The Senate

Environment and Communications References Committee

Internet Search Engine Services Online Safety Code and under 16 social media ban

November 2025

ISBN 978-1-76093-875-8 (Printed version)

ISBN 978-1-76093-875-8 (HTML version)

Printed by the Senate Printing Unit, Parliament House, Canberra

Members

Chair

Senator Sarah Hanson-Young	AG, SA

Deputy Chair

Senator Varun Ghosh	ALP, WA

Members

Senator Ross Cadell	NATS, NSW
Senator the Hon Sarah Henderson	LP, VIC
Senator Dean Smith	LP, WA
Senator Charlotte Walker	ALP, SA

Participating Members

Senator David Pocock	IND, ACT
Senator David Shoebridge	AG, NSW

Secretariat

Sean Turner, Committee Secretary
Tas Larnach, Committee Secretary
Nicola Kosseck, Principal Research Officer
Michael Finch, Senior Research Officer
Flynn Benson, Research Officer
Finn Salisbury, Graduate
Charlotte Gillies, Administrative Officer
Bryn Catlin, Administrative Officer (*to 10 October 2025*)
Elizabeth Hickey, Administrative Officer

PO Box 2600
Parliament House
Canberra ACT 2600

Telephone: 02 6277 3526
Email: ec.sen@aph.gov.au
Website: www.aph.gov.au/senate.ec

Contents

Terms of reference

The implementation of regulations aimed at protecting children and young people online, with particular reference to the Internet Search Engine Services Online Safety Code and the under 16 social media ban, including:

(a) privacy and data protection implications of age verification;
(b) the expansion of corporate data collection and user profiling capabilities enabled by code compliance requirements;
(c) the technical implementation and efficacy of age verification and content filtering mechanisms;
(d) alternative technical approaches to online safety for all users, including young people;
(e) appropriate oversight mechanisms for online safety codes;
(f) global experience and best practice; and
(g) any other related matters.

Abbreviations

AATT	Age Assurance Technology Trial
AHRC	Australian Human Rights Commission
AIIA	Australian Information Industry Association
ANU	Australian National University
ARC	Australian Research Council
AVIL	Australian Injecting and Illicit Drug Users League
AVPA	Age Verification Providers Association
DIGI	Digital Industry Group Inc.
DITRDCSA	Department of Infrastructure, Transport, Regional Development, Communications, Spots and the Arts
IAA	Internet Association of Australia Ltd
NSWACY	NSW Advocate for Children and Young People
OAIC	Office of the Australian Information Commissioner
Online Safety Act	*Online Safety Act 2021*
QUT	Queensland University of Technology
Search Engine Services Code	Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)
SMMA	Social Media Minimum Age
UK	United Kingdom
USA	United States of America
VPN	Virtual Private Network

List of recommendations

Recommendation 1

3.47 The committee recommends that the implementation of the Social Media Minimum Age obligation be delayed until 10 June 2026 to allow time for the issues in implementation and compliance to be properly considered and an education campaign for young people affected to be rolled out.

Recommendation 2

3.48 The committee recommends that the Australian Government legislate a digital duty of care to make online platforms safer for all users.

Recommendation 3

3.49 The committee recommends that the Australian Government legislate to prohibit platforms from harvesting and exploiting the data of minors and protect young people from targeted, unsolicited advertisements and algorithms as a matter of priority, with a view for this to apply to all users in the long-term to protect all Australians' safety and privacy.

Recommendation 4

3.50 The committee recommends that the eSafety Commissioner roll out an education program, including through schools, that delivers clear information to young people about the platforms that are covered by the Social Media Minimum Age obligation and what the impacts on young people will be, as well as information about digital literacy and online safety.

Chapter 1
Introduction

1.1 From 10 December 2025, certain social media platforms will be required to take reasonable steps to prevent Australians under 16 from creating or holding an account. These obligations are part of a range of regulations being introduced protect children and young people online from risks they may be exposed to through social media accounts. Additionally, the co-regulated Internet Search Engine Online Safety Code comes into effect on 27 December 2025, including requirements to ensure the highest safety settings are applied for logged-in Australian children. Amongst other things, both these measures require a mechanism for age assurance to be implemented by the relevant platforms in order to determine a user's age.

1.2 This report considers many of the important issues raised by inquiry participants about the implementation of these online safety regulations.

1.3 This chapter will first provide a brief outline of the *Online Safety Act 2021* (the Online Safety Act) and the role of the eSafety Commissioner. The chapter then explores the two significant online safety measures central to this inquiry, the Internet Search Engine Online Safety Code and the under 16 social media ban, also known as the Social Media Minimum Age (SMMA) obligation. These are two distinct regulatory measures being pursued by the government, although the measures deal with similar topics and often involve similar stakeholders. The meaning of 'age assurance', as it may apply to the implementation of these regulatory measures, will then be explained. Finally this chapter briefly outlines the conduct of the inquiry.

1.4 Chapter 2 will explore the views and concerns of inquiry participants, including in relation to the use of age assurance measures, such as privacy and data implications, efficacy and technical limitation as well as oversight mechanism.

1.5 Chapter 3 considers complementary and alternate approaches to online safety for children as raised by some inquiry participants advocating for systemic change.

The Online Safety Act

1.6 Online safety in Australia is primarily regulated under the Online Safety Act. Broadly, the Online Safety Act can be described as codifying Australia's approach to the protection of individuals online in two main ways. Firstly, it establishes an independent eSafety Commissioner with powers to respond to

specific online harms.[1] This is complemented by a systems-based approach for industry which aims to prevent harm by placing direct expectations on industry.[2]

1.7 Some key features of the Online Safety Act include a set of basic online safety expectations, various complaints and objections systems and an online content scheme. The online content scheme regulates illegal and restricted online content, with the Online Safety Act giving the eSafety Commissioner the power to 'direct an online service or platform to remove illegal content or ensure that restricted content can only be accessed by people who are 18 or older'.[3]

1.8 Illegal and restricted online content is classified as either Class 1 or Class 2. In general:

- Class 1 material—is 'material that is or would likely be refused classification under the National Classification Scheme'; and
- Class 2 material—is material that is, or would likely be, classified as either X18+ or R18+.[4]

Role of the eSafety Commissioner

1.9 The eSafety Commissioner is the primary body responsible for ensuring the safety of Australians online. It describes itself as 'Australia's independent regulator, educator and coordinator for online safety'.[5] It is an independent statutory office, and the role is appointed by the Minister for Communications.[6]

1.10 The Online Safety Act explicitly defines and explains the functions of the eSafety Commissioner. These functions include:

- promoting online safety for Australians;
- administering a complaints system for cyber-bullying and cyber-abuse material;
- administering the online content scheme;
- coordinating activities of Commonwealth Departments, authorities and agencies relating to online safety for Australians; and

---

1 Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (DITRDCSA), *Submission 27*, September 2025, p. 4.

2 DITRDCSA, *Submission 27*, p. 4.

3 eSafety Commissioner, Illegal and restricted online content, 2024, Illegal and restricted online content | eSafety Commissioner (accessed 27 October 2025).

4 eSafety Commissioner, Illegal and restricted online content, 2024, Illegal and restricted online content | eSafety Commissioner (accessed 27 October 2025).

5 eSafety Commissioner, *Submission 8*, p. 2.

6 eSafety Commissioner, *Submission 8*, p. 2.

- performing various functions related to the social media minimum age provisions.[7]

1.11 The eSafety Commissioner has several compliance and enforcement mechanisms at its disposal, though these mechanisms differ according to the specific function it is performing or scheme it is overseeing.[8] The eSafety Commissioner can issue online service providers and end-users with removal notices, end-user notices, remedial directions, link deletion notices, app removal notices and directions to comply with an industry code, among other notifications.[9] The eSafety Commissioner can also take stronger enforcement action where a civil penalty provision has been contravened, including giving a formal warning, giving an infringement notice, seeking a court-ordered injunction and seeking a court-ordered penalty.[10] Non-compliance with elements of the Online Safety Act can lead to a maximum penalty of $49.5 million.[11]

Internet search engine services online safety code

1.12 The online content scheme contained within Part 9 of the Online Safety Act regulates illegal and restricted content online. Among other things, Part 9 of the Online Safety Act:

- defines the type of material that is considered illegal or restricted (class 1 and class 2 material);
- establishes a framework for the eSafety Commissioner to give removal notices to online service providers relating to class 1 and 2 material; and
- provides a framework for the development of industry codes and standards for online service providers.[12]

1.13 The eSafety Commissioner explained that the codes are primarily intended to address issues of 'access, exposure and distribution' of class 1 and class 2 material online.[13] The codes are also intended to 'standardise and uplift industry's safety practices'.[14] Development of the industry codes is the responsibility of relevant industry bodies. As described by the eSafety Commissioner, the codes are 'co-regulatory' in that they are 'drafted by industry

---

7 *Online Safety Act 2021*, s. 25, p. 27.

8 eSafety Commissioner, *Compliance and Enforcement Policy*, October 2024, p. 4.

9 eSafety Commissioner, *Compliance and Enforcement Policy*, October 2024, p. 4.

10 eSafety Commissioner, *Compliance and Enforcement Policy*, October 2024, p. 4.

11 Online Safety Amendment (Social Media Minimum Age) Bill 2024, *Explanatory Memorandum*, p. 6.

12 *Online Safety Act 2021*, s. 105, p. 104.

13 eSafety Commissioner, *Submission 8*, p. 18.

14 eSafety Commissioner, *Submission 8*, p. 19.

for industry', but with registration of the codes and compliance with the codes overseen by the eSafety Commissioner.[15]

1.14 The Online Safety Act specifies that there are eight distinct sections of the online industry, with each expected to develop its own industry code.[16] Providers of internet search engine services are one of the eight identified industry sections.[17]

1.15 The eSafety Commissioner's submission indicated that the process for adopting industry codes was split into two phases following discussion with industry.[18] The Phase 1 industry codes deal with Class 1A and Class 1B material (child sexual exploitation material, pro-terror content, extreme crime and violence, and drug-related content).[19] Phase 2 industry codes deal with Class 1C, 2A and 2B material (online pornography, other high-impact material, and simulated gambling).[20]

1.16 As described in the Department of Infrastructure, Transport, Regional Development, Communications and the Arts' (DITRDCSA) submission, the Phase 1 codes and standards 'require industry to detect, remove and combat the generation of Class 1 material'.[21] The codes are accompanied by a common 'Head Terms', which provide a general principles-based framework designed to apply to all online service providers.[22]

1.17 Following the development and introduction of the Phase 1 Codes, Phase 2 Codes were developed to deal with material that is 'legally age restricted and designated as harmful for children by the Australian Government under the National Classification Scheme'.[23]

1.18 The Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material), representing the Phase 2 code for search engines, is set to come into effect on 27 December 2025.[24] Another set of Head Terms also accompany the

---

15 Ms Julie Inman Grant, eSafety Commissioner, *Proof Committee Hansard*, 13 October 2025, p. 70.

16 eSafety Commissioner, *Submission 8*, pp. 19–21.

17 *Online Safety Act 2021*, s. 135, pp. 127–128.

18 eSafety Commissioner, *Submission 8*, p. 18.

19 eSafety Commissioner, *Submission 8*, pp. 35–36.

20 eSafety Commissioner, *Submission 8*, pp. 35–36.

21 DITRDCSA, *Submission 27*, p. 8.

22 eSafety Commissioner, *Submission 8*, p. 22.

23 eSafety Commissioner, *Submission 8*, p. 20.

24 eSafety Commissioner, *Register of industry codes and industry standards for online safety*, 2025, Register of industry codes and industry standards for online safety | eSafety Commissioner (accessed 27 October 2025).

Phase 2 codes, enshrining 'principles that will sit alongside the safety measures for every layer of the technology stack'.[25]

1.19 The eSafety Commissioner noted that the Phase 2 codes adopt 'some key good practice measures' that it claimed are already being implemented by major platforms.[26] The submission also noted that the codes implement best practice approaches from comparable jurisdictions, ensuring 'greater regulatory parity that will enable stronger compliance by industry'.[27]

1.20 There are 25 compliance measures detailed in the code, ranging from requirements to adopt specific types of technology, to instructions on how to engage with the eSafety Commissioner and its policies, to requirements to improve existing technology and maintain dedicated trust and safety teams.[28]

1.21 The eSafety Commissioner's submission drew attention to the compliance measure that, by 27 June 2026, search engine services must 'implement appropriate age assurance mechanisms for logged-in account holders to ensure that the highest safety settings are applied when a service's systems detect that an account holder is likely to be an Australian child'.[29]

1.22 Additionally, the eSafety Commissioner highlighted the requirement that 'advertising for online pornography, high-impact violence material and self-harm material is not served to children'.[30] Further, it noted that the code 'provides enhanced protections for users who are not logged in', including default blurring of certain material to reduce the risk of accidental exposure and downranking of harmful content in search results.[31] The Commissioner's submission also stated that many of the age assurance requirements contained in the code 'expand on existing practices already routinely applied'.[32] DITRDCSA's submission echoed many of the eSafety Commissioner's main points, acknowledging the significance of similar key requirements.[33]

---

25 eSafety Commissioner, *Submission 8*, p. 22.

26 eSafety Commissioner, *Submission 8*, p. 21.

27 eSafety Commissioner, *Submission 8*, p. 21.

28 eSafety Commissioner, *Schedule 3 – Internet Search engine Services Online Safety Code (Class 1C and Class 2 Material)*, 27 June 2025, p. 5–14.

29 eSafety Commissioner, *Submission 8*, p. 23.

30 eSafety Commissioner, *Submission 8*, p. 24.

31 eSafety Commissioner, *Submission 8*, p. 24.

32 eSafety Commissioner, *Submission 8*, p. 24.

33 DITRDCSA, *Submission 27*, p. 10.

Social media minimum age rules

1.23 The Online Safety Amendment (Social Media Minimum Age) Bill 2024 received royal assent on 10 December 2024.[34] The bill introduced an additional Part to the Online Safety Act which creates 'an obligation for age-restricted social media platforms to take reasonable steps to prevent Australian children under 16 from having accounts on their platforms'.[35] This is referred to as the Social Media Minimum Age (SMMA) obligation.

1.24 According to the eSafety Commissioner, the SMMA obligation requires providers of age-restricted social media service platforms to 'take reasonable steps to prevent Australian children under 16 from having accounts on their platforms'.[36] In its regulatory guidance on the SMMA obligation, the eSafety Commissioner defined reasonable steps as consisting of 'systems, technologies, people, processes, policies and communications that support compliance with the SMMA obligation'.[37]

1.25 Its regulatory guidance also indicated that reasonable steps should ultimately serve several purposes, including: determining which accounts are held by age-restricted users and deactivating or removing those accounts, preventing age-restricted users from creating new accounts, and mitigating circumvention of measures employed by platforms.[38] Additionally, the regulatory guidance pointed to a series of guiding principles that 'should inform providers' reasonable steps to comply' with the SMMA obligation.[39]

1.26 The eSafety Commissioner has published a view that, as of 5 November 2025, Facebook, Instagram, Snapchat, Threads, TikTok, X, YouTube, Kick and Reddit are age-restricted platforms, noting this list continues to be updated prior to the SMMA obligation coming into effect.[40]

What is an age-restricted social media platform?

1.27 The Minister for Communications has four major responsibilities in the implementation of the SMMA obligation.[41] Firstly, the Minister for

---

34 Parliament of Australia, *Online Safety Amendment (Social Media Minimum Age) Bill 2024*, 2025, Online Safety Amendment (Social Media Minimum Age) Bill 2024 – Parliament of Australia (accessed 27 October 2025).

35 eSafety Commissioner, *Submission 8*, p. 24.

36 eSafety Commissioner, *Submission 8*, p. 25.

37 eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance*, September 2025, p. 19.

38 eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance*, September 2025, p. 19.

39 eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance*, September 2025, p. 21.

