by the UK Information Commissioner's Office, and –
    b. align with the relevant proposals of the Privacy Act Review report which have been accepted or accepted in principle by the Australian Government, including those which would prohibit trading in children's personal information and prohibit targeting and direct marketing to children unless in the best interests of the child.

6. Support the development of 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 has been highlighted by eSafety.

7. In line with the advice of the French review, ensure the criteria for determining 'exempt social media services' and 'reasonable steps' for compliance with duty of care (ie. age assurance) are developed in consultation with eSafety, industry and independent experts. We urge that this consultation also includes meaningful engagement with children, young people, parents, carers and the Privacy Commissioner.

8. In determining how a Children (Social Media Safety) Act will be regulated, work closely with the eSafety Commissioner, the Privacy Commissioner, and South Australia's Commissioner for Children and Young People. The best approach will be one which maximises the likelihood of upholding children's rights while aligning workably with national legislation and regulation. The French review allowed for the establishment of a standalone Regulator or the conferral of functions onto an existing state regulator or the eSafety Commissioner.

Risks inherent to the design and function of digital services

Nowadays, digital technologies are ever-present in families. By the ages of 10-13, more than half of Australian children have their own phones, almost half have a gaming account, and one-third are on social media.[1] Children use 'edtech' products in school and 'smart devices' at home. New technologies bring many benefits, but they also create new problems which laws must evolve to address.

The report by the Hon. Robert French AC recognises that the technological landscape is 'data driven' and that the 'datafication' of children is a priority for the Australian Government in relation to privacy reform. Such issues are key to understanding risks to children online.

Many risks to children's safety on social media services and other digital services stem from the services' underlying commercial models, which aim to maximise the handling of individuals' personal information in an 'attention economy'.

In consequence, children are using digital services which were designed to maximise the time users spend there, their interactions on the service, and the reach of the service. All the while, children's personal information is being collected, analysed and monetised on a vast scale.

This is why social media services are highly engaging and difficult to stop using, connect people with ever-expanding networks, and reward content creation, interaction and popularity. Design features which serve these ends include notifications, popularity measures, the 'infinite scroll', low-privacy default settings, recommender systems for content and contacts, anticipation mechanisms (eg. dots to show someone is messaging), ephemeral content, activity measures (eg. read receipts), cross-platform contact sharing, video autoplay, location tracking, disguised advertising, and weak age-gating of adult products like pornography.

Such features lead to children (and adults) spending excessive time on platforms, losing control of private information, connecting with strangers, feeling anxious or out of control about their tech use, and encountering extreme, inappropriate or 'echo-chamber' content.[2]

Social media services are not the only services that operate in this way. For example, educational technologies ('edtech') exploded into schools during the pandemic and remain prolific. Many handle data about children's learning, identification and wellbeing extensively and unscrupulously eg. sharing children's data with advertising companies for targeted marketing.[3]

(Note: the French review suggests that social media services exempt from the enforced age limit would include services provided by educational authorities, such as services whose access is controlled by a classroom teacher for teaching purposes. While we do not want such services banned, we note that in their handling of children's data they are not necessarily 'safe' at all.)

Meanwhile, generative AI poses new risks. Recently, there was a shocking case where photographs of Australian children were 'scraped' from the web (including from relatively private online spaces) and used to train popular AI tools without the knowledge or consent of the children or their parents.[4] Meanwhile, although the Australian Government has introduced welcome legislation to address creation and sharing of deepfake image-based abuse, the 'undressing apps' which enable this disgraceful practice are prolific and profitable. For example, the social network analysis company Graphika identified over 24 million unique global visitors to 34 'undressing' websites in September 2023 alone.[5]

Thus, risks affect children of all ages on many different digital platforms. Indeed, teens over the age of 14 tend to have *more* high-risk experiences online than younger children,[6] probably reflecting lower parental supervision and higher risk-taking tendencies in adolescence.

We are concerned that well-intentioned decision-makers may assume they have resolved child safety issues in the digital environment by banning under-14s from social media. In fact, risks to all children under 18 are 'baked into' a wide array of digital technologies. To really address these concerns, we must change the design of these platforms and restrict what they may do with children's personal information.

