Submission to the Environment & Communication Reference Committee's inquiry into the Internet Search Engine Services Online Safety Code

Executive Summary

This submission presents a child rights analysis of the proposed approach to age verification in Australia. It addresses questions 4 (alternative technical approaches), 6 (global experience) and 7 (other matters), and addresses some key misalignments and complications identified. Specifically:

- *On alternative technical approaches to online safety for all users, including young people.* Australia appears to have landed on an 'age-assure first' approach. Alternative models that focus on safety standards and settings first exist, and these may better advance children's rights in the digital environment.

- *On global experiences and best practice.* A number of international examples of 'safety-setting-first' have been implemented around the world, including in the UK's *Age Appropriate Design Code* and the EU's *Digital Services Act.* It is important to note that the implementation of these Codes and Acts has not been straight forward. There have been significant challenges in determining what 'safety first' means, e.g. what 'features' need to be turned on, and what content these filter out. But these challenges are different in nature to the challenges of age assurance. In short, there are no perfect solutions, but other models have merit.

- *Other matters*:
  - The co-regulatory nature of the Internet Search Engine Services Online Safety Code for Class 1C & 2 material (the 'Code'), and the process through which it was produced, is fundamentally flawed. This has inherently affected the quality of the Code, and it does not achieve the most robust child rights outcomes. The flaws in the process alone are enough to warrant their review and potential replacement with regulator drafted Codes (or Standards).
  - The Social Media Minimum Age legislation (SMMA) was rushed through parliament with an inadequate public consultation window. This warrants a timely review of the SMMA.
  - The public appear to be unaware that age assurance for internet search engines and social media platforms is coming, with 46% 1,501 adults polled not aware that age assurance for search engines was coming, and 22% unaware it was coming for search engines.They also hold a level of discomfort around the concept of age assurance, which varies by method. While this may not be a problem in its own right, it speaks to a need for more public debate and dialogue about these issues.

We recommend a renewed focus on systemic regulations that drive up safety standards on search engines and social media platforms. This could be in addition to, or instead of, current approaches.

We should remember that the issues that the Code and the SMMA are attempting to address are caused by endemic industry failure on safety standards. An approach that requires individual Australians to age-assure because of industry failures is not a fair and balanced response. A number of specific changes that could be implemented in the anticipated reform to the *Online Safety Act* are suggested.

This is a joint submission from the Australian Child Rights Taskforce, ChildFund Australia and Dr Rys Farthing, University of Canberra.

Contents

Introduction . 1
Alternative technical approaches to online safety for all users 2
Global experiences and best practice 5
Other matters 7
- Co-regulation is a flawed process that was destined to deliver poor Codes 7
- The speed of the SMMA development and implementation also causes concerns 8
- A lack of community preparedness 8
- The broader need for systemic, platform accountability 11
- The broader need to uplift digital literacy 12

Recommendations 13

About the signatories

The Australian Child Rights Taskforce is a civil society coalition of over a hundred organisations and individuals committed to the protection, promotion and fulfilment of the rights of all children and young people in Australia. The Taskforce contributes to policy and practice development in child rights and in supporting the participation of children and young people in decision making in their lives. In listening to the views and experiences of children and young people, the Taskforce recognises and supports the importance of respecting their rights in the digital world as part of their lived experiences.

ChildFund Australia is an independent international development organisation working to end poverty for children in the world's most vulnerable communities. We partner to create change for children and young people – in all their diversity – to realise and assert their rights.This includes advancing digital rights, equipping children and communities with online safety skills, advocating for system change, and strengthening support services when online harm occurs.

Dr Rys Farthing is a Professorial Research Fellow at the News and Media Research Centre (N&MRC) at the University of Canberra. She is the primary author of this submission. The N&MRC advances public understanding of the changing news and media landscape, and advocates for a media system that builds trust, inclusivity and diversity, to defend and repair the social fabric.

UNIVERSITY OF CANBERRA | NEWS AND MEDIA RESEARCH CENTRE

AUSTRALIAN CHILD RIGHTS TASKFORCE

ChildFund Australia

Introduction

Through a combination of recent policy initiatives — especially the Social Media Minimum Age Amendments ('SMMA') and the Internet Search Engine Services Online Safety Code for Class 1C & 2 material ('the Code') — Australia appears to have arrived at an 'age-assurance-first' approach.

This approach misaligns the problem with the solution. The impetus for both of these regulations is the historically poor safety practices that abound across digital platforms and search engines, but the target for the solution is end users. That is, the key problem is an industry failing and the key actors are industry, however instead of addressing industry directly, this remedy requires individual Australians users to age-assure. The onus of responsibility for causing the issue and creating the remedy do not align. Driving up safety standards more broadly through regulation that targets industry is an alternative way of remedying the problem at hand, and may better advance children's safety, privacy and rights online.[1]

Age assurance is not without its challenges and complications, from privacy concerns to technical limitations, as extensively documented in the findings from the recent age verification trials.[2] Ideally, reliance on age assurance should be minimised to advance children's rights in the online environment. We note that the complications of age assurance in Australia will be dependent on what is determined to be 'reasonable' by regulated platforms and search engines. That is requirements under the Code[3] and the SMMA[4] rest on requirements for *reasonably* practical measures or *reasonable* steps to age-assure, respectively. While guidance around age assurance suggests it can be relatively 'light touch' and proportionate,[5] it is still unclear how these will be interpreted and operationalised by platforms. Therefore, it is still worthwhile considering how these complications might affect children's rights, including safety and privacy.

This submission explores these complications and misalignments from a child rights perspective. It addresses questions 4 (alternative technical approaches), 6 (global experience) and 7 (other matters).