40 eSafety Commissioner, *Social media age restrictions*, https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions (accessed 13 November 2025)

41 eSafety Commissioner, *Submission 8*, p. 25.

Communications can specify services that are not age-restricted social media platforms.[42] Section 63C of the Online Safety Act defines the term 'age-restricted social media platform' as an electronic service whose sole purpose, or a significant purpose, is to enable online social interaction between two or more users, where the service allows users to interact with some or all other users and where the service allows users to post material on the service.[43]

1.28 Using the power to specify services that do not constitute age-restricted social media platforms, the Minister for Communications subsequently limited the scope of the broad definition of an age-restricted social media platform. On 29 July 2025, the Minister made the Online Safety (Age-Restricted Social Media Platforms) Rules 2025, which clarified that several services that would otherwise meet the definition of an 'age-restricted social media platform' would instead not be considered age restricted social media platforms.[44] This included online gaming and standalone messaging apps.[45]

1.29 The Minister for Communications can also make legislative rules that specify the 'kinds of information that providers of age-restricted social media platforms must not collect for purposes of complying with the SMMA obligation'.[46] The Minister is yet to make any such rules, nor have any rules been proposed.[47]

1.30 Additionally, the Minister for Communications is responsible for specifying when the SMMA obligation will take effect.[48] The Minister for Communications has specified that the SMMA obligation will take effect on 10 December 2025.[49]

1.31 Finally, the Minister for Communications is responsible for initiating an independent review of the SMMA obligation.[50] The committee notes that this independent review must be initiated within the two years following the 10 December 2025 compliance start date.[51]

1.32 The eSafety Commissioner's submission noted that the Office of the Australian Information Commissioner (OAIC) also has some responsibilities in the

---

42 eSafety Commissioner, *Submission 8*, p. 25.

43 *Online Safety Act 2021*, s. 63C, p. 63.

44 eSafety Commissioner, *Submission 8*, p. 25.

45 eSafety Commissioner, Social media age restrictions, 2025, Social media age restrictions | eSafety Commissioner (accessed 27 October 2025).

46 eSafety Commissioner, *Submission 8*, p. 25.

47 eSafety Commissioner, *Submission 8*, p. 25.

48 eSafety Commissioner, *Submission 8*, p. 25.

49 eSafety Commissioner, *Submission 8*, p. 25.

50 eSafety Commissioner, *Submission 8*, p. 26.

51 eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance*, September 2025, pp. 6–7.

implementation of the SMMA obligation. Specifically, the OAIC is responsible for enforcing the *Privacy Act 1988* in circumstances where a provider uses or discloses information about an individual for purposes other than determining whether the individual is an age-restricted user, or where it does not destroy material collected for age assurance purposes.[52]

1.33 Finally, the eSafety Commissioner has several responsibilities in the implementation of the SMMA obligation. It is responsible for developing regulatory guidelines for the SMMA obligation, which were published in September 2025.[53] The eSafety Commissioner is also responsible for monitoring and enforcing compliance with the SMMA obligation to take reasonable steps to prevent age-restricted users from having accounts with age-restricted social media platforms.[54] Further, it is responsible for enforcing compliance with the requirement for entities to not collect Government-issued identification material.[55]

Age assurance

1.34 In its submission to the inquiry the eSafety Commissioner noted that while the terms of reference for this inquiry refers to 'age verification', the broader and more commonly used term among regulators is 'age assurance'.[56] The eSafety Commissioner also stated that the Phase 2 industry codes and the SMMA obligation incorporate age assurance to protect children from online harms.[57]

1.35 Age assurance refers to a variety of processes and methods used to determine a person's age or age range.[58] This can include age verification, age estimation and age inference.

- Age verification refers to the process of identifying a person's age by finding, locating or sourcing their date of birth from a reliable document or source, ensuring that the source genuinely refers to the person in question, and communicating that finding to a relying party.[59]
- Age estimation is a method of determining a person's likely age or age-range by 'analysing physical or behavioural characteristics using artificial

---

52 *Online Safety Act 2021*, s. 63F, pp. 69–70.

53 eSafety Commissioner, *Submission 8*, p. 26.

54 eSafety Commissioner, *Submission 8*, p. 26.

55 eSafety Commissioner, *Submission 8*, p. 26.

56 eSafety Commissioner, *Submission 8*, p. 6.

57 eSafety Commissioner, *Submission 8*, p. 7.

58 eSafety Commissioner, *Submission 8*, p. 6.

59 DITRDCSA, *Age Assurance Technology Trial Main Report*, August 2025, p. 56.

intelligence or machine learning models'.[60] Age estimation methods include facial analysis, voice modelling, and motion pattern recognition.[61]

- Age inference refers to the method of determining a person's likely age using verifiable contextual, behavioural, transactional or environmental signals.[62] This can include verifiable life-stage indicators such as electoral enrolment, school year, transaction history, email data and device usage patterns.[63]

1.36 In November 2024, DITRDCSA announced that the Age Check Certification Scheme would conduct an Age Assurance Technology Trial.[64] This trial would 'undertake a point-in-time evaluation of market maturity – gathering evidence on the technical feasibility of existing age assurance technologies, having regard to a range of criteria including accuracy, privacy, security and accessibility'.[65]

1.37 The headline findings from the trial included that:

- age assurance can be done in Australia;
- there are not substantial technological limitations preventing age assurance from being deployed;
- there was a robust understanding of secure data handling practices;
- tested age assurance systems performed broadly consistently across demographic groups; and
- tested age assurance systems were generally secure.[66]

1.38 The following chapter will explore age assurance concerns raised by inquiry participants.

Conduct of the inquiry

Inquiry referral

1.39 On 27 August 2025, the Senate referred an inquiry into the implementation of regulations aimed at protecting children and young people online, with particular reference to the Internet Search Engine Online Safety Code and the

60 DITRDCSA, *Age Assurance Technology Trial Main Report*, August 2025, p. 73.

61 DITRDCSA, *Age Assurance Technology Trial Main Report*, August 2025, p. 73.

62 DITRDCSA, *Age Assurance Technology Trial Main Report*, August 2025, p. 89.

63 DITRDCSA, *Age Assurance Technology Trial Main Report*, August 2025, p. 91.

64 eSafety Commissioner, *Submission 8*, p. 10.

65 DITRDCSA, *Submission 27*, p. 5.

66 DITRDCSA, *Age Assurance Technology Trial Main Report*, August 2025, pp. 14–19.

under 16 social media ban, to the Senate Environment and Communications References Committee (the committee) for inquiry and report.[67]

1.40 The committee was scheduled to report on 31 October 2025. The Senate granted the committee a reporting date extension to 26 November 2025.[68]

1.41 The committee advertised the inquiry on its website and called for written submissions by 22 September 2025. The committee also wrote to various stakeholders to invite them to make a submission.

1.42 The committee received 101 submissions, as listed at **Appendix 1**.

1.43 The committee also received approximately 3400 items of correspondence which focused on very similar themes and appeared to be prepared in response to a campaign strategy. The committee agreed to publish a representative sample of these documents as de-identified correspondence under 'additional information' to the inquiry.

Public hearings

1.44 The committee held three public hearings for the inquiry, as follows:

- 24 September 2025—Parliament House, Canberra
- 13 October 2025—Parliament House, Canberra
- 28 October 2025—Parliament House, Canberra

1.45 The details of witnesses who appeared at the hearings is listed at **Appendix 2**.

Acknowledgements

1.46 The committee thanks the participants in the inquiry who provided substantial evidence on the implementation of regulations aimed at protecting children and young people online. The committee has carefully considered inquiry participants' evidence and has drawn on that evidence to prepare this report.

---

67 *Journals of the Senate*, No. 10, 27 August 2025, pp. 324–325. For full Terms of Reference see page vii of this report.

68 See, Senate Economics References Committee, *Progress report: Internet Search Engine Services Online Safety Code*, September 2025, p. 1.

Chapter 2
Issues regarding the implementation of age assurance measures

2.1 This chapter considers the key issues raised by inquiry participants on the implementation of age assurance measures under the Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) (the Search Engine Services Code) and the Social Media Minimum Age (SMMA) obligation established under Part 4A of the *Online Safety Act 2021* (the Online Safety Act).

2.2 While inquiry participants often expressed support for improving children's and young people's safety online, concerns were raised regarding the implementation of age assurance measures. These concerns centred on:

- the privacy and data implications of age assurance measures;
- the efficacy of age assurance measures and technical limitations; and
- the adequacy of oversight mechanisms for age assurance measures.

Online safety for children and young people

2.3 As outlined in this section, inquiry participants' evidence highlighted the need to support children's and young people's safety online, including by minimising exposure to age-inappropriate material. In particular, evidence was received on:

- the extensive use of technology by children and young people;
- the harms associated with age-inappropriate material; and
- the importance of online access for wellbeing and development.

Children and young people use technology extensively

2.4 Australian children and young people use technology extensively, including online search engines and social media. Indeed, the committee heard that children's use of technology is 'almost ubiquitous' and begins from an age when children cannot fully understand the risks involved.[1]

2.5 For example, the Alannah & Madeline Foundation's submission cited data which indicates 18 per cent of Australian preschool children aged 2–5 have their own laptop, tablet or personal computer and 16 per cent have access to someone else's device.[2] The Alannah & Madeline Foundation also cited data from the United Kingdom (UK) which indicates 96 per cent of children aged 8–14 have

[1] Alannah & Madeline Foundation, *Submission 3*, p. 3.

[2] Alannah & Madeline Foundation, *Submission 3*, p. 5 (citing data from the Office of the Australian Information Commissioner).

used a search engine and, on average, a child user of Google 'visits the service 152 times a month'.[3]

2.6 Moreover, data cited by UNICEF indicates '84% of children will have a social media presence by the age of two, and by age 12 every single child in Australia will be online'.[4]

2.7 Yet, for many children and young people, being online means exposure to age-inappropriate material. The eSafety Commissioner's recent *Keeping Kids Safe Online* survey of 3454 Australian children aged 10–17, found 74 per cent had encountered content associated with harm online.[5] Of the children surveyed:

- 47 per cent had seen fight videos online;
- 32 per cent had seen sexual images or videos online;
- 27 per cent had seen material showing or encouraging illegal drug use;
- 22 per cent had seen extreme real-life violence online;
- 19 per cent had seen material suggesting how a person can suicide or self-harm; and
- 12 per cent had seen violent sexual images or videos online.[6]

2.8 In addition to other concerning findings, the eSafety Commissioner said that more than half of children surveyed (53 per cent) had experienced cyberbullying and more than a quarter (27 per cent) had personally experienced online hate.[7]

Harms associated with age-inappropriate material

2.9 The committee heard that children and young people face a range of risks associated with exposure to age-inappropriate material.

2.10 The eSafety Commissioner told the committee that children and young people 'may be at greater risk than adults of experiencing a range of adverse impacts, including to their mental health, as a result of exposure to online content associated with harm'.[8] Further, the eSafety Commissioner submitted that children from certain cohorts are at greater risk of experiencing harm online:

> eSafety research shows that certain cohorts of children, including Aboriginal and Torres Strait Islander children, children with disability and LGBTIQ+

---

3 Alannah & Madeline Foundation, *Submission 3*, p. 3.

4 See, UNICEF, *Submission 13*, p. [1].

5 eSafety Commissioner, The online experiences of children in Australia, https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia (accessed 11 November 2025).

6 eSafety Commissioner, *Submission 8*, p. 13.

7 eSafety Commissioner, The online experiences of children in Australia, https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia (accessed 11 November 2025).

8 eSafety Commissioner, *Submission 8*, p. 13.

> teens, are at greater risk of harm online, including being more likely to encounter content associated with harm online.[9]

2.11 In its submission, the Australian Human Rights Commission (AHRC) outlined the harms associated with children's and young people's exposure to online pornography as follows:

> Reports indicate that nearly half of children between 9–16 experience regular exposure to sexual images. Studies have found that 'pornography both contributes to and reinforces the kinds of social norms and attitudes that have been identified as drivers of violence against women', and that viewing pornography is 'associated with unsafe sexual health practice'.[10]

2.12 The AHRC also noted data from 2022 which showed 23 per cent of 14 to 17-year-olds had 'encountered violent sexual material online'. The AHRC considered young people's exposure to such content 'may be associated with harmful sexual practices, sexual violence, stronger beliefs in gender stereotypes and sexually objectifying views of women'.[11]

2.13 Further, the committee received evidence of the harms experienced by children and young people from other forms of age-inappropriate material. For instance, the Alannah & Madeline Foundation submitted that self-harm material can be 'an immersive, destructive 'cycle' for some teens' and is 'especially troubling given the rise in self-harm among young adolescent girls since the late 2000s'.[12]

Harms associated with social media

2.14 Inquiry participants' evidence emphasised that social media is a vector of age-inappropriate content and can expose children and young people to anti-social behaviour and unlawful conduct, such as sexual harassment and cyber bullying.

2.15 For instance, Collective Shout, a campaign organisation against the objectification of women and the sexualisation of girls, submitted that social media platforms have 'become tools of sexual harassment' which are routinely used to sexually harass girls in school.[13] Further, Collective Shout submitted that research it undertook in 2024 indicates a connection between students' social media use and 'increased sexual behaviours in schools', including by having a 'major influence' on shaping 'inappropriate sexual norms' among students.[14]

2.16 Inquiry participants also considered that social media use can adversely impact children's and young people's mental health. While the AHRC acknowledged

---

9 eSafety Commissioner, *Submission 8*, p. 15.

10 Australian Human Rights Commission, *Submission 53*, p. 7.

11 Australian Human Rights Commission, *Submission 53*, p. 7.

12 Alannah & Madeline Foundation, *Submission 3*, p. 5.

13 See, Collective Shout, *Submission 33*, p. 6.

14 Collective Shout, *Submission 33*, p. 6.

social media is 'important for some children and young people who already face barriers to inclusion, safety and wellbeing', the AHRC submitted that:

> … social media can be harmful for children and young people due to the ease of access to age-inappropriate content. It can also negatively impact mental health through exposure to cyberbullying and addictive design features that encourage excessive use. Inadequate content moderation means children and young people often encounter harmful material without adequate safeguards or support. These risks are further amplified by algorithmic systems that prioritise engagement, making it more likely that vulnerable users are exposed to sensational or damaging content.[15]

2.17 The eSafety Commissioner's *Keeping Kids Safe Online* survey provides insight into the ways in which Australian children experience cyberbullying. For instance, of the children surveyed:

- 38 per cent had someone say hurtful things to them;
- 25 per cent had humiliating or hurtful things said about them;
- 16 per cent had been sent or tagged in offensive or upsetting videos/photos;
- 13 per cent had been told to hurt or kill themselves, or that they should die; and
- 7 per cent had humiliating or hurtful fake photos or videos of them shared online.[16]

2.18 The committee heard that, at its worst, social media has contributed to the suicide deaths of children and young people around the world.[17] In one Australian case, Collective Shout outlined the tragic circumstances of a 15-year-old from a regional town in New South Wales who was 'bullied to death' after a 'fake nude photo' of her was circulated extensively on social media.[18] Further, Collective Shout submitted that '[a]t least five Australian boys to date (that we know of) have ended their lives due to being tricked by sextortion scammers', following a significant increase in reports of 'financial sextortion targeting minors'.[19]

---

15 Australian Human Rights Commission, *Submission 53*, pp. 6–7.

16 eSafety Commissioner, How common is cyberbullying among children in Australia?, https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/snapshot-cyberbullying (accessed 11 November 2025).