Aligning with a Children's Online Privacy Code

In light of the above concerns, we strongly supported the announcement by the Australian Government that a Children's Online Privacy Code will be created and registered within two years of the Privacy and Other Legislation Amendment Bill 2024 being passed into law. Under the terms of the draft bill, an enforceable Code will be developed and registered by the Information Commissioner to apply to all social media services, relevant electronic services and designated internet services likely to be accessed by children under 18 (excluding legitimate health services).

A high-quality Children's Online Privacy Code could force positive changes to digital platforms. For example, it might require platforms to set children's accounts to private by default, switch off geolocation and profiling options by default, and not 'nudge' children to provide personal information, unless these things are in the best interests of the child. It might even ban the recommender systems that have historically connected children to age-inappropriate content and contacts. A Code could also require platforms to have age-appropriate mechanisms for children to report problems and seek help.

Supporting and aligning with a Code would help the Government of South Australia to address the strong public appetite for better privacy protections for children[7] and would have significant positive flow-on effects for online safety.

Furthermore, we argue that a strong, child-rights-based Code to determine what digital platforms may do with children's personal information is essential for any jurisdiction that wishes to implement age assurance or distinguish between high- and low-risk digital services.

In the draft bill, the Government of South Australia makes provision for a duty of care for social media services to 'take all reasonable steps' to prevent access by children, recognising this will mean age verification and estimation mechanisms. The draft bill also makes provision for 'exempt social media services' to be excluded from enforced age limits. The French review advised that exempt services are those which 'pose little or little significant risk to children', adding:

> 'The criteria for determining an exempt social media service and guidance as to what might constitute "reasonable steps" to comply with the statutory duties would have to be developed by the regulator drawing upon the expertise and experience of the Commonwealth eSafety Commissioner's office, age assurance providers, social media service providers, independent experts and other stakeholders.'[8]

We submit that it will also be essential to draw upon the expertise of the Privacy Commissioner and, in future, ensure alignment with the Children's Online Privacy Code.

Strengthening the 'duty of care' framing

The draft bill proposes to introduce a duty of care for any (non-exempt) social media service to take reasonable steps to prevent access by any child in South Australia under the age of 14 and to any child aged 14 or 15 who does not have parental consent. Should social media services contravene this duty of care, the Regulator will have powers to serve infringement notices. The Supreme Court may issue compensation orders if a breach of duty of care is found to be wilful, reckless or repeated.

Broadly, we welcome the adoption of a 'duty of care' framing in relation to social media services' treatment of children. This represents a step away from the historical approach of pushing responsibility for online safety back onto individual users, including children.

However, we believe a duty of care should not revolve simply around the enforcement of a social media service's age limit.

We note that the French review engaged with the Online Safety Act reviewers and the National Children's Commissioner to discuss 'The utility of imposing a duty of care on social media providers as opposed to a ban', 'The ways the duty of care may be approached' and 'Defining the duty of care to encourage social media platforms to take proactive action on online safety'.[9]

Meanwhile, the current review of the Online Safety Act included in its terms of reference the matter of 'Whether the regulatory arrangements, tools and powers available to the [eSafety] Commissioner should be amended and/or simplified, including through consideration of … the introduction of a duty of care requirement towards users (similar to the United Kingdom's Online Safety Act 2023 or the primary duty of care under Australia's work health and safety legislation)'.[10]

The Online Safety Act review's issues paper elaborated 'A statutory duty of care approach places duties on the entities who control and are responsible for a hazardous environment to achieve a desired outcome (harm prevention) … A statutory duty of care includes an overarching obligation to exercise care in relation to user harm (including through risk assessments and implementing mitigation measures).'[11]

In our submission to the Online Safety Act review, we supported the idea of a duty of care framework and argued that it should include an enforceable requirement for providers of digital products and services to treat the best interests of the child as a primary consideration in any decisions affecting children. Platforms should demonstrate this commitment through child rights impact assessments to identify, prevent and address threats to children's rights.

A service might also demonstrate its upholding of a duty of care by embedding a 'safety by design' approach and by making industry data about online safety available to regulators and researchers.

The age limit for social media in South Australia may be raised to 14 and enforced, but children aged 14-17 (as well as any younger children who manage to bypass the age assurance mechanism) will still be using social media. As such, we urge that a 'duty of care' obligation for social media services should go beyond age-gating and require providers to take meaningful steps to identify, prevent and address threats to all children under 18 that occur on and through their services.