This is a joint submission from the Australian Child Rights Taskforce, ChildFund Australia and Dr Rys Farthing (Professorial Research Fellow at the University of Canberra). We welcome this inquiry, and the opportunity to explore how these policy initiatives affect children's rights more broadly.

---

[1] This is not to suggest that age assurance has no place in online safety, just that it is not the only possible approach

[2] Age Check Certification Scheme (2025) *Age Assurance Technology Trial Part A Main Report*, available online at https://ageassurance.com.au/report/

[3] Compliance measure 2 outlines that 'where technically feasible and *reasonably practicable*, a provider of an internet search engine service must: implement appropriate age assurance measures for account holders…' (emphasis added) See AMTA, CESA, DIGI & IGEA (2025) *Schedule 3 – Internet Search Engine Services Online Safety Code (Class 1C & 2 Material)*, available online at https://onlinesafety.org.au/wp-content/uploads/2025/07/Schedule-3-Internet-Search-Engine-Services-Online-Safety-Code-Class-1C-and-Class-2-Material.pdf

[4] Part 1 of Schedule 1 of the amendments that formed the SMMA outlined that 'there are age restrictions for certain social media platforms. A provider of such a platform must take *reasonable steps* to prevent children who have not reached a minimum age from having accounts' (emphasis added). See *Online Safety Amendment (Social Media Minimum Age) Bill 2024,* available online at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7284

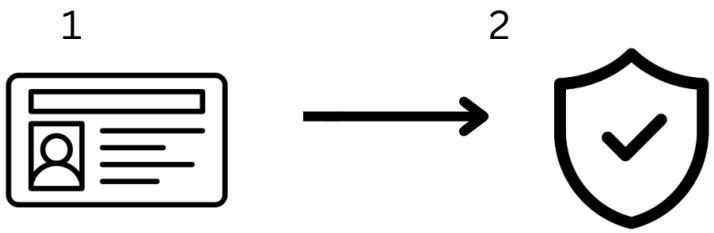
[5] Office of the eSafety Commissioner (2025) *Social Media Minimum Age Regulatory Guidance* online at https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1757993771370

Alternative technical approaches to online safety for all users, including young people

From a child rights perspective, it is unclear why an age-assurance-first approach is necessary to advance children's rights online. Alternative models exist that require driving up safety standards first, and then using age assurance as and if necessary (which we call here a 'safety-settings-first' approach).

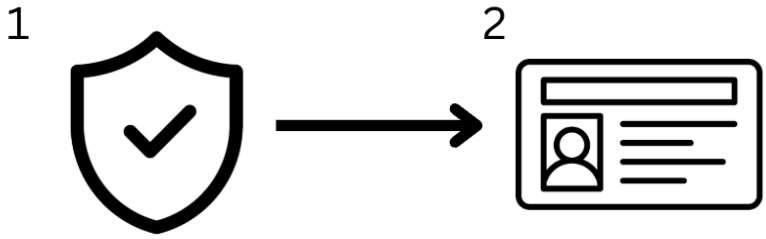
This approach relies on increasing safety standards on platforms overall and the strategic use of default settings, and should deliver better safety outcomes for child users online. For example, it is unclear from a child rights perspective why all internet search engines would be required to age-assure account holders, and *then* apply 'safe search' and other safety features to children's accounts. An alternate, safety-settings-first approach could require search engines to turn on safe search options for all accounts and anonymous searches, and age-assure only where an account holder wants to turn off 'safe search' features (see Figure 1). This has the effect of minimising the amount of age assurance that is needed, and provides a way for users to continue to use their accounts without having to go through age assurance processes. In an old school analogy, this is akin to allowing anyone into the Blockbuster video store, and only checking ages when people try to enter the adult video room at the back. It reduces the amount of age assurance checks needed to the bare minimum to achieve the aim.

Age-assure first approach



Age-assure all account holders, and *then* turn on safety features when a child is identified

Safety-setting first approach



Turn on safety settings and features for everyone, and *then* age-assure if/when users want to turn them off

Figure 1: An overview of an 'age assurance first' approach compared to a 'safety feature first' approach

When compared to a 'safety-settings-first approach, an age-assurance-first approach also produces four distinct 'gaps' that challenge the advancement of children's rights.

Firstly, an age-assure first approach creates a loophole that may undermine children's safety outcomes. Under the Code, where age assurance is required first, to *then* trigger application of safety-settings, users who are not logged in to registered accounts may not necessarily have safety-settings turned on by default. This is not a strong safety outcome for children. The Social Media Minimum Age requirements suffer from a similar flaw. Children can still view and access harmful content — still prioritised and ordered by the risky algorithms that drive them — by using social media platforms while logged out.[6]

We note that we are *not* calling for more blocking, nor for the prevention of anonymous search nor for social media content to be inaccessible while logged out. These would be worse outcomes for all, including children. Instead, we are pointing out that the current approach does not deliver the outcomes outlined in the Second Reading speech,[7] where a focus on safety standards might better achieve it.

Secondly, an age-assure first approach compared to an overall safety-settings first approach, misses many of the risks young people experience online. Further, a focus on driving up general safety standards, through the use of safety settings and so on, may address a more comprehensive range of risks for children in the digital environment. The OECD,[8] and global experts Sonia Livingstone and Maria Stoilova[9] — as adopted by the European Commission in their approach to protecting children online— have developed a typology of online harms that identifies five C's ('5C's') of harms (see Figure 2).