17 See, for example, Collective Shout, *Submission 33*, pp. 2–3.

18 Collective Shout, *Submission 33*, pp. 2–3.

19 Collective Shout, *Submission 33*, p. 3.

Balancing harms with online access

2.19 Alongside the risks of age-inappropriate content, the committee received evidence on the importance of regulation that supports children's and young people's online safety and promotes their development and wellbeing.[20]

2.20 Indeed, the committee heard that young people's access to social media is important for social participation. As the Youth Affairs Council Victoria said:

> We live in an increasingly digitised world, and social media is an important third space for young people. It's often where they connect, build community, seek support and access information about the world around them, as well as being a crucial space for collective advocacy. This is especially true for marginalised young people, including LGBTQIA+ young people, disabled young people and young people living in regional and rural areas. [21]

2.21 UNICEF submitted that as young people 'disproportionately occupy online spaces more than any other group, the design and regulation of those spaces will have a greater impact on them and for longer than any other generation before them'.[22] UNICEF noted that young people consider being online 'critical to their healthy development and wellbeing, and that being online is fundamental to their lives'. [23] UNICEF added:

> In fact, UNICEF Australia's recent research found that 81% of Aussie teens who use social media say it has a positive influence on their lives. In the online world, children and young people access important information and vital support, and it is also where they connect, socialise and express themselves.
>
> We know that children face risks online, be it from bullying or exposure to harmful content, but we need to protect children within the digital world, not prohibit them from using it.[24]

2.22 Similarly, Ms Elizabeth Thomas, Senior Director, Public Policy, Digital Safety at Microsoft, gave evidence to the committee that emphasised the need for children to safely access online spaces to support their development and social participation:

> Empowering children to engage safely online is critical to enable them to make the most of the digital environment, including through access to

---

20 See, for example, UNICEF, *Submission 13*, p. [1].

21 Ms Lauren Frost, Advocacy Manager, Policy and Communications, Youth Affairs Council Victoria, *Committee Hansard*, 13 October 2025, p. 34.

22 UNICEF, *Submission 13*, p. [1]. Note, internal citations have been removed from this quote.

23 UNICEF, *Submission 13*, p. [1]. Note, internal citations have been removed from this quote.

24 UNICEF, *Submission 13*, p. [1]. Note, internal citations have been removed from this quote.

> educational resources, connecting with others, and developing important digital literacy and citizenship skills.[25]

2.23 While some inquiry participants supported aspects of the Search Engine Services Code and the SMMA obligation as measures likely to reduce children's exposure to age-inappropriate material,[26] many inquiry participants questioned the efficacy of the associated age assurance measures in achieving a safer online experience.[27]

2.24 For instance, despite the Social Media Minimum Age Bill being passed in December 2024, the committee received evidence indicating ongoing concerns about the impact of the restrictions. The AHRC submitted that it:

> … continues to hold serious reservations about the Social Media Ban due to the disproportionate impact it can have on the right to access information (particularly for vulnerable or marginalised groups) and concerns about age assurance.[28]

2.25 Indeed, the AHRC considered that the eSafety Commissioner 'should conduct further consultation and human rights analysis of the impact and implementation of the Social Media Ban, with a larger and more diverse group of children and young people'.[29]

Concerns regarding the privacy risks of age assurance measures

2.26 As outlined in Chapter 1, age assurance measures under the Search Engine Services Code and the SMMA obligation will come into effect in December 2025.[30] Among other things, the Search Engine Services Code will require search engine providers to:

> (a) implement appropriate age assurance measures for account holders; and

---

25 Ms Elizabeth Thomas, Senior Director, Public Policy, Digital Safety, Microsoft, *Committee Hansard*, 13 October 2025, p. 3.

26 Alannah & Madeline Foundation, *Submission 3*, p. 6.

27 See, for example, Ms Rachel Lord, Senior Manager, Government Affairs and Public Policy, YouTube AUNZ, Google, *Committee Hansard*, 13 October 2025, p. 3.

28 Australian Human Rights Commission, *Submission 53*, p. 6.

29 Australian Human Rights Commission, *Submission 53*, p. 5.

30 Note, age assurance under the SMMA will come into effect on 10 December 2025 and age assurance under the Search Engine Services Code will come into effect on 27 December 2025. See, eSafety Commissioner, *Submission 8*, pp. 23 and 32.

(b) apply tools and/or settings, like 'safe search' functionality, at the highest safety setting by default for an account holder its age assurance systems indicate is likely to be an Australian child…[31]

2.27 Similarly, the SMMA obligation will require social media platforms to apply age assurance measures to ensure account holders are over the age of 16. Neither the Search Engine Services Code nor the *Online Safety Amendment (Social Media Minimum Age) Act 2024* (SMMA Act), which establishes the SMMA obligation, stipulates that a platform provider must use a specific age assurance technology.

2.28 As outlined in this section, inquiry participants raised concerns about the implementation of age assurance measures.

Privacy implications of age assurance measures

2.29 The committee heard that, under the Search Engine Services Code and the SMMA obligation, Australians will likely need to upload significant personal data, such as identification documents or biometric information, to verify their age online.[32]

2.30 Yet many inquiry participants expressed deep reservations about the privacy implications of requiring Australians to provide sensitive personal data to search engine services or social media companies.[33] For instance, Digital Rights Watch submitted:

> The introduction of age verification for online content raises profound concerns about privacy, data protection, and proportionality. Invasion of privacy is inherent in any system that requires individuals to prove their age before accessing certain material.[34]

2.31 The committee heard that age assurance puts identity data at risk for people of all ages. As Bloom-Ed told the committee:

> … the data collection planned has grave implications for young people's privacy and puts their identity data at risk. Additionally, the data collection planned for teens and young people will also impact Australian adults and their privacy, as sites will be assessing information about age from user statements and inference technology.[35]

---

31 Schedule 3 – Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material), p. 5.

32 See, QUT Digital Media Research Centre, *Submission 14*, p. [4].

33 See, for example, Queensland Council for Civil Liberties, *Submission 18*, pp. [2–3].

34 Digital Rights Watch, *Submission 12*, p. 6.

35 Bloom-Ed, *Submission 23*, p. [3].

2.32 The committee also heard that for many Australians, and particularly for younger people, maintaining their online privacy is a major concern.[36] Data submitted by the NSW Advocate for Children and Young People (NSWACY) suggests young people are concerned data breaches 'are becoming more common and invasive age verification methods that collect, and store data are a significant privacy concern and may increase vulnerability'.[37] NSWACY submitted that such concerns have led most young people to use a range of tools to help protect their online privacy, including 'using incognito mode or VPNs and providing false information'.[38]

2.33 Other inquiry participants also highlighted that platform users face substantial risks to their privacy from the storage of their personal information for age verification.[39] For instance, Away from Keyboard cautioned that, without appropriate regulation, the Search Engine Services Code could:

> … unintentionally entrench surveillance-based business models. Without tight regulation, age-assurance data and behavioural analytics may be collected far beyond what is necessary to establish age, creating permanent profiles of children, carers and older Australians. These risks are acute for regional and low-literacy communities, where users may be less able to scrutinise privacy policies or exercise their rights.[40]

2.34 The Australian Research Alliance for Children and Youth (ARACY) warned that age verification measures must protect young peoples' privacy or risk their digital disengagement:

> Verification regimes that don't protect privacy will drive disengagement. Any age-verification scheme must prioritise privacy safeguards and transparent data handling, or risk driving young people away from accessing digital spaces altogether. This would negatively affect their mental health as online spaces are where young people find connection to and affirmation from peers.[41]

2.35 In considering the privacy implications of age assurance, Cybercy, a cyber literacy and behavioural change consultancy, cautioned that the online protections of children and young people are threatened, in part, due to the size

---

36 See, for example, Bloom-Ed, *Submission 23*, p. [3]; yourtown, *Submission 19*, p. 4; Australian Research Alliance for Children and Youth, *Submission 5*, p. [1]; Australian Research Council Centre of Excellence for the Digital Child, *Submission 10*, p. 2.

37 NSW Advocate for Children and Young People, *Submission 1*, p. [3].

38 NSW Advocate for Children and Young People, *Submission 1*, p. [4].

39 See, for example, Bloom-Ed, *Submission 23*, p. [3]; Australian Research Council Centre of Excellence for the Digital Child, *Submission 10*, p. 2.

40 Away from Keyboard, *Submission 26*, p. 6.

41 Australian Research Alliance for Children and Youth, *Submission 5*, p. [1].

of the global cybercrime market outstripping the cybersecurity market. As Cybercy submitted:

> The global cybercrime market is now USD $13.8 trillion, growing at 15% annually. By contrast, the cybersecurity products and services market is USD $432 billion, growing at 12.5% annually.
>
> This imbalance tells a clear story: despite record spending on technology, the economics still favour attackers. For children and young people, this means technical protections will always lag behind the ingenuity of those who exploit them.[42]

Concerns about corporate data collection

2.36 Many inquiry participants considered that age verification measures will exacerbate existing concerns about corporate data collection and will, ultimately, increase the risk of misuse of users' data.[43]

2.37 The committee heard that, while statistics are currently limited, the collection of children's and young people's online data appears to be prolific.[44] Indeed, data cited by UNICEF indicates that before a child turns 13 an estimated 72 million points of data will have been collected about them.[45] Further, UNICEF argued that it is often unclear to users (of all ages) how their data is being used:

> The digital ecosystem is so complex and seamless that often neither children or their adult guardians are fully aware of how their data is being captured and used, nor what the potential benefits and risks are. And while an individual's data tends to be treated the same way regardless of who they are, children's data is different - children are less able to understand the long-term implications of consenting to their data being collected.[46]

2.38 Further, inquiry participants raised concerns that technology companies lack the ability to adequately protect sensitive user data.

2.39 Digital Rights Watch, for example, criticised the requirement for Australians to provide personal data to 'privacy-invading companies':

> … [The] requirement to age-gate Australian users will provide some of the world's largest privacy-invading companies with direct access to yet more private data about Australians - whether that's captured with ID documents or inferred with one of the other age-assurance methods.[47]

---

42 Cybercy, *Submission 2*, p. [1].

43 See, for example, Cybercy, *Submission 2*, p. 2.

44 UNICEF, *Submission 13*, p. [2].

45 UNICEF, *Submission 13*, p. [2]; See, also ARC Centre for Excellence for the Digital Child, *Submission 10*, p. 3.

46 UNICEF, *Submission 13*, p. [2].

47 Digital Rights Watch, *Submission 12*, p. 11.

2.40 Collective Shout's submission contended that several large social media platforms and video streaming companies, including those subject to the SMMA obligation, have already been 'found by the US Federal Trade Commission (FTC) to be engaging in vast surveillance of users, with few privacy controls, and inadequate safeguards for kids and teens'. Collective Shout further noted the FTC had sued certain social media companies for 'collecting and using children's information without consent'.[48]

2.41 TikTok was questioned by the committee about concerns on the scope of the company's data collection practices, noting TikTok gathers a broad range of information including contact lists, device information, location data, what is watched by children and for how long, scrolling and key stroke patterns in addition to algorithmic profiling.[49]

2.42 Ms Ella Woods-Joyce, Public Policy Lead, Content and Safety at TikTok Australia advised the committee that the company's 'data and privacy practices are actually broadly consistent with our peers'. Ms Woods-Joyce added that TikTok is:

> … very transparent about the data that we collect. In fact, we take a data privacy minimisation approach to things. We don't want more data than we need to make sure that the app is running safely and securely and that it's working as it's intended.[50]

Adequacy of data protection regulations

2.43 A number of inquiry participants addressed the adequacy of Australia's data protection regulations, in light of the likely increase of personal data being uploaded under the age assurance measures. For instance, Digital Rights Watch argued that Australia's data protection laws are 'not strong enough to accommodate the mass uptake' of sensitive information associated with facial recognition technology.[51]

2.44 Commenting on the SMMA Act, which establishes the SMMA obligation, the Internet Association of Australia (IAA) observed that:

> … the Act explicitly prohibits entities from the collection of government issued identification as the sole means of fulfilling its obligations under the Act. However, we note that platforms are permitted to collect such information if it is being offered alongside other measures. The Act is then vague as to the retention periods for such information that have been collected. We are thus not convinced that the provisions relating to privacy are sufficient and believe that as it pertains to age verification measures,

---

48 See, Collective Shout, *Submission 33*, p. 9.

49 See, Senator Sarah Henderson, *Committee Hansard*, 28 October 2025, p. 16.

50 Ms Ella Woods-Joyce, Public Policy Lead, Content and Safety, TikTok Australia, *Committee Hansard*, 28 October 2025, p. 16.

51 Digital Rights Watch, *Submission 12*, p. 11.

> there should be no collection or retention of any identification material by the entities themselves.[52]

2.45 The IAA added that its concerns regarding data retention for the SMMA were 'exacerbated' by Australia's 'overly complex and convoluted data retention regime' which resulted in entities tending to 'over-collect and retain data longer than is necessary, often due to confusion and fear of non-compliance'.[53] The Queensland Council for Civil Liberties raised a similar concern and observed that unnecessary data retention was identified as an issue in an Australian Government commissioned report in August 2025 on the Age Assurance Technology Trial (AATT). That report, commissioned by the Australian Government through the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (but conducted independently of the department and its regulators),[54] noted:

> We found some concerning evidence that in the absence of specific guidance, service providers were apparently over-anticipating the eventual needs of regulators about providing personal information for future investigations. Some providers were found to be building tools to enable regulators, law enforcement or Coroners to retrace the actions taken by individuals to verify their age which could lead to increased risk of privacy breaches due to unnecessary and disproportionate collection and retention of data.[55]

2.46 The eSafety Commissioner is responsible for monitoring and enforcing 'compliance with the requirement to not collect government issued ID or use an accredited service under the *Digital ID Act 2024*, without providing reasonable alternative means'.[56] In September 2025, the eSafety Commissioner released guidance on the SMMA obligation which, among other things, outlined the Commissioner's expectations regarding privacy-preserving practices and data minimisation. In particular, the eSafety Commissioner stated:

- that social media companies' compliance with the SMMA obligation will not be considered reasonable unless they meet their information and privacy obligations under the Part 4A of the Online Safety Act;
- that providers 'should assess the minimum information and data needed to make decisions appropriate for their service and circumstances' and 'avoid handling of sensitive personal information' where possible; and

---

52 Internet Association of Australia, *Submission 9*, p. 3.

53 Internet Association of Australia, *Submission 9*, p. 3.

54 Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts, *Age Assurance Technology Trial: Part A—Main report*, August 2025, p. 12.

55 Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts, *Age Assurance Technology Trial: Part A—Main report*, August 2025, p. 19.

56 eSafety Commissioner, *Submission 8*, p. 25.

- that there is no expectation for 'providers to retain personal information as a record of individual age checks'.[57]

2.47 While the IAA acknowledged regulatory guidance from the eSafety Commissioner, the IAA called for clearer examples of what the eSafety Commissioner 'may request of providers in order to prove compliance so as to reduce confusion and uncertainty'.[58]

2.48 Given the concerns raised in relation to data collection, several inquiry participants made recommendations on how regulations for age verification can be amended to protect users' data and privacy. For example, in relation to the Online Safety Code, the Alannah and Madeline Foundation advocated for a 'safety-by-default' approach:

> It would be our preference to see codes for industry require a 'safety-by-default' approach, with the highest safety standards in place for all users by default and age assurance employed only as a 'next step' for individuals who seek to access adult materials. We believe this would reduce data harvesting and 'friction' for children who use search engines for appropriate purposes. At present, it is unclear to us whether the code allows for this approach; unfortunately, it does not appear to treat this approach as a preference. We speculate that an approach which prioritises safety and privacy by default is only likely if codes are developed by a regulator answerable to the public, rather than being drafted by industry as is currently the case.[59]

2.49 Yet, noting that age assurance measures are likely to eventuate in Australia, the Alannah and Madeline Foundation called for regulatory changes to help ensure the protection of children's rights, including 'implementation of 'tranche 2' of the Privacy Act reforms and creation of a strong, comprehensive Children's Online Privacy Code to place appropriate limits around companies' handling of individuals' personal data.'[60]

2.50 The committee received many further examples from inquiry participants on prospective measures to minimise the privacy risks associated with data collection by corporations for age assurance purposes. In one key example, the Age Verification Providers Association (AVPA) proposed the use of third-party age verification providers, and related privacy practices, for age assurance purposes. Use of a third-party age verification provider would mean that a user would provide their data for a third-party who would independently verify the user's age and then report the user's age status to a platform operator without

---

57 eSafety Commissioner, *Social Media Minimum Age: Regulatory Guidance*, September 2025, p. 25.