An approach to age assurance that upholds children's rights

In proposing to restrict social media services to ages 16+ and to 14- and 15-year-olds with parental permission, the draft bill implies the adoption of some form of age assurance. The French review anticipated that 'age verification and estimation mechanisms' would be required.

The French review also stated 'But the means currently available for verification and estimation are still in development. The hard fact is that there is no error free means of determination of the age of users of an account.'[12] French highlighted the need for eSafety's expert advice on this matter.

We believe it is important that Australian jurisdictions are proactive in understanding and appropriately regulating new and emerging technological 'solutions' to age assurance – an umbrella term which refers to a range of approaches that establish age to varying levels of certainty.

Age assurance can play a valuable role in relation to children's online safety. For example, the Foundation welcomed the news that the eSafety Commissioner would pilot an age assurance trial aimed at preventing children's exposure to pornography. eSafety's proposed approach – tokenised, double-blind, informed by the euCONSENT model – appeared ethical and proportionate to the risks pornography poses to children.

However, age assurance is not a magic wand. It only identifies that a child is present; it does not make digital products or services safe or appropriate for children.

Many digital platforms could bypass the need for age assurance by designing their products and services to be safe for children in the first place. Recognition of this fact is implied by the draft bill's carve-out of exemptions for social media services assessed to pose 'little or little significant risk to children' and the creation of a Fund that would research 'provision of safe and beneficial social media services for children'.

In contrast, a social media platform whose primary safety measure is age-gating to exclude under-14s might still be very unsafe for 14- to 17-year-olds (and any younger children who succeed in gaining access).

That said, age assurance technologies might well have a significant future in Australia, and it is vital to prepare. Age assurance solutions are immature but evolving rapidly.[13] eSafety notes that industry stakeholders like Roblox, Google, Yubo and Meta have trialled, or announced their intention to trial, various approaches using ID scans, selfies, and facial age estimation technology.[14]

Regulation of age assurance has been poor. A report commissioned by the UK Information Commissioner observed 'These products have emerged largely in a standards lacuna.'[15] This creates a new set of risks to children eg. that companies will use age assurance technologies to maximise collection, sharing and use of children's personal information, including in potentially invasive areas like biometrics.

As noted earlier, the development of a Children's Online Privacy Code will be vital here. In the interim, we urge the Government of South Australia to support and align with the following proposed or pending approaches in relation to age assurance:

- eSafety's call for a regulatory scheme for the accreditation and oversight of age assurance providers in Australia to promote privacy, security, strong governance, transparency, trustworthiness, fairness, and respect for human rights.[16]

- The proposals of the Privacy Act review (accepted in principle by the Australian Government) to prohibit trading in children's personal information; prohibit targeting and direct marketing to children unless it is in the best interests of the child; require that collection notices and privacy policies be clear and understandable to children; and require that entities have regard to the best interests of the child when considering whether collection, use or disclosure of children's personal information is fair and reasonable in the circumstances.[17]
- The 'Joint statement on a common international approach to age assurance' led by the UK Information Commissioner's Office, which states that age assurance should be (amongst other things) lawful, proportionate, transparent, non-discriminatory, up-to-date, privacy-preserving and accountable. Providers should collect only the information necessary for the purpose of age assurance, be guided by the best interests of the child, and recognise that other approaches like education and safety-by-design are also needed in order to keep children safe online.[18]
- The elements of a high-quality system for verifying personal details without sharing unnecessary documentation or information eg. a system that is tokenised, double-blind, reusable – identified by the Australian Government in their work to introduce a Digital ID System and a Trust Exchange (TEx) system.[19]

It is important to ensure that new technologies function to benefit children and not to harm or exploit them.

Regulation of social media services in relation to children

The draft bill proposes to create a Regulator of Child Social Media Safety. The regulator's role would include serving infringement notices to services that contravene their duty of care; bringing legal action against services on behalf of children who have suffered harm as a result of social media access; determining which social media services should be exempt from age-gating; determining what constitutes 'reasonable steps' for services to uphold their duty of care; and managing the Children's Online Safety Fund. The Fund would consist of payments from services which have contravened their duty of care, with possible additional funds from government. It is anticipated that the Fund could be used to fund social media safety research and education for children, as well as to support children who have suffered harm.