	Content	**Conduct**	**Contact**	**Consumer**
Risk	Children accessing inappropriate content, hateful, harmful, pornographic, illegal, and inauthentic content (bots, AI slop etc) risks	Children behaving inappropriately (e.g. cyberbullying). Including hateful, harmful, illegal, and other problematic behaviour	Inappropriate contacts with children (e.g. grooming). These can be hateful, harmful, illegal, and problematic contacts	Consumer and financial risks for children online, e.g marketing, scams, commercial profiling, financial and security risks
Cross cutting	Risks that are inherent to the contemporary digital world such as privacy, advanced and immersive technology risks, risks of overuse and misuse, risk to health and wellbeing etc			

Figure 2: The 5C's typology of online risks for children

All of the 5C's may 'manifest when appropriate and proportionate measures are not in place to ensure a high level of privacy, safety and security for minors on the service, causing potential infringement of a

[6] For example, one of the authors of this paper undertook a quick, ad hoc 'experiment' looking at what YouTube Shorts would recommend to a logged out, Australian account. They found that a logged out account that searches 'White Replacement Theory' will be served videos (shorts) of Thomas Sewell, 'white grievance' content such as Tucker Carlson and videos about the radicalism of religions etc. Out of the 50 sequential videos (shorts) they recommended while logged out, 23 were loosely considered 'race-aligned' material. This was not an evaluation of the nature of the content, rather a technical analysis of the capacity for 'un-logged in accounts' to enter content specific rabbit holes quickly. If this is of interest to the Committee, a more systematic research briefing can be developed.

[7] As described by Minister Rowland 'for too many young Australians, social media can be harmful. Almost two-thirds of 14- to 17-year-old Australians have viewed extremely harmful content online, including drug abuse, suicide or self-harm, as well as violent material. A quarter have been exposed to content promoting unsafe eating habits.' The harms noted were all content harms — content that children will continue to be able to access on social media platforms by not logging in to an account. See Michelle Rowland (2024) *Second Reading Speech, Online Safety Amendment (Social Media Minimum Age) Bill 2024*, available online at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F28041%2F0017%22

[8] OECD (2021) *Children in the digital environment - Revised typology of risks,* available online at https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html

[9] Sonia Livingstone & Maria Stoilova (2021). *The 4Cs: Classifying Online Risk to Children*, available online at https://doi.org/10.21241/ssoar.71817

number of children's rights'.[10] An age-assurance-first approach as adopted in the Code may help minimise risks associated with content, but it does not address conduct, consumer, contact or cross-cutting risks. Likewise, the SMMA approach does not address any of these risks for 16 & 17 year olds, nor does it actually reduce the 'risk profile' of platforms with regards to the 5C's inherently, as discussed in 'Other Matters' below. Focussing on safety standards and settings first may deliver better, more comprehensive child rights outcomes.

Thirdly, the privacy and accuracy concerns around age assurance methods also affect children, and reliance on age-assurance maximises these challenges to children. Children have the right to privacy as enshrined in the Convention on the Rights of the Child.[11] Global child rights experts have noted that age verification techniques and children's privacy interact, noting that sadly 'age assurance is often ineffective in protecting children from online risk of harm. Further, as currently implemented it risks children's other rights – to non-discrimination, privacy, to be heard, and their civil rights and freedoms, and remedy'.[12] At the same time as age assurance is being used in the Australian digital policy landscape, Australian children's right to privacy online is currently being reaffirmed with the introduction of the Children's Online Privacy Code.

While children's right to privacy is not absolute — and age assurance may have a role to play in the mosaic of interventions needed to ensure children's rights online — when implementing age assurance techniques, children's right to privacy and access should be considered alongside their right to safety. Simply put, age assurance technologies should not be deployed unnecessarily, or at the expense of other more rights respecting approaches.

Lastly, an age-assurance first approach may not be as future proof. Reducing the overall risk profile of digital products will become increasingly important as AI models and systems are deployed. While the problem of safety for unregistered users — as highlighted in Figure 1 — might feel less important in an age of digital platforms, it is set to grow. Social media platforms and search engines by their nature encourage users to create accounts. AI is substantively different. While some AI is deployed on platforms, AI is a technology that can be deployed whether users are aware that they are using a service or not (within and outside of platforms). That is, we know when we are using YouTube so we can choose to log in or not, but we may not be aware when we access underlying Claude AI technology. A focus on driving up safety standards for all users — logged in, logged out, adult, child — could be more future proof.

[10] European Commission (2025) *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065* available online at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors

[11] And reiterated in the UN General comment on children's rights in relation to the digital world. See UN Committee on the Rights of the Child (2021) *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[12] Sonia Livingstone, Abhilash Nair, Mariya Stoilova, Simone van der Hof & Cansu Caglar (2024) 'Children's Rights and Online Age Assurance Systems: The Way Forward'. *The International Journal of Children's Rights*, *32*(3), 721-747. https://doi.org/10.1163/15718182-32030001

Global experiences and best practice

A number of examples of 'safety-settings-first' have been implemented around the world, enhanced by systems-focussed (systemic) regulations to drive up safety standards for users, including in:

- The EU's *Digital Services Act.* The EU's Act takes a systems-focussed, risk-based approach, that includes activating safety-settings first. The Act requires large platforms and search engines to undertake systems focussed risk assessments and mitigate potential risks on their services, including risks to children. Guidelines on the Implementation of Article 28 outline a range of safety settings that large platforms and search engines need to apply when they are reasonably certain that an account belongs to a child,[13] but specifically notes that there is no expectation of additional age assurance to trigger this. Article 28 states that: 'providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service' but that 'compliance with the obligations set out in this Article *shall not oblige* providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor' (emphasis added). The Act requires platforms to turn on these privacy, safety and security settings 'when they are aware with reasonable certainty that the recipient of the service is a minor' — which explicitly does not require additional age assurance.[14]