58 Internet Association of Australia, *Submission 9*, p. 3.

59 Alannah and Madeline Foundation, *Submission 3*, p. 3.

60 Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, 13 October 2025, p. 59.

disclosing any further identifying information. Mr Iain Corby, Executive Director, summarised this process as follows:

> Regulations requiring online age assurance should mandate privacy by design using independent third-party checks. Users should have the option of a double-blind architecture, which means the platform can never discover the identity of the user and the age assurance provider cannot tell which platform the user is accessing. They should take advantage of zero-knowledge proof tokens, so platforms don't get any extra data about a person from the age check.[61]

2.51 Mr Corby emphasised that third-party providers need to be audited, certified and monitored by data protection authorities to provide confidence to consumers about the safety of their data.[62] Mr Corby added that '[h]aving established your age, then the third-party provider deletes all that data—any data they used for that purpose.'[63]

2.52 However, the committee also heard concerns about third-party age verification providers' access to sensitive user data.[64] For instance, the Australian Research Council Centre of Excellence for the Digital Child submitted:

> Previous research has explored the significant risk this poses to privacy and interests of consensual and legal adult consumers too. This research cites scepticism over the reliability and efficacy of the proposed arrangements around third-party age verification services or governments preserving privacy and anonymity of its users when storing personal data securely. In an age where data is monetised and considered a valuable commodity; allowing third-parties to host such intimate and personal data raises justified security and privacy concerns for all Australian users.[65]

2.53 Broader concerns in relation to enhancing Australia's privacy regulations are further discussed in Chater 3 of this report.

Concerns regarding the limitations of age assurance technologies

2.54 In addition to concerns around the use of data collection and the privacy implications of age assurance by digital platforms, inquiry participants also raised concerns about the accuracy, suitability and reliability of the most prevalent age assurance mechanisms, including those that provide verification of an exact age, age estimation of likely age or age-range and age inference.

---

61 Mr Iain Corby, Age Verification Providers Association, *Committee Hansard*, 13 October 2025, p. 57.

62 Mr Iain Corby, Age Verification Providers Association, *Committee Hansard*, 13 October 2025, p. 57.

63 Mr Iain Corby, Age Verification Providers Association, *Committee Hansard*, 13 October 2025, p. 58.

64 See, for example, Mr Joel Canham, *Submission 39*, p. [1].

65 Australian Research Council Centre of Excellence for the Digital Child, *Submission 10*, p. 2.

2.55 For example, the QUT Digital Media Research Centre highlighted that 'many of the "best" age-estimation technologies still have unacceptably high error rates'.[66] Similarly the AHRC advised '[c]urrent age assurance technologies are not yet capable of implementing the Australian social media ban in a way that avoids significant human rights risks.'[67] Further, the Scarlet Alliance submitted that '[w]hile the recent Age Assurance Technology Trial claimed success, it did not finda single ubiquitous solution that would suit all use cases'.[68] Indeed, the Scarlet Alliance considered that several findings of the AATT suggest 'flawed technologies' may be implemented under the Phase 2 Codes.[69]

2.56 Further, one of the most common criticisms from inquiry participants was that age-verification measures could be easily circumvented.[70] These concerns are explored further below.

Facial age estimation

2.57 Many inquiry participants expressed concern about the accuracy of facial age estimation technology, particularly for women, people of colour, and young people.[71]

2.58 The AHRC, for example, explained that there are documented inaccuracies of facial recognition technology for certain demographic groups. It stated:

> The Age Assurance Technology Trial found that facial age estimation systems perform less reliably for individuals with darker skin tones and for those aged 16–20, raising serious concerns about equality and discrimination.[72]

2.59 Some participants also questioned the ability of facial estimation technology to detect the use of masks and other circumvention methods. Mr Leo Puglisi, for

---

66 QUT Digital Media Research Centre, *Submission 14*, p. [7].

67 Australian Human Rights Commission, *Submission 53*, p. 10

68 Scarlet Alliance, *Submission 17*, p. [3].

69 Scarlet Alliance, *Submission 17*, p. [4].

70 See, for example, ANU Law Reform and Social Justice Research Hub, *Submission 28*, p. [5]; Mr Leo Puglisi, Founder and Chief Anchor, Six News Australia, *Committee Hansard*, 13 October 2025, p. 40; Digital Rights Watch, *Submission 12*, p. 12.

71 See, for example, Digital Rights Watch, *Submission 12*, p. 7; Bloom-Ed, *Submission 23*, p. [6]; Human Rights Commission, *Submission 53*, p. 10.

72 Australian Human Rights Commission, *Submission 53*, p. 10. (Citing Age Check Certification Scheme, Age Assurance Technology Trial Part D Age Estimation (Trial Report, August 2025) p. 70-73); eSafety, Social Media Minimum Age Regulatory Guidance (Regulatory Guidance, September 2025), p. 13.

example, noted in the United Kingdom, users have bypassed age estimation with the use of computer-generated images.[73]

2.60 In contrast, AVPA advised that standard testing of age estimation technology included the ability to identify the use of masks, deepfakes or AI.[74]

2.61 The AATT similarly reported that of the systems tested:

> Biometric liveness checks were commonly implemented and aligned with ISO/IEC 30107 (presentation attack detection) standards, helping to guard against spoofing and deepfake risks. Systems were also generally effective at identifying document forgeries, including AI-generated fakes.[75]

2.62 Recognising the limitations of facial age estimation, a number of inquiry participants supported its use only as a first-pass estimation process. Mr Corby, for example, proposed that facial age estimation is a low friction estimation method that serves as an adequate first gateway in successive validation techniques. Users closer to the legal minimum may have to undertake further methods to verify their age such as an email address or mobile phone number.[76] He explained:

> There has been a lot of noise about facial age estimation and how you can't be more accurate than to within, say, 1.3 to 1.5 years for the top three, which was shown in the trial. We've never argued that it would be possible to implement an exact 16-plus or 18-plus minimum age using the estimation techniques. That's really not why they're there. They're there to help people who are well over those ages. [77]

2.63 Mr Corby further stressed that facial age estimation would not be useful for establishing an actual birthdate for the purposes of young people opening a new social media account, which would require age verification with access to an official source confirming actual date of birth.[78]

2.64 In giving evidence to the committee, some platforms confirmed that facial age estimation is already being used to some extent. For example, Ms Mia Garlick, Regional Director of Policy with Meta, advised that Meta uses a third-party provider for its age assurance process and users are given the option of providing a video selfie or government ID.[79]

---

73 Mr Leo Puglisi, 6 News, *Committee Hansard*, 13 October 2025, p. 40.

74 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 60.

75 DITRDCSA, *Age Assurance Technology Trial – Final Report*, August 2025, p. 62.

76 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 57.

77 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 58.

78 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 60.

79 Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 28 October 2025, p. 8.

Age inferencing

2.65 Most platforms acknowledged that initial implementation of the SMMA obligation would draw on existing data held by the platforms, including where users have self-identified that they are under 16, and from usage patterns that identify users who are likely to be under 16.[80]

2.66 However, the committee was also advised that more fine-grained inferences across age brackets, such as distinguishing 13 from 16, was 'inherently less reliable', as identified in the AATT, because 'adolescents often have limited public records, payment credentials or distinct online habits.'[81]

2.67 Mr Iain Corby noted the high likelihood platforms would utilise age inferencing, stating:

> The reality is that most of the social media platforms will be using all the data that they have on their users at present to assess their age initially, and then it will only be those who are pretty close to the age of 16 who would need to appeal that. Those appeals are never going to be handled with estimation anyway; they can only be handled with a real date of birth.[82]

2.68 Mr Corby also highlighted alternate age inference techniques are available such as hand gesture analysis, which has a very high level of accuracy,[83] and which avoids the bias issues that are associated with facial age estimation.[84]

2.69 The AHRC advised that age inferencing from behavioural patterns, contextual data and metadata already held by platforms 'avoids users having to submit additional personal information and reduces barriers to access'.[85] However, it noted the process is intrusive and risks normalising routine analysis of users' personal content and interactions.[86]

2.70 Given the limitations of age estimation mechanisms, and the definitive 16-year age setting of the SMMA restrictions, a number of inquiry participants concluded that a staged or 'waterfall' approach to age assurance was the most effective approach for digital platforms.[87]

---

80 See, for example, Ms Jennifer Stout, Senior Vice President, Global Policy and Platform Operations, Snap Inc, *Committee Hansard*, 28 October 2025, pp. 7–8.

81 Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 28 October 2025, p. 1.

82 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 61.

83 Age Verification Providers Association, *Submission 54*, p. 7.

84 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 61.

85 Australian Human Rights Commission, *Submission 53*, p. 11.

86 Australian Human Rights Commission, *Submission 53*, p. 12.

87 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 57.

2.71 The Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (DITRDCSA), for example, cited the AATT findings that a 'waterfall approach – where different age assurance approaches are combined – will boost confidence in age estimates'.[88]

2.72 The Australian Information Industry Association (AIIA) reiterated the findings of the AATT that 'there is no one-size-fits-all solution' to age assurance. It explained that:

> Just as online services vary greatly in how they operate and the risks they pose to children, so too should age assurance measures be tailored to fit those differences. A social media platform with extensive user-generated content and high interaction among strangers presents very different risks compared to, say, an educational website or a search engine.[89]

Age verification

2.73 Where a date of birth is required to confirm a user's exact age, age verification would be necessary.

2.74 In addition to the data and security issues raised above, some inquiry participants raised technical concerns about the use of individual identity documentation for age verification.

2.75 If users were required to submit photo ID to platforms or to third party verification providers, Digital Rights Watch noted there are ways to circumvent the verification including 'the ability of children to procure photo ID, perhaps by borrowing that of a parent or older sibling.'[90] They further noted that 'there are a number of channels through which a person may purchase a fake ID, either Australian or foreign.'[91]

2.76 DITRDCSA noted that the AATT 'did not reveal any substantial technological limitations to the implementation of age verification technologies in Australia.'[92] Addressing security and fraud concerns, the AATT report highlighted that, of the age verification systems trialled:

> Systems were also generally effective at identifying document forgeries, including AI-generated fakes. However, several providers lacked the ability to check documents against live government databases to determine whether a document had been reported lost or stolen. The evaluation found

88 DITRDCSA, *Submission 27*, September 2025, p. 5.

89 Australian Information Industry Association, *Submission 11*, p. 3.

90 Digital Rights Watch, *Submission 12*, p. [6].

91 Digital Rights Watch, *Submission 12*, p. [6].

92 DITRDCSA, *Age Assurance Technology Trial – Final Report*, August 2025, p. 60.

> that security against injection attacks – where malicious code or media bypasses the biometric capture process – is improving but still emerging.[93]

2.77 The Australian Research Council (ARC) Centre of Excellence for the Digital Child explained that 'ultimately the only way age can be clearly and efficiently determined by technology companies is to use government issued ID.'[94]

2.78 As noted earlier, the use of government-issued identification documentation for the purpose of complying with the SMMA obligation is permitted, with limitations, under the Online Safety Act. The eSafety Commissioner explained that a provider must offer a reasonable alternative method of age assurance and only where that method is not suitable can Government-issued identification material be collected.[95] Additionally, providers are 'restricted from collecting information that is of a kind specified in legislative rules made by the Minister.'[96]

2.79 In terms of technical implementation, AVPA emphasised that, if proof of an exact minimum age is required, federal and state governments may need to facilitate privacy-preserving one-way blind checks against their own datasets for young people,[97] as opposed to individuals submitting their own identity documents.

2.80 This sentiment echoed concerns expressed in the AATT report that age verification for young people may face constraints. The AATT stated that 'while technically feasible, exact age verification for children is constrained by limited access to hard data'. Further, it outlined that 'government-backed blind-access APIs [application program interface] to records (e.g., schools, healthcare) may be needed to improve precision.'[98]

2.81 However, some participants raised concerns that any reliance on government ID may create barriers for those who have difficulty accessing them.[99] One submission noted '[s]pecial consideration should be given to vulnerable children, such as those in care, to ensure they aren't excluded from online access.'[100]

---

93 DITRDCSA, *Age Assurance Technology Trial – Final Report*, August 2025, p. 62.

94 Australian Research Council (ARC) Centre of Excellence for the Digital Child, *Submission 10*, p. 3.

95 eSafety Commissioner, *Submission 8*, p. 25.

96 eSafety Commissioner, *Submission 8*, p. 25 [citing Section 63D and 63DB of the *Online Safety Act 2021*]. As at September 2025 no such rules have been made or proposed.

97 Age Verification Providers Australia, *Submission 53*, p. 2.

98 DITRDCSA, *Age Assurance Technology Trial – Final Report*, August 2025, p. 61.

99 See, for example, NSW Advocate for Children and Young People, *Submission 1*, [p. 5]; ARC Centre of Excellence for the Digital Child, *Submission 10*, p. 4.

100 NSW Advocate for Children and Young People, *Submission 1*, p. [5].

2.82 The QUT Digital Media Research Centre similarly noted that age verification mechanisms are likely to result in 'uneven burdens and exclusions for marginalised communities'.[101]

2.83 In recognition of the limitations, Mr Corby of AVPA advised the committee that 'there should also be a manual process of professionals in the community attesting to your age if you just can't get access to any alternative'[102], a system that is already available in the UK under a government endorsed scheme.[103]

2.84 The AHRC similarly noted that accessible review pathways are required for users to challenge an age assurance outcome, recommending that:

> … eSafety amends the Social Media Minium Age Regulatory Guidance to mandate that an informed human in the loop be present and engaged in any challenge to an age assurance outcome.[104]

2.85 Review mechanisms for an incorrect age assurance assessment are discussed further in this chapter under 'Accountability, oversight and transparency'.

2.86 Inquiry participants made additional recommendations to strengthen the implementation of age verification. The committee was advised, for example, that '[c]hildren who find a way around one-off age verification methods will no longer be protected from such content', [105] therefore age verification processes should be ongoing, not be a one-time verification.[106]

2.87 The committee was also advised that age-verification providers should require certification against IEEE and ISO standards, and be subject to regular auditing.[107]

2.88 Additionally, the committee heard that regulators should promote interoperability and the reuse of age verification tokens across services 'to cut friction to the user experience and minimise the cost to platforms'.[108]

---

101 QUT Digital Media Research Centre, *Submission 14*, p. [7].

102 Mr Iain Corby, The Age Verification Providers Association, *Committee Hansard*, 13 October 2025, p. 58.

103 Th Age Verification Providers Association, *Submission 54*, p. 4.

104 Australian Human Rights Commissions, *Submission 53*, p. 5.

105 The Australian National University Law Reform and Social Justice Research Hub, *Submission 28*, p. [5].

106 The Australian National University Law Reform and Social Justice Research Hub, *Submission 28*, p. [1].

107 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 57.

108 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, p. 57.

Circumvention

Virtual Private Networks

2.89 Regardless of the chosen age assurance mechanism, many inquiry participants argued that tech savvy children and young people will bypass age gateways using Virtual Private Networks (VPNs) which can be used to disguise a user's location.[109]

2.90 Digital rights organisation Electronic Frontiers Australia advised that age estimation technology and age-gating obligations can be easily circumvented, [110] noting '[d]etermined youth can, and will, use VPNs, borrowed adult accounts, trade credentials or use technology based hacks.'[111]

2.91 Some inquiry participants highlighted that in the United Kingdom's experience, their age assurance requirements led to a 'significant surge' in the use of VPNs, as a 'swift backlash' to the age gateways.[112] The QUT Digital Media Research Centre noted that 'VPN apps quickly became the most downloaded free tools in the Apple apps store'.[113]

2.92 Similarly Bloom-Ed warned that Australia must learn from the experiences of the United Kingdom, United States and France 'where age verification laws led to increased VPN use and access to less regulated platforms.'[114]

2.93 In contrast the committee heard from the age verification industry that, when age assurance measures are implemented correctly, VPNs cannot be used to bypass them.