We see merit in the idea of leveraging resources to support children's online safety from industry stakeholders who are found to have failed in that respect. This seems a fairer approach than leaving families, schools and police to cope alone with problems which occurred partly due to unsafe design and/or operation of services.

We also welcome the prospect of more resources for online safety education and research.

However, we have some hesitation about the idea of a bespoke state regulator, given the time and resources involved and the importance of national reform in this space. The French review suggested that alternative approaches could be to confer additional functions to an existing state regulator or eSafety.

We urge that the approach adopted should be one which maximises the likelihood of children's rights being upheld in full in ways which align workably with national regulation and legislation.

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] Office of the Australian Information Commissioner (OAIC), 'Australian Community Attitudes to Privacy Survey 2023,' 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
[2] 5Rights Foundation, 'Disrupted Childhood: The cost of persuasive design,' 2023, https://5rightsfoundation.com/in-action/disrupted-childhood-the-cost-of-persuasive-design-2023.html ; 5Rights Foundation, 'Pathways: how digital design puts children at risk,' 2021, https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf
[3] Human Rights Watch, ' "How dare they peep into my private life?" Children's rights violations by governments that endorsed online learning during the Covid-19 pandemic,' 2022, https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
[4] Human Rights Watch, 'Australia: Children's Personal Photos Misused to Power AI Tools,' 2024, https://www.hrw.org/news/2024/07/03/australia-childrens-personal-photos-misused-power-ai-tools
[5] Graphika, 'A Revealing Picture,' 2023, https://www.graphika.com/reports/a-revealing-picture
[6] eSafety, 'Mind the Gap: Parental awareness of children's exposure to risks online,' 2022, https://www.esafety.gov.au/research/mind-gap
[7] OAIC, 'Australian Community Attitudes to Privacy Survey 2023'
[8] The Hon. Robert French AC, 'Report of the Independent Legal Examination into Banning Children's Access to Social Media,' 2024, https://apo.org.au/node/328256
[9] French, 'Report of the Independent Legal Examination into Banning Children's Access to Social Media'
[10] Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Statutory Review of the Online Safety Act 2021,' 2024, https://www.infrastructure.gov.au/department/media/publications/statutory-review-online-safety-act-2021-issues-paper
[11] Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Statutory Review of the Online Safety Act 2021'
[12] French, 'Report of the Independent Legal Examination into Banning Children's Access to Social Media'
[13] 5Rights Foundation, 'But how do they know it's a child? Age assurance in the Digital World,' 2021, https://5rightsfoundation.com/resource/but-how-do-they-know-its-a-child/ ; Tony Allen, Lynsey McColl, Katharine Walters, Harry Evans, 'Measurement of Age Assurance Technologies,' ICO, 2022, https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf ; eSafety, 'Roadmap for age verification,' 2023, https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf ; Ofcom and ICO, 'Measurement of Age Assurance Technologies,' 2021, https://www.drcf.org.uk/publications/papers/measurement-of-age-assurance-technologies
[14] eSafety, 'Roadmap for age verification'
[15] Ofcom and ICO, 'Measurement of Age Assurance Technologies,' 2021, https://www.drcf.org.uk/publications/papers/measurement-of-age-assurance-technologies
[16] eSafety, 'Roadmap for age verification'
[17] Australian Government, 'Response: Privacy Act Review Report,' 2024, pp.27, 29, 33
[18] UK Information Commissioner's Office, 'Principles,' 2024, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/joint-statement-on-a-common-international-approach-to-age-assurance/principles/
[19] Australian Government, 'How Digital ID Works', 2024, https://www.digitalidsystem.gov.au/what-is-digital-id/how-digital-id-works ; Australian Government, 'The Trusted Digital Identity Framework,' 2024, https://www.digitalidsystem.gov.au/tdif ; Toby Murray, 'The government is developing a new digital ID system. It must first gain the public's trust,' *The Conversation*, 13 Aug 2024, https://theconversation.com/the-government-is-developing-a-new-digital-id-system-it-must-first-gain-the-publics-trust-236689