- The UK's *Age Appropriate Design Code*. The UK Code is a systems-focussed piece of legislation that requires online services to assess for and mitigate against risk (via data protection impact access), without requirements for additional age assurance. For example, where an online platform reasonably expected that it had child users, or might be processing children's data, enhanced privacy and safety features were required to be turned on. This did not require search engines or platforms to implement additional age assurance as a first step — a reasonable expectation that data belonging to a child was enough to trigger additional protections. Standard 3 of the Code notes that the 'code is not prescriptive about exactly what methods (platforms) should use to establish age, or what level of certainty different methods provide', but that platforms 'should always use a method that is appropriate to the risks that arise from your data processing.' That is, if a safety-first (and privacy-first) approach is adopted, the risks presented by data processing decrease. The safer and more private a platform, the less it needs to age-assure.

  Further, the Code outlined that age assurance techniques must be deployed in ways that are privacy respecting. It states that platforms 'may be able to collect and record personal data which provides an assurance of age' but they also 'need to comply with data protection obligations for (the) collection and retention of that data, including data minimisation, purpose limitation, storage limitation and security obligations. The key to this is making sure that (platforms) only collect the minimum amount of personal data (they) need to give (them) an appropriate level of certainty about the age of (their) individual users'.[15]

- The UK's *Online Safety Act*. The UK's *Online Safety A*ct also adopted a systems-focussed, risk-based approach, and requires services to undertake a risk assessment to identify risks to children and mitigate these at a broad level. It required online services to ensure that age inappropriate material

[13] European Commission (2025) *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065* available online at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors

[14] European Commission (2022) *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act),* available online at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

[15] (UK) Information Commissioners Office (2022) *Age appropriate design: a code of practice for online services,* available online at 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/

was not accessible to children. Taking a safety-feature-first-approach, this required digital services to turn off access to this material where users had not assured the platform that they were adults. Ofcom — the regulator in charge of this — has described a relatively robust set of requirements to meet the Regulator's expectations, but again, age assurance is not always necessary where platforms are made safe or as a first resort. For example, PornHub, requires strong methods of age verification to allow access because of the nature of their service. Other mixed risk platforms may choose to turn off access to age inappropriate material, unless a user logs in and assures their age as an adult. We note that the implementation of the UK's *Act* still has had challenges, including building knowledge of what 'safety features' are needed and identifying what content is flagged as 'age inappropriate'. These implementation challenges are more directly focused on identified harms, and provide a more engaged body of knowledge than the narrow technical challenges of age assurance.[16]

Australia appears to be unique in this context, in that it explicitly requires age-assurance first to *then* trigger additional safety settings and standards to be applied for children.

However, the drive for similar principles-based, systemic regulation has not entirely missed Australia. Alongside the introduction of the SMMA and the progressive implementation of the *Online Safety Act* 2021 (which lead to the Search Engine Code), a systemic focus to bring the Act into line with international best practice has been attracting support, including in Government. For example, the Government has committed to the introduction of a Digital Duty of Care.[17]

We support this reform, as it intends to shift the onus of responsibility onto platforms to engineer safer, more rights-respecting products in the first instance. While it is unclear how this duty will be enacted or operationalised, it has the capacity to rebalance Australia's *Online Safety Act* away from a focus on who users are or what they are seeing online, and towards ensuring that digital platforms improve their safety standards (ideally, with greater transparency and accountability).[18] This should shift us closer to what is often described as a 'safety-by-design' approach. In principle, safer, more privacy-respecting products should reduce the need to rely on age assurance mechanisms. For example, legislation 'banning' kids from social media products would not have been necessary if they were safe. Likewise, search engines with strong safety features should reduce the regulatory impetus to create 'walled gardens' for children and young people.

This approach could also be applied consistently to AI products and applications.

[16] These exact same challenges are still needed under the Australian model anyhow, as 'safety features' etc need to be turned on after age assurance. It's simply that this safety-feature-first model somewhat mitigates the complexity and extent of age assurance and all of its complications

[17] The Hon Michelle Rowland (2024) *New Duty of Care obligations on platforms will keep Australians safer online* https://minister.infrastructure.gov.au/rowland/media-release/new-duty-care-obligations-platforms-will-keep-australians-safer-online

[18] For discussion around what a good digital duty of care might look like, see Reset.Tech Australia (2024) *A duty of care in Australia's Online Safety Act,* available online ar https://au.reset.tech/news/briefing-a-duty-of-care/

Other matters

Co-regulation is a flawed process that was destined to deliver poor Codes

Like all of Australia's online safety codes, the *Internet Search Engine Services Online Safety Code for Class 1C & 2 material* was developed through co-regulatory processes. While elsewhere in the world, co-regulation means regulators working with industry and civil society. In Australia, co-regulation means that industry drafts its own code, and the regulator has a constrained role (to sign off or reject these codes) and civil society sits on the sidelines.

This process is inherently flawed and undermines the development of rigorous standards. The Code is framed and authored by tech lobby groups and industry representatives; the Australian Mobile Telecommunications Association (AMTA), Communications Alliance, the Consumer Electronics Suppliers Association (CESA), the Digital Industry Group Inc (DIGI), and the Interactive Games and Entertainment Association (IGEA). There is no incentive for these lobby groups and representatives to set high expectations for themselves.