2.94 AVPA, for example, argued that breaches experienced in the United Kingdom were in part due to lax assurance protocols on the part of platforms, and that users' ages can still be determined despite the use of VPNs.[115] Mr Corby explained:

> … the platforms, particularly social media, need to look at the nature of the traffic they're getting from VPNs. You can always spot VPN traffic and see whether it looks as if it's likely to be from a user who is under age in

---

[109] See, for example, ARC Centre of Excellence for the Digital Child, *Submission 10*, p. 5; Qoria, *Submission 4*, p. 2; Digital Rights Watch, *Submission 12*, p. 12; Away From Keyboard, *Submission 26*, pp. 7-8; Australian Child Rights Taskforce, ChildFund Australia and Dr Rys Farthing, *Submission 25*, p. 11.

[110] Mr John Pane, Chair, Electronic Frontiers Australia Inc., *Committee Hansard*, 13 October 2025, p. 46.

[111] Electronic Frontiers Australia Inc., *Submission 32*, p. 3.

[112] See, for example, ARC Centre of Excellence for the Digital Child, *Submission 10*, p. 5; QUT Digital Media Research Centre, *Submission 14*, p. [11].

[113] QUT Digital Media Research Centre, *Submission 14*, p. [11].

[114] Bloom-Ed, *Submission 23*, p. 2.

[115] Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, pp. 60-61.

> Australia. If it turns out that they're never using social media platforms during school hours in Australia, the currency on their browser is set to the Australian dollar and they're using AEDT as their time zone, then you would ask them to prove that they're not in Australia or to do an age check.[116]

2.95 DITRDCSA's submission also highlighted that the AATT 'debunks the idea that a virtual private network, or VPN, can bypass well-designed age assurance systems', and that geolocation and VPN detection services 'can support enforcement by identifying circumvention attempts.'[117]

2.96 However, the committee was advised by X Corp that there are no effective means to prevent VPN use as a potential circumvention tool for age restrictions 'short of a blanket prohibition or the adoption of disproportionate, invasive, and costly technical measures.'[118]

Logged-out usage

2.97 Whilst age assurance will be required for logged-in users, logged out browsing will not be subject to age assurance measures. Inquiry participants discussed the risks of users moving to a logged-out state to avoid age assurance requirements.

2.98 Some social media platforms, for example, raised concerns that the new SMMA obligation, requiring the accounts of users under 16 to be disabled and preventing the creation of new accounts, would remove a range of account-level safeguards and parental choice protections that the services have developed to strengthen child safety.[119]

2.99 Away From Keyboard also noted that loopholes exist for logged-out users noting '[f]ilters typically apply to logged-in accounts; search results, link previews and "incognito" browsing remain largely unfiltered.'[120]

2.100 However, the committee was advised that some safeguards do exist in logged-out browsing to reduce unintentional exposure to age-inappropriate material.[121] Most significantly, by default, search engine tools and settings must be set to

---

116 Mr Iain Corby, AVPA, *Committee Hansard*, 13 October 2025, pp. 60-61.

117 DITRDCSA, *Submission 27*, September 2025, p. 5.

118 X Corp, *Submission 16*, p. 3.

119 Ms Rachel Lord, Senior Manager, Government Affairs and Public Policy, YouTube AUNZ, *Committee Hansard*, 13 October 2025, p. 9; Ms Stefanee Lovett, Director or Government Affairs and Public Policy, Google, *Committee Hansard*, 13 October 2025, p. 6, Ms Elizabeth Thomas, Senior Director of Public Policy and Digital Safety, Microsoft, *Committee Hansard*, 13 October 2025, p. 6.

120 Away From Keyboard, *Submission 26*, p. 8.

121 Dr Jennifer Duxbury, Director, Policy, Regulatory Affairs and Research, Digital Industry Group Inc. (DIGI), *Committee Hansard*, 24 September 2025, p. 6.

blur online pornographic and high impact violence material for logged out users. [122] The Digital Industry Group Inc. (DIGI) further explained:

> The code also requires providers to apply additional protections for all users which are automatically applied without the user needing to opt-in. These include requirements to prevent, for all users, pornography and violence from appearing in search results for search queries that do not intend to solicit the material and autocomplete predictions that are sexually explicit or violent. The Internet Search Engine Services code also requires services to promote trustworthy content over self-harm material, prevent autocomplete predictions seeking self-harm material, and provide crisis information for all users.[123]

2.101 Inquiry participants articulated how some of the existing measures to protect children from inadvertently seeing age-inappropriate content operate in practice. YouTube representatives, for example, confirmed age-restricted content is blocked out for all logged-out users of YouTube as a baseline protection as well as disabling participation features such as commenting or uploading videos.[124]

2.102 Yahoo similarly advised that it turns:

> … SafeSearch settings on by default for all users, whether they're logged in or logged out, and they have to manually change those. For any child, for example, who was to search on Yahoo for adult content on purpose or by accident, that content would not be displayed unless they were to go in and manually change those search settings.[125]

2.103 DIGI explained that these measures are bolstered by the requirements of the Designated Internet Services Code, requiring pornography sites to 'do their part' to ensure such material is age-gated.[126]

Inadvertent censorship of health information and lawful content

2.104 During the inquiry, the committee received evidence of potential unintended consequences from implementing content filtering associated with Australia's age assurance measures. In particular, inquiry participants expressed concerns that automated content filters may inadvertently block access to sexual health information and block of other lawful content.

---

[122] DIGI, *Submission 6*, pp. 23-24; DITRDCSA, *Submission 27*, p. 27.

[123] DIGI, *Submission 6*, pp. 23-24.

[124] Ms Rachel Lord, Senior Manager, Government Affairs and Public Policy, YouTube AUNZ, *Committee Hansard*, 13 October 2025, p. 7.

[125] Mr Logan Smith, Director, Public Policy and Human Rights, Yahoo, *Committee Hansard*, 13 October 2025, p. 18.

[126] Dr Duxbury, DIGI, *Committee Hansard*, 24 September 2025, p. 6.

Restricting access to essential health information

2.105 Under the Search Engine Services Code, internet search engine services must, among other things, implement measures to:

- prevent Australian children from accessing or being exposed to pornography and high-impact violence material in search results; [127] and
- reduce end-users' unintentional exposure to online pornography, high-impact violence material and self-harm material.[128]

2.106 In particular, internet search engine services will be required to 'implement ranking systems and algorithms designed to reduce the risk of online pornography and high-impact violence material appearing in search results'.[129]

2.107 However, several inquiry participants raised concerns that as Phase 2 codes lack safeguards to protect access to sexual health information, such information will likely be blocked by algorithmic technologies targeting Class 2 material such as pornography.[130]

2.108 For example, the AHRC submitted that content moderation systems 'have a history of over censorship', including by major platforms that have misclassified LGBTQIA+ content as 'sexually explicit or inappropriate', to the determinant of young people 'who already face significant barriers to accessing inclusive health education'.[131]

2.109 Similarly, the Scarlet Alliance warned that the Phase 2 codes mandate approaches that are 'likely to over-capture and restrict access to consent and relationships education material, sexual assault information, and sexual health, family planning and abortion information, for both young people and adults'.[132]

2.110 Furthermore, the committee heard that blocking access to evidence-based sexual health information risks public health and risks peoples' sexual rights.[133] Bloom-Ed, a peak body for evidence-based relationships and sexuality education, submitted that access to evidence-based sexual health information is a 'vital

---

127 See, Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material), June 2025, p. 5.

128 See, Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material), June 2025, pp. 6–7.

129 Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material), June 2025, p. 6.

130 See, for example, ARC Centre for Excellence for the Digital Child, *Submission 10*, pp. 6–7; Eros Association, *Submission 15*, p. 2; Scarlet Alliance, *Submission 17*, p. 6; Bloom-Ed, *Submission 23*, p. [4];

131 Australian Human Rights Commission, *Submission 53*, p. 20.

132 Scarlet Alliance, *Submission 17*, p. [6].

133 Bloom-Ed, *Submission 23*, p. [4].

component of preventive health'.[134] Limiting access to such information, it argued:

> … risks worsening existing health inequities, particularly for those in regional and remote communities where online resources often represent the primary or only means of accessing sexual and reproductive healthcare information. Limiting or blocking access to such information may also inhibit pathways to essential services, including abortion care, HIV prevention and treatment, and other forms of reproductive health support. Thus, the indiscriminate filtering of sexual content has the potential to undermine the health and rights of young people, while creating, or further bolstering, barriers for those who already experience structural inequities.[135]

2.111 While the AHRC considered that the Search Engine Services Code 'contributes positively to the fulfilment of several human rights', the commission also considered it 'important to ensure that such measures do not inadvertently limit access to safe and inclusive information - particularly for LGBTQIA+ young people.'[136] As such, the AHRC considered that '[p]rotective frameworks should therefore be designed in ways that uphold the rights of all young people to access developmentally appropriate and non-exploitative resources.'[137]

2.112 To help achieve this, the AHRC proposed further definitional clarity, recommending: 'The Australian Government and eSafety clarify that Class 1C and Class 2 materials excludes legitimate sexual health and educational content.'[138] The AHRC additionally recommended that:

> eSafety works with industry to create safeguards within Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) to ensure that measures to restrict access to pornography do not inadvertently block access to inclusive, evidence-based sexual health and relationship information, particularly for LGBTQIA+ young people.[139]

Blocking of lawful content

2.113 Some inquiry participants raised concerns that automated tools for filtering content risks inadvertently blocking lawful content from adults. For instance, the Eros Association submitted that:

> Automated tools that detect "nudity" or "pornography" risk wrongly classifying lawful content, including R18+ and X18+ material. This could

134 Bloom-Ed, *Submission 23*, p. [4].

135 Bloom-Ed, *Submission 23*, p. [4].

136 Australian Human Rights Commission, *Submission 53*, pp. 7–8.

137 Australian Human Rights Commission, *Submission 53*, p. 8.

138 Australian Human Rights Commission, *Submission 53*, p. 5.

139 Australian Human Rights Commission, *Submission 53*, p. 4.

> result in adults being denied access to entertainment and information they are legally entitled to view.[140]

2.114 Submitters also raised concerns that the Search Engine Services Code or the SMMA obligation will enable operators of search engine or social media platforms to make censorship decisions regarding information that is lawful.[141]

Accountability, oversight and transparency

2.115 This part of the report outlines inquiry participants' evidence on the accountability, oversight and transparency standards needed to support the effective implementation and operation of the online safety codes and the SMMA obligation.

2.116 The committee heard that the '[o]versight of online safety codes must be independent, transparent, and accountable',[142] and some inquiry participants called for stronger accountability and oversight standards.[143] In particular, inquiry participants' emphasised the importance of independent oversight, monitoring and review mechanisms.

The importance of independent oversight and monitoring

2.117 In giving evidence to the committee, DIGI, which led the development of the Search Engine Services Code, stated that there are a 'number of ways in which the Online Safety Act will work to ensure that the codes are operating correctly'.[144] DIGI explained:

> … the commissioner has oversight of the codes and has powers of enforcement. Under the act, the commissioner also has extensive powers to gather information, including those under the basic online safety expectation processes. Those also cover the expectation on services to take action to protect under-18s from being exposed to this sort of material. Those processes are built into the act. In addition, the codes also provide a range of additional transparency measures. Platforms need to report to the commissioner about the measures that they're implementing, and they also have to explain why those measures are appropriate in accordance with the terms of the code. Appropriateness in the codes is also judged in relation to a range of human rights. Platforms have to consider human rights, including freedom of speech, privacy and children's digital rights. That is an avenue

---

140 Eros Association, *Submission 15*, p. 2.

141 See, for example, Eros Association, *Submission 15*, p. 1; Australian Injecting and Illicit Drug Users League (AVIL), *Submission 24*, p. 2.

142 QUT Digital Media Research Centre, *Submission 14*, p. 9.

143 See, for example, QUT Digital Media Research Centre, *Submission 14*, pp. 9–10; Cybercy, *Submission 2*, p. 2.

144 Dr Jennifer Duxbury, Director, Policy, Regulatory Affairs and Research, Digital Industry Group Inc., *Committee Hansard*, 24 September 2025, p. 2.

> for the commissioner to get sight of how those judgements are being made.[145]

2.118 Despite these measures, some inquiry participants raised concerns that industry-led development and implementation of the codes is flawed and will lead to poor outcomes.[146] For instance, Dr Rys Farthing, a policy expert on child rights, explained to the committee the pitfalls of co-regulation:

> When you hand industry the pen to write their own codes, you don't necessarily get the strongest safety outcomes, the strongest privacy outcomes or the best outcomes for Australian users.[147]

2.119 By way of contrast, Dr Farthing highlighted that legislation for the online privacy code for children includes powers for the Privacy Commissioner to draft the code directly. Dr Farthing noted this was due to it being 'widely understood that co-regulatory process, where you get a tech lobby group to draft a code, isn't going to produce the best outcomes.'[148]

2.120 The QUT Digital Media Research Centre similarly considered that '[i]ndustry self-regulation has repeatedly failed, with platforms setting standards that suit their commercial interests rather than the public good'.[149] Accordingly, the QUT Digital Media Research Centre considered that leaving implementation and evaluation of the codes to industry 'risks regulatory capture, mission creep, and weak enforcement'.[150]

2.121 Moreover, the committee heard that oversight of the online safety codes should engage a broad range of independent stakeholders. For instance, the QUT Digital Media Research Centre submitted that:

> A sustainable oversight model should be multi-stakeholder, drawing on the expertise of independent academics, civil society organisations, educators, child welfare experts, and privacy advocates. Oversight should not be dominated by industry actors or confined to centralised government agencies alone. Effective accountability requires distributed models of evaluation and consultation, rooted in community needs and local contexts.[151]

---

145 Dr Jennifer Duxbury, Director, Policy, Regulatory Affairs and Research, Digital Industry Group Inc., *Committee Hansard*, 24 September 2025, p. 2.

146 See, for example, Dr Rys Farthing, *Committee Hansard*, 13 October 2025, p. 68; QUT Digital Media Research Centre, *Submission 14*, p. 9.