The failures of co-regulation in Australia to deliver quality outcomes for children's rights has been extensively documented.[19] Firstly, there are many examples where industry has chosen — whether for comfort or for profit — to produce worse safety outcomes when *compared to regulators*. For example, in other online safety codes,[20] the tech lobby set minimum requirements to turn safety and privacy settings to 'high' only for children aged 15-years and under. This defies the definition of a child outlined in the *Online Safety Act* itself which defines a child as up until 18. Elsewhere in the world, where regulators themselves draft codes, minimum requirements around safety and privacy settings protect all children up until the age of 18. Secondly, incredibly, these safety standards are also 'lower' when *compared to common industry practice*. For example, both Meta and TikTok default all accounts belonging to children under the age of 18 to 'high' privacy settings anyhow.[21] Despite this, their industry representatives embedded lower standards in Australia's regulatory framework. This issue is that through the process of co-regulation, industry *could and did* lowball Australian regulatory standards; our Codes are now worse than global norms and worse than common practice.

While the Office of the eSafety Commissioner has some powers to reject draft codes presented for registration where they fail to meet community expectations, this is a relatively blunt option. Further, there is no meaningful mechanism for ensuring informed contributions from civil society. While industry was required to run a consultation around their proposed Codes, we describe this as not a meaningful mechanism. This was experienced as difficult to engage in, contributions were deliberately ignored,[22] and did not allow for sufficient informed input from affected cohorts, including children and young people. In

---

[19] Reset.Tech Australia (2022) *How outdated approaches to regulation harm children,* available online at https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/

[20] Specifically, see compliance measure 7 in AMTA, CESA, DIGI & IGEA (2023) Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material), available online at https://onlinesafety.org.au/wp-content/uploads/2023/06/230616_1_SMS-Schedule_REGISTERED-160623.pdf

[21] See for example Meta (2024) *Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents*, available online at https://about.fb.com/news/2024/09/instagram-teen-accounts/, or TikTok (2024) *TikTok's rules* https://www.tiktok.com/safety/en/guardians-guide

[22] For example, when Reset.Tech Australia raised the issue that the draft Codes presented for consultation did not extend protections to the age of 18, so that 16 & 17 year olds were left at risk, the code drafters responded with "*In response to feedback the Code provisions concerning privacy settings on children's accounts have been amended to apply to children under 16*." I.e. Nothing had been amended at all, and no changes to the draft presented had been made despite the claim they had responded to feedback. See AMTA, CESA, DIGI & IGEA (2022) *Submissions log and industry associations' responses to public consultation feedback*, available online at https://onlinesafety.org.au/wp-content/uploads/2022/11/221118_Submissions-log-responses_FINAL.pdf

all, the process creates a significant power asymmetry that incentivises industry to lowball Australia with weak codes.

It is worth noting that the process of co-regulation has been deemed to be inadequate in other areas of digital regulation, such as the Children's Online Privacy Code and the Scams Prevention Framework. In the former, specific legislation was passed to allow the Privacy Commissioner to draft the Code.[23] In the latter, the Assistant Treasurer outlined how a voluntary code drafted by these same industry groups 'falls short of what is needed and what is expected by the Australian community', while announcing a regulator drafted Code would be developed.[24]

The push to age verify search engines emerges from a discredited and outmoded co-regulation process. The unique co-regulatory process under the *Online Safety Ac*t is obsolete. There must be a commitment under future reforms to review and replacement with informed regulator drafted Codes or Standards that drive safety and appropriate rights protections for all including children and young people.

The speed of the SMMA development and implementation also causes concerns

The Social Media Minimum Age requirement legislation was rushed through Parliament with inadequate public consultation. The window for public and expert consultations to the Environment and Communications Legislation Committee was 24 hours with a request for submissions to be limited to 1-2 pages.[25] In our view, experts, civil society and children and young people themselves were constrained from appropriately engaging due to this process.

And yet the strength of public feeling meant that a total of 15,000 submissions were received.[26] The Committee had to analyse these and write their final report within 4 days. In our view the Committee was also constrained by this process and cannot have had the opportunity to appropriately explore the technical and rights-based issues involved.

Within this context, it is difficult to see how due consideration to the challenges of age assurance were adequately assessed by parliamentary processes to date.

A lack of community preparedness

In September 2025, YouGov polled 1,501 representative adults and found a relative lack of awareness around introduction of age assurance across social media platforms and search engines. Almost half of Australians are unaware that age assurance for search engines is coming (see Figure 3), while one in five are unaware that age assurance for social media platforms is coming (see Figure 4).

[23] *Privacy and Other Legislation Amendment Act* 2024, available online at https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7249
[24] Joseph Brookes (2024) 'Platforms' scam code 'falls short' of $2.7b problem' *InnovationAus*, available online at https://www.innovationaus.com/platforms-scam-code-falls-short-of-2-7b-problem/
[25] Senate Standing Committees on Environment and Communications (2024) *Inquiry into Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]*, available online at https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/SocialMediaMinimumAge
[26] Maani Truu (2024) 'Social media age ban inquiry flooded with 15,000 submissions after Elon Musk weighs in' *ABC,* available online at https://www.abc.net.au/news/2024-11-25/social-media-age-ban-inquiry-flooded-with-submissions/104644208

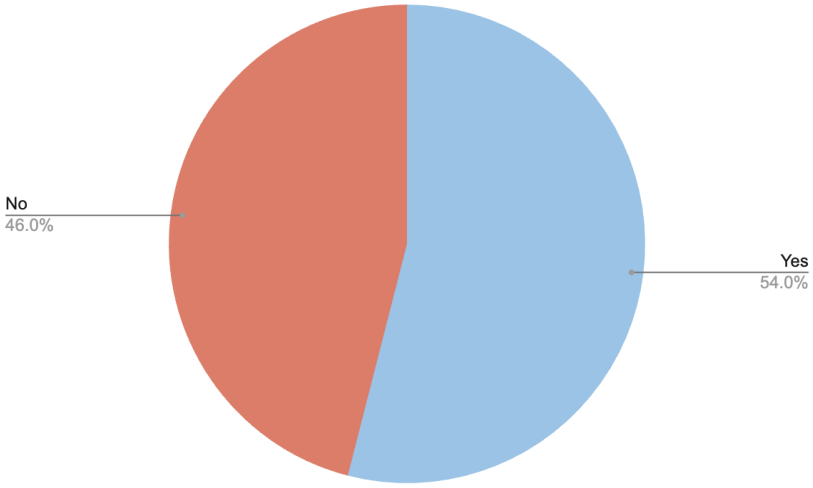


Figure 3: Responses to the question 'To meet new regulations, search engines may soon have to verify the ages of all users who have accounts in Australia. Are you aware of these upcoming changes?' n=1,501

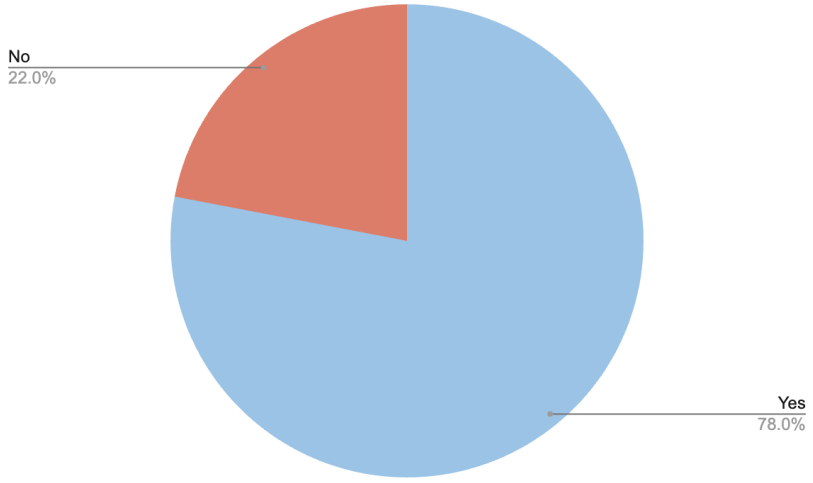


Figure 4: Responses to the question 'To meet new regulations, social media platforms may soon have to verify the ages of all users who have accounts in Australia. Are you aware of these upcoming changes?' n=1,501

On top of a lack of awareness, there was a level of public discomfort with the upcoming changes (see Figure 5). Almost half of participants described themselves as not comfortable with the upcoming age assurance requirements on search engines for example (49% not comfortable, 38% comfortable), while there was a higher level of comfort around age assurance on social media platforms (44% not comfortable, 46% comfortable). This perhaps reflects a greater public awareness regarding the SMMA. It is worth noting that comfort levels varied depending on proposed methods (see Figure 6), so the details of implementation will be important. Although we asked only about a handful of methods, methods more traditionally understood by the public such as using ID rated more favourably than less invasive methods like data profiling or facial analysis.

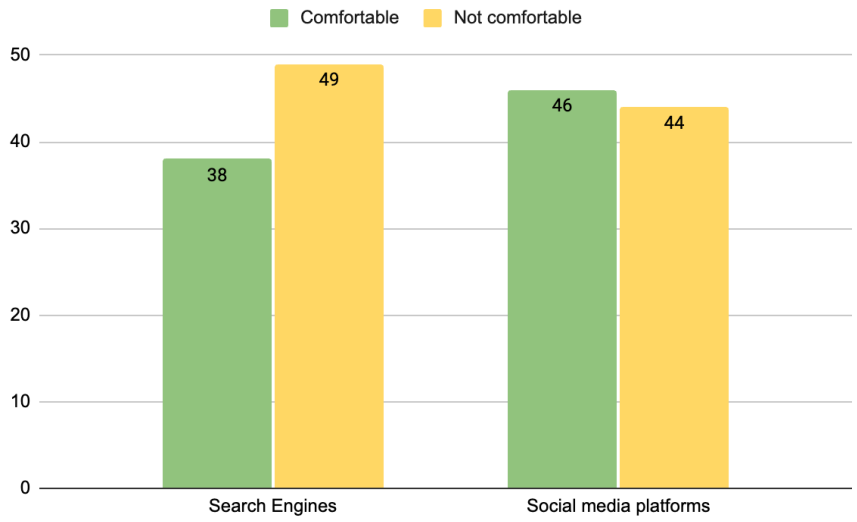


Figure 5: Responses as % to the question 'How comfortable or uncomfortable are you, if at all, with the idea of search engines verifying your age?' and 'How comfortable or uncomfortable are you, if at all, with the idea of social media platforms verifying your age?' Don't know is not graphed. n= 1,501