147 Dr Rys Farthing, *Committee Hansard*, 13 October 2025, p. 68.

148 Dr Rys Farthing, *Committee Hansard*, 13 October 2025, p. 67.

149 QUT Digital Media Research Centre, *Submission 14*, p. 9.

150 QUT Digital Media Research Centre, *Submission 14*, p. 9.

151 QUT Digital Media Research Centre, *Submission 14*, p. 10.

2.122 Further, youth services provider, yourtown, recommended that 'oversight mechanisms include independent child rights experts, youth representatives and civil society organisations to ensure the Code reflects community values and the lived experiences of children and young people'.[152] The Australian Research Alliance for Children and Youth submitted that '[o]versight of online safety codes must embed direct youth representation'.[153]

2.123 To monitor the impact of the Phase 2 Codes and the SMMA obligation, Scarlet Alliance argued that an independent oversight body should be established with representatives from 'public health and sexuality education organisations, LGBTQI+ organisations, peer and harm reduction organisations and other human rights stakeholders'.[154] Scarlet Alliance considered such a body is 'essential to minimise the risks of overcapture and restriction of sexuality, LGBTQI+, health promotion, harm reduction and other public interest content for internet users of all ages'.[155]

2.124 Digital Rights Watch submitted that the AHRC and the Office of the Information Commissioner (OAIC) should have an increased role in overseeing the Phase 2 Codes:

> It is insufficient for the eSafety Commissioner and industry participants to be the ultimate arbiter of the success of the Codes. To ensure that human rights and privacy are respected during the implementation and review of the Code, they must also be overseen by The Australian Human Rights Commission and the OAIC.[156]

Assessing impact

2.125 Some inquiry participants considered that current oversight mechanisms are overly focussed on regulatory compliance rather than assessing whether the codes and the SMMA are meeting their intended outcomes.[157]

2.126 For instance, the QUT Digital Media Research Centre submitted that to achieve effective regulatory outcomes 'oversight must shift away from purely technical box-ticking…and instead ask whether interventions are improving'.[158] Such a

---

152 Yourtown, *Submission 19*, p. 6.

153 Australian Research Alliance for Children and Youth, *Submission 5*, p. 2.

154 Scarlet Alliance, *Submission 17*, p. [6].

155 Scarlet Alliance, *Submission 17*, p. [6].

156 Digital Rights Watch, *Submission 12*, p. 17.

157 See, for example, Cybercy, *Submission 2*, p. 2; Away from Keyboard, *Submission 26*, p. 11.

158 QUT Digital Media Research Centre, *Submission 14*, p. 10.

shift requires 'long-term investment in independent, public interest research with guaranteed access to platform data'.[159]

2.127 Away from Keyboard similarly submitted:

> Oversight of online safety codes in Australia currently emphasises process compliance rather than outcome effectiveness. Platforms can self-report on their adherence to codes, but there is no systematic way to verify whether children are actually safer, harmful content is actually reduced, or carers have become more digitally literate. Without rigorous oversight, regulation risks becoming symbolic rather than transformative.[160]

2.128 Further, Away from Keyboard made several recommendations to improve the oversight and transparency of the impact of the codes, including mandating public dashboards showing information on key harm reduction metrics and commissioning independent expert evaluations of the codes every two years.[161]

2.129 To increase transparency, the AHRC similarly considered that the eSafety Commissioner should update its SMMA obligation guidance to 'require age-restricted social media platforms to publish annual transparency reports'.[162] The AHRC recommended that the reports 'include anonymised, aggregated data' on:

- account removals;
- age assurance outcomes;
- review processes; and
- the number of successful challenges.[163]

Review mechanisms

2.130 Some inquiry participant considered that the oversight arrangements for the Search Engine Safety Code and the SMMA obligation should include robust mechanisms that ensure age assurance related decisions are subject to review.

2.131 For example, the AHRC expressed concern that the Search Engine Safety Code 'does not prescribe a mechanism for users to challenge the outcome of an incorrect age assurance process.'[164] The AHRC submitted that this omission was problematic given the automation involved in age assurance technologies that carry 'known risks of error, demographic bias and limited transparency'.[165] As

---

159 QUT Digital Media Research Centre, *Submission 14*, p. 10.

160 Away from Keyboard, *Submission 26*, p. 11.

161 Away from Keyboard, *Submission 26*, pp. 12–13, 19.

162 Australian Human Rights Commission, *Submission 53*, p. 17.

163 Australian Human Rights Commission, *Submission 53*, p. 17.

164 Australian Human Rights Commission, *Submission 53*, p. 16.

165 Australian Human Rights Commission, *Submission 53*, p. 16.

such, the AHRC recommended that an additional compliance measure be added to the Search Engine Safety Code to require 'an accessible review pathway for users to challenge an age assurance outcome'.[166]

2.132 Further, Mr Joel Canham, an owner of a small online creative community platform, considered that oversight measures should specify 'what review mechanism exists for wrongful blocking or content removal'.[167] Further, Bloom-Ed recommended that:

- protections for educational content be embedded in the safety codes to prevent overreach; and
- clear mechanisms be established to 'prevent industry-led censorship of health and education platforms'.[168]

2.133 Unlike the Search Engine Safety Code, the eSafety Commissioner's regulatory guidance on the SMMA obligation states that providers 'should offer accessible, fair, and timely complaints or review mechanisms for end-users'.[169] Such mechanisms would address:

- adverse outcomes resulting from any age assurance processes;
- adverse outcomes resulting from reports of underage accounts; and
- account deactivation / removal decisions.[170]

2.134 While acknowledging the eSafety Commissioner's SMMA regulatory guidance, the AHRC contended that the guidance 'does not go far enough in safeguarding the integrity of these review processes'.[171] In particular, the AHRC recommended that the SMMA regulatory guidance be updated to strengthen provisions for human involvement in reviewable decisions.[172]

2.135 Additionally, the AHRC recommended that the independent statutory review of the SMMA obligation—required to commence within two years of the obligation taking effect—be supported by the eSafety Commissioner 'immediately' establishing baseline parameters and data collection about the use of social media by under-16s.[173]

---

166 Australian Human Rights Commission, *Submission 53*, pp. 16–17.

167 Mr Joel Canham, *Submission 39*, p. [2].

168 Bloom-Ed, *Submission 23*, p. [2].

169 eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance*, September 2025, p. 41.

170 eSafety Commissioner, *Social Media Minimum Age Regulatory Guidance*, September 2025, p. 41.

171 Australian Human Rights Commission, *Submission 53*, p. 17.

172 Australian Human Rights Commission, *Submission 53*, pp. 15–16.

173 See, Australian Human Rights Commission, *Submission 53*, p. 18.

Minister's rule making power

2.136 In addition to issues outlined above, the AHRC noted that under the Online Safety Act the Minister for Communications has 'sole discretion to determine what social media platforms must comply with the Guidance via disallowance instruments'.[174] This approach 'gives the Minister broad powers to decide' which social media platforms must comply with the SMMA obligation.[175]

2.137 While acknowledging the importance of flexibility in the regulation of the digital environment, the AHRC considered that the 'absence of clear decision-making standards or safeguards around the exercise of discretion increases the risk of arbitrary or politically motivated decisions'.[176]

2.138 The AHRC recommended that the Online Safety Act be amended to establish clear decision-making criteria that are 'evidence-based, transparent and consistent with the best interests of children'.[177]

Next chapter

2.139 The following chapter considers evidence from inquiry participants in relation to complementary and alternative approaches to enhance children's safety online and concludes with the committee's view.

---

174 Australian Human Rights Commission, *Submission 53*, p. 15.

175 Australian Human Rights Commission, *Submission 53*, p. 15.

176 Australian Human Rights Commission, *Submission 53*, p. 15.

177 Australian Human Rights Commission, *Submission 53*, p. 15.

Chapter 3
Complementary and alternate approaches to online safety

3.1 This chapter considers inquiry participants' evidence on the complementary and alternate approaches to regulation aimed at improving children's and young peoples' online safety. In particular, the chapter considers evidence on:

- digital duty of care;
- education, digital literacy and social change;
- device level controls; and
- enhanced privacy laws.

3.2 The chapter concludes with the committee's view and recommendations.

Overview

3.3 Although the majority of inquiry participants indicated significant concerns about the risks for children and young people in the digital environment and on social media, many did not believe the industry codes, legislated SMMA obligation, or the use of age assurance to give effect to those restrictions, were effective solutions.

3.4 Instead, many participants advocated for a more systemic approach to children's online safety, calling for social media and online spaces to be made safer for young people, rather than restricting their access.[1] The Australian Human Rights Commission (AHRC), for example, argued:

> Regulatory efforts like this must focus on embedding safety by design features that respect, protect and promote human rights. Age assurance should not be treated as the default or preferred method of online safety, particularly where it risks undermining privacy, equality and freedom of expression. [2]

3.5 Inquiry participants supported a range of alternative and complementary regulatory approaches to protect children and young people online which they argued are more effective, systematic and future-proof. The AHRC summarised this sentiment:

> Other safety by design approaches (such as content filtering, crisis response tools, education and Digital Duty of Care) could offer a more proportionate

---

1 See, for example, Australian Human Rights Commission, *Submission 53*, p. 13; Dr Rys Farthing, *Committee Hansard*, 13 October 2025, p. 67; Ms Lauren Frost, Advocacy Manager, Policy and Communications, Youth Affairs Council Victoria, *Committee Hansard*, 13 October 2025, p. 34; Ms Johanna Weaver, Tech Policy Design Institute, *Committee Hansard*, 13 October 2025, p. 66.

2 Australian Human Rights Commission, *Submission 53*, p. 13.

> and rights-respecting pathway to protecting children online. These approaches have potential to shift responsibility from users to service providers and can be implemented with less risk of compromising privacy, autonomy or inclusion.[3]

3.6 Dr Rys Farthing similarly expressed support for an approach that targets the risks platforms have engineered, not who the user is. [4] He argued for an upstream, systemic approach that would see platforms conducting risk assessments on content, explaining:

> Every single piece of how they work, from what the like button looks like to how the content recommender system prioritises content in your feed, is code that's written by humans. That can be changed. If we take that systemic focus that looks at what the systems and processes that digital platforms and services build are and actually place requirements on them to drive up safety, to drive up security and to drive up privacy, then I think we start to see the risk profile of the digital world decrease.[5]

3.7 The Tech Policy Design Institute raised additional concerns that the current legislative measures risk being interpreted as a 'job done' solution, rather than part of an ongoing process of improvement. Whilst noting Australia is making positive changes in this space, Ms Johanna Weaver, Co-Founder and Executive Director of the Tech Policy Design Institute, advised that urgent reforms need to continue and should extend to duty of care, privacy and competition reforms if systemic change is to be realised.[6]

Digital duty of care

3.8 Inquiry participants indicated strong support for digital duty of care obligations to be placed on digital platforms, as a wide-reaching mechanism to strengthen online safety.[7]

3.9 In 2024, the Government announced the introduction of new Duty of Care obligations, as recommended in the statutory review of the *Online Safety Act 2021*.[8] A digital duty of care would place a legal responsibility on all digital

---

3 Australian Human Rights Commissions, *Submission 53*, p. 4.

4 Dr Rys Farthing, *Committee Hansard*, 13 October 2025, p. 66.

5 Dr Rys Farthing, *Committee Hansard*, 13 October 2025, p. 68.

6 Ms Johanna Weaver, Co-Founder and Executive Director, Tech Policy Design Institute, *Committee Hansard*, 13 October 2025, p. 66.

7 See, for example, Australian Human Rights Commissions, *Submission 53*, p. 5; Ms Lauren Frost, Advocacy Manager, Policy and Communications, Youth Affairs Council Victoria, *Committee Hansard*, 13 October 2025, p. 34;

8 The Hon Michelle Rowland, Media Release, *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

platforms to proactively keep Australians safe and prevent harms more effectively. The Independent Review of the Online Safety Act Report explained:

> A duty of care shifts the emphasis of regulation from reactively tackling specific pieces of material to remediate the harm, to taking a preventative and systems-based approach. [9]

3.10 Ms Lucy Thomas OAM of Project Rockit explained how a duty of care obligation is 'a much more future-proofed, future-focused and effective method' than potentially excluding young people in their digital participation. She explained the duty-of-care approach:

> … embeds a safety-by-design ethos by ensuring that platforms that design these digital environments—and profit from our use of them—are compelled to create environments that are worthy of young people.[10]

3.11 Inquiry participants highlighted that the SMMA obligation does not capture all platforms, nor all mechanisms of harm. [11] A similar point was made by the report of the independent statutory review of the *Online Safety Act 2021*,[12] which noted '[t]here are other vectors of harm not properly captured by a focus on content, including contact and conduct.' [13]

3.12 The committee was advised that duty of care obligations should be prioritised to address these shortfalls, and address 'deeper issues' such as algorithms, recommender systems, infinite scrolling, addictive designs, misinformation, AI, and more.[14] Inquiry participants also highlighted that duty of care obligations can address all age groups, address harmful content and matters around personal data extraction. Mr Pane of Electronic Frontiers Australia, for example, explained:

> A digital duty of care requires platform design to not only inherently minimise content or function related harm but also severely restrict personal data extraction and prohibit algorithmic manipulation.[15]

---

9 Delia Rickard PSM, *Report of the statutory review of the Online Safety Act 2021*, October 2024, p. 50.

10 Ms Lucy Thomas OAM, Chief Executive Officer, Project Rockit, *Committee Hansard*, 13 October 2025, p. 32

11 Ms Nicola Palfrey, Head of Clinical Practice, Headspace National Youth Mental Health Foundation, *Committee Hansard*, 13 October 2025, p. 32.

12 Under section 239A of the Online Safety Act 2021, the Minister for Communications is required to initiate an independent review of the Act within three years of the Act's commencement. The initial review of the Act was brought forward by one year.

13 Delia Rickard PSM, *Report of the statutory review of the Online Safety Act 2021*, October 2024, p. 50.

14 See, for example, Ms Lauren Frost, Advocacy Manager, Policy and Communications, Youth Affairs Council Victoria, *Committee Hansard*, 13 October 2025, p. 34.

15 Mr John Pane, Chair, Electronic Frontiers Australia Inc., *Committee Hansard*, 13 October 2025, p. 43.

3.13 Some participants also noted that a digital duty of care also provides a flexible and open-ended approach that incentivises and encourages better behaviour for minimising inappropriate content, and gives rise to proactive ongoing regulatory engagement.[16] The abovementioned 2024 review of the Online Safety Act echoed this sentiment, noting:

> It is also an approach that can deal with technologies and harms not yet dreamed of. It can help future proof regulation. Algorithms, recommender systems, addictive design, artificial intelligence, and generative artificial intelligence, business decisions and more are all factors that shape an individual's online experience and have the potential to create significant harm.[17]

3.14 Significantly, the committee was advised that duty of care obligations can be implemented in parallel with the current legislative approach. Dr Rys Farthing, for example, highlighted:

> At the moment, in Australia, the focus appears to be more on finding out which piece of content is what and which user is what. We're looking at really specific instances of use and users, rather than looking at how platforms engineer risk. Those approaches can go hand in hand. You could do both at the same time.[18]

Education, digital literacy and social change (parental empowerment)

3.15 Many inquiry participants championed the need for enhanced education and digital literacy as essential to achieving a comprehensive approach to children's online safety.[19] For example, Ms Lauren Frost of the Youth Affairs Council Victoria, argued:

> We believe we should be investing in co-designed education programs and resources for young people, parents, carers, youth workers and educators to ensure that young people are supported and confident to engage with online spaces safely and, importantly, to ensure they know where to go for support if they experience online harm.[20]

3.16 The Centre for Multicultural youth echoed this sentiment, noting that education training and support for digital literacy are critical, particularly if children find a way around the proposed controls or are driven underground. Ms Harini Kasthuriarachchi explained:

---

16 Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 13 October 2025, p. 46.

17 Delia Rickard PSM, *Report of the statutory review of the Online Safety Act 2021*, October 2024, p. 51.

18 Dr Rys Farthing, *Committee Hansard*, 13 October 2025, p. 66.

19 See, for example, Ms Harini Kasthuriarachchi, Policy Officer, Centre for Multicultural Youth, *Committee Hansard*, 13 October 2025, pp. 39-40; Ms Lauren Frost, Advocacy Manager, Policy and Communications, Youth Affairs Council Victoria, *Committee Hansard*, 13 October 2025, p. 34.

20 Ms Lauren Frost, Advocacy Manager, Policy and Communications, Youth Affairs Council Victoria, *Committee Hansard*, 13 October 2025, p. 34.

> It's important to remember that this ban isn't intended to punish young people; its intention is to try [and] manage the risks that social media pose. Alongside the ban and implementation, it's really important that we communicate really clearly with young people that, if they do encounter issues if and when they do access social media, there are supports for them and they should reach out to adults or the eSafety Commission—whoever might be relevant. We must ensure that they're not being punished for platforms continuing to be unsafe. There are risks we know are continuing to be perpetuated.[21]

3.17 QUT Media Centre praised the emphasis on digital literacy and civic education in Finland, Sweden, and Indonesia, where digital literacy resources and training are targeted at a broad cross-section of the community. QUT Media Centre explained that a whole-of-society approach to digital literacy builds resilience against misinformation and harmful online content. Recognising 'that critical thinking and digital literacy skills are important sites of development for young people as well as a lifelong skill for all current and future users of digital systems.' It further noted:

> These strategies work not by seeking to eliminate risk entirely, which is impossible, but by equipping young people with the skills and confidence to navigate complex digital environments safely.[22]

3.18 Some participants also emphasised the need to empower parents as well as initiating social change.[23] Ms O'Shea from Digital Rights Watch, for example, noted there is a lot of work to be done in digital literacy that can't be ignored and is going to be 'generations long'.[24] She encouraged having meaningful conversations with parents and 'encouraging greater conversations between parents and children about responsible use', whilst also acknowledging the difficulties parents can face.[25]

3.19 Mr Pane, Electronic Frontiers Australia, highlighted the need for social change to support regulatory reforms. He contended that introducing digital safety and digital health as part of the curricula at primary and secondary level schooling

---

21 Ms Harini Kasthuriarachchi, Policy Officer, Centre for Multicultural Youth, *Committee Hansard*, 13 October 2025, pp. 39-40.