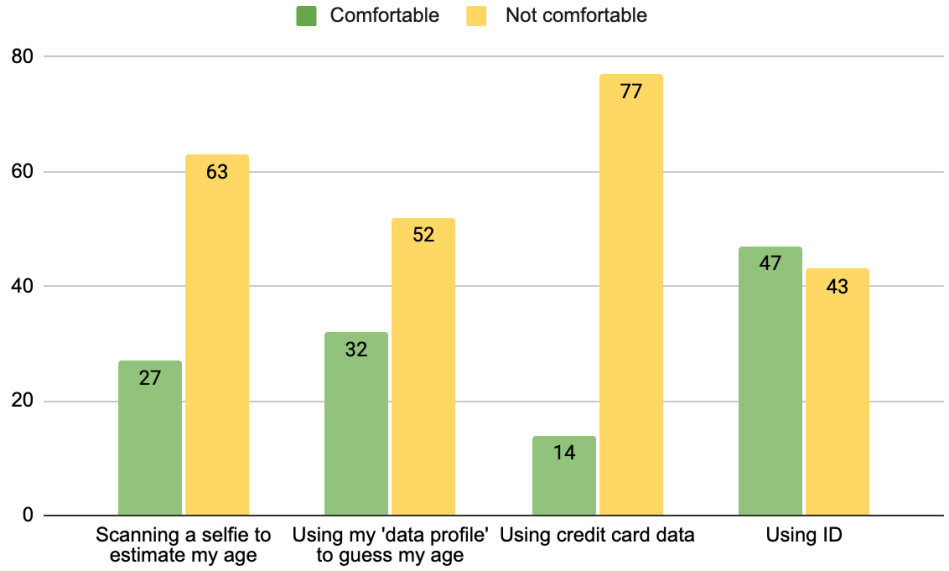


Figure 6: Responses as % to the question 'Age verification can use a huge range of techniques to find out your age, such as some of those presented below. Are there any that you feel particularly comfortable or uncomfortable with?'. Participants were able to select feeling comfortable or uncomfortable with each proposed option. Don't know is not graphed. n= 1,501

While patchy awareness may not be a problem in its own right, it does speak to the paucity of public debate and dialogue around these issues. Within this context, the Environment and Communications References Committee's *Inquiry into Internet Search Engine Services Online Safety Code* is especially welcome. Raising awareness and public debate about the nuance of these issues will be its own, important democratic outcome.

The broader need for systemic, platform accountability to protect children in the digital world

While it may be beyond the scope of this Inquiry, we think there is still value in examining — and where necessary challenging— the underlying approach of the SMMA, as it has in part led to the reliance on age assurance. The SMMA requirements frame the problem as an issue of 'who uses a platform', *not* as a problem of unsafe platforms. This will inherently engineer solutions that treat young people as the problem.

There has been significant expert agreement that the SMMA restrictions are not the best solution to protect children online.[27] Four central arguments are distilled here:

1. The restrictions affect children's rights. Children have the right to protection from harm through content, but they also have the right to access, including in the digital world. While the social media platforms that are restricted under the legislation have risks, they also function as online services which can provide information, educational and social value to young people. Better consideration is required to ensure that the rights of children and young people to information, expression, association, education and personal development are not compromised.[28] There are significant implementation issues beyond the question of age assurance. For example:
    a. There are simple technical means that allow users to skirt compliance with the use of VPNs, as we have seen elsewhere in the world.[29]
    b. Questions about what digital services count as social media are vexed and contested. We have seen this play out in the lobbying around YouTube's exclusion, but we see this in other areas of online safety regulation as well.[30]
2. The impact of the restrictions is unclear. While the effect could delay children's entry on to risky social media services until they are 16 years old, unless the 'delay' is filled with digital literacy training and capacity development, it may fail to deliver many safety outcomes for children. A delay without a plan of what to do to better support 13-15-year-olds to prepare to access risky platforms feels a bit futile. This is discussed further below.
3. The approach does not require the platforms to become any safer. It doesn't change the risk profile of the digital world, rather it just attempts to keep children away from it for longer. That is, the SMMA restrictions don't actually target the platforms by encouraging improvements in content or reductions in risk, it targets who is allowed to use the platform. There are other approaches to regulation that address this fundamental risk profile that do not produce the same challenges as the SMMA. Legislation can aim to protect young people *within* the digital world,

---

[27] Australian Child Rights Taskforce (2024) *Open letter about the social media bans* https://au.reset.tech/news/open-letter-about-social-media-bans/

[28] As a concrete example, one recent study found that nearly half of Australian Gen Z aged 18- to 26- years old (for the purposes of this survey) use social media to access news. This could suggest that younger teens affected by the SMMA restrictions (13- to 15-year olds) do so as well. See Sora Park, Caroline Fisher, Kieran McGuinness, Jee Young Lee, Kerry McCallum, Xiaolan Cai, Mona Chatskin, Lilik Mardjianto & Pinker Yao (2024) *Digital News Report: Australia 2024* https://apo.org.au/sites/default/files/resource-files/2024-06/apo-nid326816_6.pdf

[29] For example,

- When the UK rolled in age assurance requirements for adult focussed services (pornography and dating sites, etc) they found that VPNs became the most downloaded App in the Apple App Store, with one VPN provider reporting a 1,800% spike in UK daily sign-ups over the weekend after age check rules took effect. See Liv McMahon (2025) 'VPNs top download charts as age verification law kicks in' *BBC*, available online at https://www.bbc.com/news/articles/cn72ydj70g5o
- In Florida, when age verification requirements were introduced and PornHub removed its services from the state in response, there was a 1,150% increase in VPN demand. See Joshua Nelken-Zitser (2025) 'After Pornhub left Florida, VPN demand surged by more than 1,000%' *Business Insider*, available online at https://www.businessinsider.com/pornhub-exited-florida-vpn-demand-surged-by-over-1000-percent-2025-1

[30] For example, X is currently in a legal dispute with eSafety regarding its designation as a Relevant Electronic Service, which means it is covered by a regulator drafted, industry standard under the *Online Safety Act.* X would prefer to be designated as a Social Media Service, and therefore regulated under the industry drafted Code. (The preference to be covered by an industry drafted code speaks to the weaknesses of the outcomes of the co-regulatory process). See Tom Williams (2025) 'X takes legal action against Australian eSafety standard: Elon Musk's platform argues new rules should not apply' *Information Age*, available online at https://ia.acs.org.au/article/2025/x-takes-legal-action-against-australian-esafety-standard.html

rather than protecting them *from* it. There are good international models for this as discussed above, from the Guidelines for the Protection of Minors in the EU emerging from the *Digital Services Act* to the UK's *Age Appropriate Design Code*. The Australian Government has committed to elements of a similar approach with proposals for a Digital Duty of Care. This approach has a systemic focus that holds platforms to account and aims to reduce the risk profile of the digital environment.[31] While there will be lessons to be learnt from this approach — and there are many ways it could be implemented ineffectively or poorly,[32] especially in the current global political climate — a commitment to systemic regulation seems central to advancing children's rights in the digital world. We understand the need to ensure a considered timeline and process to ensure a Digital Duty of Care is effectively introduced into legislation.

For young people, there is no 'real' divide anymore between the digital world and the 'real' world as they live their lives. A focus on legislation that advances children's rights in the world, is probably going to be more future proof than legislation that aims to carve them out of the 'risky bits' of the world.

The broader need to uplift digital literacy

While it may be beyond the scope of this Inquiry, it is worth reinforcing the importance of a focus on the development of digital literacy skills. Controls that merely delay access — which is the outcome sought through age assurance — risk multiple failures. While some are discussed above, such as young people circumventing controls with VPNs or using platforms while not logged in, more centrally for this argument is the reality that many young people would simply enter platforms later without the scaffolded practice that builds safe habits.

Digital literacy is an important part of children's online rights and long-term safety. Digital literacy is more than technical competence. It is about equipping children and young people with the skills to critically evaluate information, understand their privacy and data rights, protect themselves from exploitation and manipulation, and use digital tools in safe and empowering ways. These skills are an essential part of realising children's rights online, and to ensuring that they do not become further marginalised as digital technologies evolve.

Australia needs to drive up safety standards on platforms, *and* build digital literacy and digital citizenship into curriculum and education strategy throughout childhood *and* support uptake of evidence-based sustained literacy programs across schools and community services. This may also require targeted support to avoid widening inequalities. While Australia currently has specific funding for digital literacy and indeed, it is the role of eSafety to provide further education, the SMMA means efforts must be increased to meet the gap.

Otherwise, age bans will leave many under-prepared when they inevitably return online. A measured package, platform duties, universal literacy, and independent evaluation, better aligns incentives, protects rights, and builds durable resilience. This complements, not substitutes, platform safety duties.

[31] The Hon Michelle Rowland (2024) *New Duty of Care obligations on platforms will keep Australians safer online* https://minister.infrastructure.gov.au/rowland/media-release/new-duty-care-obligations-platforms-will-keep-australians-safer-online
[32] See for example Lorna Woods & Rys Farthing (2024) 'The dangers of pluralisation' *The PolicyMaker* available online at https://thepolicymaker.appi.org.au/the-dangers-of-pluralisation-a-singular-duty-of-care-in-the-online-safety-act/

Recommendations

We appreciate the scope of this inquiry is to explore the impacts of age assurance and age verification technologies. The drivers for the takeup of these technologies both stem from the *Online Safety Act;* the SMMA as now incorporated as part 4A of the *Act*, and the Code arose from the Basic Online Safety Expectations in the *Act*. We believe that alternate, or additional, systemic solutions should also be built into the *Act*.

The upcoming reforms to the *Act,* spurred by the statutory review (conducted by Delia Rickard in 2024),[33] provide a timely opportunity. While we appreciate that this review did not directly address the SMMA or the Code, we understand that comprehensive reforms are under consideration and believe this process presents an opportunity for this Committee.

In this context, we would recommend that:

- Australia moves away from an age-assure first approach, and embraces a safety-setting first approach. That is, a commitment to age-assure as a last resort would bolster our commitment to data minimisation, and reduce potential unintended consequences.

- A commitment to the *Online Safety Act* reforms is maintained, especially to the introduction of an overarching duty of care.[34] We note that the geopolitical environment around online safety requirements at the moment is fraught. We understand that complex policy reforms require care and consideration. We support this ongoing work.

- All of the online safety codes, including for class 1A&B materials, and 1C&2 materials, should be reviewed and progressively replaced by regulator drafted codes ('standards'). Co-regulation is a flawed approach and it is worrying to see such changes to Australia's digital information ecosystem still driven by this obsolete practice.

- The SMMA requirements will be reviewed for effectiveness and impact within one year. The review should address the four broad critiques of the policy as outlined above, to include the:

    - Impact of children's rights, both the right to protection from harmful content, but also rights to access and information
    - Ability for the policy to achieve its stated aims, given the implementation issues such as use of VPNs and definitions of social media platforms
    - Effects of the delay in so far as it interacts with necessary digital literacy skills for young people (noting that other effects might be longer term and difficult to evaluate at the 12 month mark)
    - Effects of the delay in terms of reducing the risk profile of social media platforms.

[33] Delia Rickard PSM (2024) *Report of the Statutory Review of the Online Safety Act 2021*, online at https://www.infrastructure.gov.au/department/media/publications/report-statutory-review-online-safety-act-2021

[34] For discussion around what a good digital duty of care might look like, see Reset.Tech Australia (2024) *A duty of care in Australia's Online Safety Act,* available online ar https://au.reset.tech/news/briefing-a-duty-of-care/