22 QUT Media Centre, *Submission 14*, [p. 12].

23 See, for example, Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 13 October 2025, p. 47; Mr John Pane, Chair, Electronic Frontiers Australia Inc., *Committee Hansard*, 13 October 2025, p. 47; Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 51.

24 Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 13 October 2025, p. 47.

25 Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 13 October 2025, p. 47.

must be accompanied by parental responsibility in relation to the types of devices young children are given.[26]

3.20 Online safety technology company Qoria reinforced the importance of parental empowerment in achieving better outcomes in a child's digital life, including via technology loaded on a device. Mr Tim Levy, Qoria Founder and Managing Director, emphasised 'safety starts with protecting the device' because 'that's the gateway to the internet.'[27] Mr Levy also raised concerns that the 'the rights and roles of parents in online safety seem to be completely absent from all these discussions', describing this as a fatal flaw.[28]

Device level controls

3.21 The committee heard from inquiry participants that although duty of care obligations are important, 'outsourcing safety to global platforms'[29] will not be adequate to achieve the wide-reaching results necessary for children's online safety and must be backed by device-level controls. [30]

3.22 Mr Levy called for a focus on policy settings 'that facilitate the simple, reliable, and interoperable use of these tools, ensuring parents' choices are respected across all devices and platforms.'[31] He explained to the committee that parental use of downloadable device controls won't prevent the use of VPNs 'to get around the kind of geofenced protections that we're trying to put in place in this country'.[32] Instead, Mr Levy emphasised that greater interoperability between the parental control systems of tech giants and greater access to enterprise safe technologies for families were key to achieving effective device-level controls.[33]

3.23 Ms Weaver of the Tech Policy Design Centre echoed this advice, stating that interoperability and addressing barriers to on-device protection need to be part of a systemic change.[34]

3.24 Qoria submitted that enterprise technology controls are 'the method (so-called "end point protection") which is prioritised by businesses to protect their

---

26 Mr John Pane, Chair, Electronic Frontiers Australia Inc., *Committee Hansard*, 13 October 2025, p. 47.

27 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 55.

28 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 51.

29 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 52.

30 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 54.

31 Qoria, *Submission 4*, p. 4.

32 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 56.

33 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, pp. 51, 55.

34 Ms Johanna Weaver, Tech Polic Design Centre, *Committee Hansard*, 13 October 2025, p. 66.

information, services and devices.'[35] Mr Levy explained that these technologies can control whether VPNs are used and how, can stop access to the dark web and direct children to safer versions of search engines.[36] When installed at an 'enterprise' level, such as by schools, Qoria's experience in the United States demonstrates that safety tools 'ensure age-appropriate access to all online platforms … and the entirety of the web.'[37] He noted:

> Enterprise safety technology provides almost all the security, privacy and safety measures that parents are begging for. But, that technology is being withheld by Google, Apple and Microsoft who only provide that access to enterprise app developers.[38]

3.25 The committee was advised that the buying power and demand from enterprises has driven enterprise access to safety technology. However, Google, Apple and Microsoft are 'not allowing true competition in safety technology in the consumer world because parents don't have buying power.'[39]

3.26 Mr Levy noted that licensing issues can be solved with enhanced competition, including through pressure such as utilising levers in government procurement practices.[40] He stated '[i]f you free us up with interoperable access to this technology, the market will solve the problem of parents.'[41]

Prohibiting monetisation of children's data

3.27 In addition to the above concerns relating to the risk of potential misuse of data collected for the purposes of age verification, inquiry participants submitted that a broad prohibition on the monetisation of children's data is a necessary feature in a systemic approach to online safety.

3.28 Submitting that 'data is the currency of the online world', UNICEF outlined some of the emerging risks for children relating to data and privacy, including 'through data monetisation, microtargeted advertising, profiling and automated decision-making.'[42]

3.29 Digital Rights Watch Chair, Ms Elizabeth O'Shea, advised that prohibiting the monetisation of children's data is one mechanism to minimise profiling and 'the

---

35 Qoria, *Submission 4*, p. 3.

36 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, pp. 51, 56.

37 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 51.

38 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 51.

39 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 53.

40 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 52.

41 Mr Tim Levy, Founder, Managing Director, Qoria, *Committee Hansard*, 13 October 2025, p. 54.

42 UNICEF, *Submission 13*, p. [2].

tendency for social media platforms to send young people down rabbit holes'.[43] Further, Ms O'Shea emphasised that 'there is a whole advertising ecosystem that we might wish to interrogate', calling for greater transparency around where advertising revenue for digital platforms comes from. Ms O'Shea explained:

> … we know that gambling companies, alcohol companies and junk-food companies are big advertisers on social media. A prohibition on gambling advertising for young people is a straightforward policy reform that could reduce harm and that, as I understand it, is supported by the vast majority of Australians.[44]

3.30 Additionally, one inquiry participant questioned advertising claims made by social media platforms, stating:

> It may well be true that they're not serving ads of organisations that pay for advertising on their platform, but those platforms are full of influencers, and a lot of them are doing so to promote a product. That's advertising, so I would question that.[45]

Enhanced privacy laws

3.31 Enhanced privacy protections were also noted as essential for a comprehensive online safety regulatory framework.

3.32 The Privacy Commissioner, Ms Carly Kind, noted that there are new privacy protections in the Social Media Minimum Age scheme, generally relating to purpose limitation of information collected, and associated requirements to destroy information collected for age-assurance purposes when its purpose is fulfilled.[46]

3.33 Additionally, the Children's Online Privacy Code is being drafted by the Office of the Australin Information Commissioner (OAIC). The Alannah and Madeline Foundation expressed its support for the 'development and appropriate resourcing of a meaningful, comprehensive Children's Online Privacy Code which treats the best interests of the child as its central priority.'[47]

3.34 However, some participants were concerned that the framework within which the children's privacy code was being drafted is fundamentally flawed, particularly the Australian Privacy Principles.[48] Mr Pane of Electronic Frontiers Australia explained to the committee:

---

43 Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 13 October 2025, p. 47.

44 Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 13 October 2025, p. 47.

45 Mr John Pane, Chair, Electronic Frontiers Australia Inc., *Committee Hansard*, 13 October 2025, p. 48.

46 Ms Carly Kind, Privacy Commissioner, *Committee Hansard*, 13 October 2025, p. 79.

47 Alannah & Madeline Foundation, *Submission 3*, p. 5.

48 Electronic Frontiers Australia, *Submission 32*, p. 2.

> The existing APPs are already fundamentally flawed and have not kept pace with technology, despite their claims of being technologically neutral. This means, again, the government is poised to pass privacy regulation based on a redundant and antiquated regulatory precedent.
>
> A genuinely safe internet for children begins with a mandated digital duty of care backed by privacy laws strong enough to prevent and prosecute against the systemic harms caused by surveillance based capitalism…[49]

3.35 Some inquiry participants argued there is a need for Privacy Act amendments, and urged the adoption of the remaining recommendations of the Privacy Act Review Report which were accepted or accepted in principle by the government.[50] Digital Rights Watch explained:

> We would advocate that we need to move to a world of data minimisation and that that should be enshrined in the Privacy Act through various amendments that the government has accepted need to be made to the Privacy Act but have not yet progressed.[51]

3.36 In particular, inquiry participants indicated support for privacy reforms introducing a fair and reasonable test,[52] requiring 'that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.'[53]

Committee view

3.37 Like many inquiry participants, the committee welcomes efforts to improve online safety for Australian children and young people. The committee recognises that online safety is a difficult space to regulate given the complex, decentralised and evolving nature of the digital world.

3.38 Nonetheless, it is vital that Australia pursues highly effective safeguards that enable children and young people to participate in the online world without being exposed to age-inappropriate material and without experiencing anti-social behaviour or unlawful conduct, such as bullying and sexual harassment. Such harms demonstrably undermine children's and young people's wellbeing.

3.39 At the same time, children and young people are growing up in world where online technologies are ubiquitous and, indeed, instrumental to social participation. Search engines and digital media platforms serve as vast repositories of information from which young people can learn. Similarly, social

---

49 Mr John Pane, Chair, Electronic Frontiers Australia Inc., *Committee Hansard*, 13 October 2025, p. 44.

50 Alannah & Madeline Foundation, *Submission 3*, p. 5.

51 Ms Elizabeth O'Shea, Chair, Digital Rights Watch, *Committee Hansard*, 13 October 2025, p. 44.

52 See, for example, Queensland Council for Civil Liberties, *Submission 18*, p. 4; Alannah & Madeline Foundation, *Submission 3*, p. 8; Ms Johanna Weaver, Co-founder and Executive Director, Tech Policy Design Centre, *Committee Hansard*, 13 October 2025, p. 66.

53 Attorney-General's Department, *Privacy Act Review Report*, December 2022, p. 14.

media platforms are often spaces where young people engage with their peers and the world.

3.40 Achieving the right balance between online protections for children and young people and supporting their online participation is clearly a challenging task. The age assurance measures under the Search Engine Services Code and the SMMA obligation are substantial measures that will have a major effect on the online experience of millions of Australians. Indeed, the SMMA obligation is a world first regulation.

3.41 However, a central concern for the committee is whether the current Australian regulations reflect world's best practice for children's and young people's online safety and, if not, what needs to be improved.

3.42 Unfortunately, much of the evidence to this inquiry highlights serious concerns regarding the implementation of age assurance measures under the Search Engine Services Code and the SMMA obligation. In the committee's view, many of these concerns remain unresolved and risk undermining the intent of improved online safety for children and young people. Indeed, the committee views many of the issues raised during the inquiry as significant problems that could meaningfully undermine the efficacy of Australia's soon-to-be implemented age assurance measures.

3.43 At the time of the committee's report, age assurance under the SMMA is two weeks away from commencing and age assurance under the Search Engine Services Code will commence in a month. Given the significance of these changes, the committee is concerned that so many of the details around the implementation of age assurance remain uncertain. Crucially, this includes a lack of detail on the specific age verification mechanisms that search engine operators and social media companies intend to apply to their respective platforms.

3.44 The committee is concerned that simply banning young people from a certain number of platforms will drive them to other, less safe and less controlled platforms that are not covered by the SMMA obligation. Platforms like Telegram, Roblox and other gaming platforms also contain serious risks for young people but are not currently captured by the SMMA obligation.

3.45 The SMMA obligation could mean that platforms no longer provide age-appropriate accounts for young people, for example Instagram accounts that have direct messages automatically turned off. In addition, young people accessing platforms like YouTube in a logged out state will mean that they have the age-appropriate safeguards that the platforms currently provide removed.

3.46 The committee is concerned that there has not been an adequate education program rolled out to young people who will be cut off from their online communities and connections when the SMMA obligation comes into place, especially young people who are already socially isolated.

Recommendation 1

3.47 The committee recommends that the implementation of the Social Media Minimum Age obligation be delayed until 10 June 2026 to allow time for the issues in implementation and compliance to be properly considered and an education campaign for young people affected to be rolled out.

Recommendation 2

3.48 The committee recommends that the Australian Government legislate a digital duty of care to make online platforms safer for all users.

Recommendation 3

3.49 The committee recommends that the Australian Government legislate to prohibit platforms from harvesting and exploiting the data of minors and protect young people from targeted, unsolicited advertisements and algorithms as a matter of priority, with a view for this to apply to all users in the long-term to protect all Australians' safety and privacy.

Recommendation 4

3.50 The committee recommends that the eSafety Commissioner roll out an education program, including through schools, that delivers clear information to young people about the platforms that are covered by the Social Media Minimum Age obligation and what the impacts on young people will be, as well as information about digital literacy and online safety.

Senator Sarah Hanson-Young
Chair
Greens Senator for South Australia

Labor Senators' dissenting report

Introduction

1.1 On 27 August 2025, the 48th Australian Parliament referred the implementation of regulations aimed at protecting children and young people online, with particular reference to the Internet Search Engine Services Online Safety Code (the Online Safety Code) and the Social Media Minimum Age (SMMA) obligation to the Environment and Communications References Committee for inquiry and report. The appointment and conduct of the inquiry are set out in Chapter 1 of the committee's report.

1.2 Labor Senators would like to thank all submitters and witnesses who provided evidence during the inquiry. While the goal of improving the safety of children and young people online and minimising their exposure to harm was widely supported, we acknowledge the range of views expressed about how to achieve this in practice and on the Online Safety Code and the SMMA obligation.

1.3 As noted in the Chapter 2 of the committee's report, the inquiry received evidence on a variety of subjects, including: (a) the extensive use of technology by children and young people; (b) the harms associated with age-inappropriate material; (c) the importance of online access for wellbeing and development; (d) the privacy and data implications of age assurance measures; (e) the efficacy of age assurance measures and technical limitations; and (f) the adequacy of oversight mechanisms for age assurance measures.

1.4 Balancing the objectives, risks and concerns that emerged from the evidence to this inquiry will require holistic, coherent, practical, and evidence-based policies.

1.5 Labor Senators appreciate the evidence and analysis set out in the committee's report and support, in whole or in part, several of its recommendations. However, we have some reservations about some of the conclusions that have been reached from this evidence, and with some of the recommendations that have been made in the committee report. Labor Senators' views on aspects of the evidence and the committee report recommendations are outlined below.

Importance of online safety and the inadequacy of earlier measures

1.6 Evidence received by the inquiry (and outlined in the committee's report) emphasised that young people use technology extensively, often have access to electronic devices from a young age, and use search engines and social media frequently.

1.7 The Alannah and Madeline Foundation has found that 'use of digital technologies is almost ubiquitous among Australian children and typically

starts at an age when children are far too young to fully understand or manage the risks.'

1.8 Based on surveys, it is estimated that four in five Australian children aged eight to twelve used at least one social media service in 2024 and around 36% of children aged eight to twelve who used social media had their own account.[1]

1.9 There was evidence that children and young people are more susceptible to harms associated with social media usage than older users,[2] and that social media use was linked to a decline in the mental wellbeing of young people.[3]

1.10 Some of the specific concerns raised included:

(a) the availability of dangerous self-harm material online and its potential to cause serious harm, particularly to vulnerable groups;[4]
(b) the damaging effects of exposure to pornography and sexual material at a young age either online or through social media, its impact on attitudes to women, relationships and sex, and its influence in shaping inappropriate and unhealthy sexual behaviours and norms;[5]
(c) the tendency of algorithms to promote extreme, polarising, sensationalist, and discriminatory content to young people;[6] and
(d) the link between social media use and increases in behavioural issues in classrooms[7] and eating disorders.[8]

1.11 The eSafety Commissioner has indicated that almost two-thirds of 14–17-year-olds are exposed to extreme or harmful content.

1.12 Evidence also suggested that unsafe social media content disproportionately impacts vulnerable groups. Surveys of children aged 10 to 17 showed that exposure to content that suggests self-harm or suicide was higher among trans

---

1 eSafety Commissioner, *Submission 8*, p. 10.

2 eSafety Commissioner, *Submission 8*, p. 13.

3 See, Collective Shout, *Submission 33*, p. 3; Alannah and Madeline Foundation, *Submission 3*, p. 5.

4 Alannah and Madeline Foundation, *Submission 3*, p. 5

5 See, Ms Julie Inman Grant, eSafety Commissioner, *Committee Hansard*, 13 October 2025, p. 71; NSW Advocate for Children and Young People, *Submission 1*, p. 2; eSafety Commissioner, *Submission 8*, pp. 14–15; Collective Shout, *Submission 33*, p. 6.

6 See, Ms Harini Kasthuriararchchi, Policy Officer, Centre for Multicultural Youth, *Committee Hansard*, 13 October 2025, p. 36; ANU Law Reform and Social Justice Research Hub, *Submission 28*, p. 3.

7 Collective Shout, *Submission 33*, p. 6.

8 Collective Shout, *Submission 33*, p. 3.

and gender-diverse children (46%), sexually diverse teens (43%), First Nations children (31%) and children with disability (27%).[9]

1.13 It is clear from the evidence received by the inquiry that earlier safeguards and regulations were inadequate to keep young people safe online.

1.14 There was evidence that many parents felt insufficiently equipped to monitor the online activities of their children. The Alannah and Madeline Foundation found 'only 43% of parents used controls or other means of blocking or filtering websites, with usage dropping once children reached their teens. Another survey found only half of Australian parents believed they could apply controls or change filter preferences without help'.[10]

1.15 In addition, many Australian parents felt social media was not suitable for children and that significant proportions of Australian parents believed children were not safe on social media platforms.[11]

Online Safety Code and SMMA obligation

1.16 Evidence indicates that the incentive structures of many online platforms prioritise engagement over safety and that protections have not kept pace with emerging risks. Some of those risks are set out above and in the committee report.

1.17 Research undertaken by the eSafety Commissioner indicates that 95% of caregivers say online safety is one of their most difficult parenting challenges.

1.18 The Online Safety Code and the SMMA obligation represent important measures to try to improve the safety of children and young Australians in the online world. By creating obligations on platforms and companies, the measures take steps to strengthen platform accountability without penalising Australian children or parents.

1.19 The SMMA obligation sets a national consistent minimum age of 16, which reflects research showing heightened vulnerability in early adolescence and a need for additional safeguards during this developmental stage.

1.20 The goal is to protect, not isolate, children and young people by trying to exclude harmful online content and behaviour while maintaining access to connection, support, and learning online.

1.21 The SMMA obligation creates a norm that will assist in reducing online harm to children and young people and supports Australian parents.

---

9 eSafety Commissioner, *Submission 8*, p. 15.

10 Alannah and Madeline Foundation, *Submission 3*, p. 6.

11 Collective Shout, *Submission 33*, p. 5.

1.22 The Online Safety Code endeavours to remove harmful and age-inappropriate content in an online environment with constantly evolving technology.

1.23 It was developed by industry with consultation from eSafety and complements the SMMA obligation by introducing additional safeguards.

Specific concerns raised before the inquiry

Age assurance and privacy

1.24 Labor Senators acknowledge the range of views expressed to the inquiry about the methods of age assurance and the best ways to manage the safety of people online while continuing to protect individual privacy.

1.25 Labor Senators acknowledge the community expectation that collection of personal information is done in a way that upholds privacy.

1.26 The Alannah and Madeline Foundation found that '56% of Australian parents agree 'It is not clear to me how I can protect my child / children's personal information while using a service'; 60% of parents say they often have no choice but to sign their child up to a particular service; and 55% of teens agree 'It's important to me that my personal information is kept private, but it's confusing and I don't really understand it'.[12]

1.27 The Age Assurance Technology Trial (the Trial) illustrates that age assurance is both technically feasible and is already being used in Australia and internationally.

1.28 The Trial found a wide range of age assurance approaches existed, including official identification checks, AI-based age estimation, and inference from user behaviour. The Trial also concluded that there is no one-size-fits all solution to age assurance, and that multiple effective technologies can be used to be best matched to the context and risk profile of the service.[13]

1.29 Overall, a staged or 'waterfall' approach to age assurance was recommended by a number of inquiry participants.[14]

1.30 Importantly, no Australian will be forced to use government identification for age assurance under the SMMA obligation as the legislation requires that 'platforms must not collect government-issued identification or require the use of Digital ID (provided by an accredited service, within the meaning of the Digital ID Act 2024), unless a reasonable alternative is also offered'.[15]

---

12 Alannah and Madeline Foundation, *Submission 3*, p. 8.

13 AIIA, *Submission 11*, p. 2.

14 Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, *Committee Hansard*, 13 October 2025, p. 57.

15 DITRDCA, *Submission 27*, p. 12.

1.31 Labor Senators also note the evidence received about other measures that may help to minimise privacy risks associated with data collection by corporations for age assurance purposes, such as third-party age verification providers.

1.32 The legislation contains stringent data protection requirements. As Collective Shout noted in its submission that the legislation will require companies to 'ring-fence to destroy data collected for age assurance once the age check is complete'.[16]

1.33 Mr Iain Corby from the Age Verification Providers Association (UK) also noted '[t]he OAIC have provided very detailed guidance on what their expectations are for privacy in this area'.[17]

1.34 Labor Senators also recognise the Online Safety Code and methods of Age Assurance need to be continually reviewed and updated such that providers will improve their approaches to age assurance over time, including 'where new approaches are more effective, privacy-preserving or decrease the burden on users'.[18]

Risk of creating barriers to sexual education and health material

1.35 Labor Senators recognise the concern of stakeholders including sex educators and health service providers that there exists a risk that genuine health information and sex education material may be misclassified as Class 2 material, which includes online pornography. Labor Senators also note that gender diverse and sexually diverse young people may 'face barriers to comprehensive sex education', and as a result may seek online spaces in search of understanding, connection and information.

1.36 However, genuine health information and sex education material does not constitute Class 2 material within the definition of the Online Safety Act, and continual, ongoing review from the eSafety Commissioner, as defined under the Act, will permit adjustment of how material is classified in practise.

Conclusion and Recommendations

1.37 Labor Senators do not agree with the committee report recommendation 1. Labor Senators do not believe it is suitable to further delay the implementation of the SMMA obligation. Social media platforms have been consulted extensively and have had more than 12 months to prepare for the SMMA obligation. Further, the Trial showed that while Age Assurance may not be

---

16 Collective Shout, *Submission 33*, p. 8.

17 Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, 13 October 2025, p. 59.

18 eSafety Commissioner, *Submission 8*, p. 12.

perfect and may require review and adjustment, it is an important tool in efforts to minimise harms caused by exposure to inappropriate content online.

1.38 Labor Senators agree with committee report recommendation 2 that the Australian Government should legislate a digital duty of care to make online platforms safer for all users, and we note that the government's consultation process on a digital duty of care has already commenced.[19]

1.39 Labor Senators note committee report recommendation 3 and observe that the SMMA obligation will significantly reduce the ability of social media companies to harvest and exploit the data of minors and young people.

1.40 Labor Senators agree with the intent of committee report recommendation 4 and note that the Australian Government has significantly increased funding for eSafety in Australia, including by funding eSafety awareness campaigns, supporting the eSafety Champions Network in schools, as well as providing toolkits and resources on the eSafety website. Additionally, the Albanese Government has invested $6 million in the Alannah and Madeline Foundation to improve online safety in schools.

Senator Varun Ghosh
Deputy Chair
Labor Senator for Western Australia

Senator Charlotte Walker
Member
Labor Senator for South Australia

[19] Dr Jennifer Duxbury, Director, Policy, Regulatory Affairs and Research, Digital Industry Group Inc, *Committee Hansard*, 24 September 2025, p. 2. See also Australian Human Rights Commission, *Submission 53*, p. 8.

Coalition Senators' dissenting report

Introduction

1.1 Coalition senators support measures which improve the online safety of Australian children and young people. The Coalition has consistently advocated for stronger protections, higher accountability for platforms and clear rules to minimise access to harmful content by minors.

1.2 Coalition senators do not support Recommendation 1 of the report by the Senate Environment and Communications References Committee (Committee) which proposes the Social Media Minimum Age (SMMA) obligation be delayed until 10 June 2026. This delay is not justified nor is it in the best interests of Australian families.

1.3 Coalition senators remain concerned about implementation failures relating to the SMMA laws for which the Albanese government and the Minister for Communications are directly responsible, but this does not justify delaying the commencement date which would cause further confusion and uncertainty.

Poor communications

1.4 The Albanese government has had more than 12 months since the passage of the SMMA legislation to prepare, communicate and coordinate the implementation of the social media ban for children aged under 16. The decision to launch a public awareness campaign on 14 October 2025, less than two months before the commencement date, represents a failure to plan by the Minister for Communications.

1.5 The Committee's report correctly raises concerns that young people have been left unprepared as there has not been an adequate education program rolled out to young people who will be cut off from their online communities.[1]

1.6 The Government must take responsibility for this failure to adequately communicate this very considerable change in the law which will detrimentally impact on many young people. Notwithstanding, this cannot be used as an excuse to delay measures to improve children's online safety.

1.7 The SMMA laws were designed with a twelve month lead-in period to enable platforms, schools, parents and regulators to prepare and a further six month delay creates additional risk at a time when Australian children are increasingly exposed to violent material, harmful content and predatory contact.

---

[1] See, Senate Environment and Communications References Committee, *Internet Search Engine Online Safety Code and under 16 social media ban*, October 2025, p. 50.

Digital ID

1.8 Coalition senators note that the Albanese government has repeatedly assured Australians that the SSMA obligations will not require them to use digital ID or government identification.

1.9 A fact sheet issued by the Minister for Communications' department states clearly that 'no Australian will be compelled to use government identification (including Digital ID) to prove their age online, and platforms must offer reasonable alternatives to users'.[2]

1.10 Public messaging has also reinforced this position. In a radio interview discussing claims the SMMA laws were, in effect, a Digital ID scheme, Prime Minister Albanese reiterated the Government's opposition against the use of a Digital ID.[3]

1.11 Evidence to the Committee demonstrated some platforms intend to rely on government identification when their initial, non-intrusive age-assurance methods are inconclusive.[4] Meta confirmed it uses government identification as a fallback – 'people are given the option of either a video selfie … or government ID'.[5] This is inconsistent with the Government's stated position and has contributed to community confusion.

1.12 The Committee also heard that the recommended 'waterfall approach' starting with the least intrusive age assurance method, and escalating only when necessary, is not being consistently implemented by platforms, despite being identified as best practice during the Age Assurance Technology Trial.[6]

1.13 Coalition senators remain concerned there is a gap between the Albanese government's assurances and the approaches proposed by some platforms. This risks undermining public trust. These issues require clear and immediate guidance, not a delay to the implementation of child safety measures already passed by the Parliament.

---

2 Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Social Media Minimum Age – Fact sheet*, p. 1.

3 The Hon Anthony Albanese MP, Prime Minister, 'Radio interview - Nova Sydney', *Transcript*, 10 November 2025. 'WIPFLI: Prime Minister, just quickly, a lot of the feedback, and we spoke to Anika Wells, our Communications Minister, about this also. A lot of the feedback has been, 'oh, this is the government's attempt to create a Digital ID so they can steal more information'. I see it over and over again. Anika Wells confirmed that's not the case. I think it would just help for the Australian people to also hear you confirm that's not the case, as you've said before. PRIME MINISTER: It is certainly not the case. This is about giving people power back to families.'

4 See, ARC Centre of Excellence for the Digital Child, AIIA & AATT confirming limitations of age estimation and META.

5 Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 28 October 2025, p. 8.

6 Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 28 October 2025, p. 2.

Privacy concerns

1.14 Privacy risks raised during evidence are real, but they stem from Australia's outdated privacy framework and the Albanese Government's failure to legislate long-promised reforms with some witnesses warning 'Australia's existing privacy framework has never been fit for purpose'.[7]

1.15 Coalition senators agree that privacy preserving methods should be prioritised by measures such as strengthening the Privacy Act, finalising Digital ID legislation and correcting Government guidance, not by suspending age protections designed to keep 15 year olds off platforms that host violent content, pornography and predatory contact.

Push to unregulated platforms

1.16 The Committee's report acknowledges the risk that banning social media access without proper management could drive young people toward even less safe platforms.

1.17 Coalition senators assert this risk exists now and delays will worsen the risk by keeping children on platforms with weak protections, and we must ensure platform compliance and Government preparedness, not shelve the commencement date.

Conclusion

1.18 Coalition senators support the intent of the SMMA legislation and stronger online safety regulations.

1.19 Coalition senators oppose Recommendation 1 and instead call on the Albanese government to fix its implementation failures, provide proper communication to families and ensure platforms meet their responsibilities under the law.

Senator the Hon Sarah Henderson
Member
Liberal Senator for Victoria

Senator Dean Smith
Member
Liberal Senator for Western Australia

[7] Mr John Pane, Chair, Electronic Frontiers Australia Inc., *Committee Hansard*, 13 October 2025, p. 44.

Appendix 1
Submissions and Additional Information

1 NSW Advocate for Children and Young People
2 Cybercy Pty Ltd
3 Alannah & Madeline Foundation
4 Qoria
5 ARACY
6 Digital Industry Group Inc.
7 Telecommunications Industry Ombudsman
8 eSafety Commissioner
9 Internet Association of Australia Ltd
10 ARC Centre of Excellence for the Digital Child
11 Australian Information Industry Association
12 Digital Rights Watch
13 UNICEF Australia
14 QUT Digital Media Research Centre
15 The Eros Association
16 X
17 Scarlet Alliance, Australian Sex Workers Association
18 Queensland Council for Civil Liberties
19 yourtown
20 ReachOut Australia
21 Hackeroos Pty Ltd
22 Dr Angie Simmons
23 Bloom-Ed
24 Australian Injecting and Illicit Drug Users League (AIVL)
25 Australian Child Rights Taskforce, ChildFund Australia and Dr Rys Farthing, University of Canberra
26 Away from Keyboard Inc.
27 Department of Infrastructure, Transport, Regional Development, Communications and the Arts
28 ANU Law Reform and Social Justice Research Hub
29 Nicolette Boele MP
30 Stand Up Now Australia
31 Aligned Council of Australia
32 Electronic Frontiers Australia Inc
33 Collective Shout
34 Mr Bronson Tohara
35 Mr. David Sharples
36 Mr Jason Moore
37 Dr Robyn Stephenson

38 Mr Arthur Wielgosz
39 Mr Joel Canham
40 Mr Timothy Gurowski
41 Mr Ashley Burke
42 Ms Ingrid Peter
43 Mr Mark Armstrong
44 Mrs Laura Robertson
45 Mr Greg Tannahill
46 Mr Gregory Atkins
47 Mr Ryan Ballinger
48 Mr James Steward
49 Mr Jack Davenport
50 Mr Geoffrey Stafford
51 Mr Elvis Sinosic
52 Dr Adam Burke
53 Australian Human Rights Commission
54 Age Verification Providers Association
55 Mr Steve Forkin
56 John Krylyszyn
57 Adam Kachwalla
58 Name Withheld
59 Confidential
60 Name Withheld
61 Name Withheld
62 Name Withheld
63 Name Withheld
64 Name Withheld
65 Free Speech Union of Australia
- Attachment 1

66 Name Withheld
67 Name Withheld
68 Name Withheld
69 Name Withheld
70 Name Withheld
71 Name Withheld
72 Name Withheld
73 Name Withheld
74 Name Withheld
75 Name Withheld
76 Name Withheld
77 Name Withheld
78 Name Withheld
79 Name Withheld

80 Name Withheld
81 Name Withheld
82 Name Withheld
83 Name Withheld
84 Name Withheld
85 Name Withheld
86 Name Withheld
87 Name Withheld
88 Name Withheld
90 Name Withheld
91 Name Withheld
92 Name Withheld
93 Name Withheld
94 Name Withheld
95 Name Withheld
96 Name Withheld
97 Confidential
98 Confidential
99 Confidential
100 Confidential
101 Confidential

Additional Information

1 Centre for Multicultural Youth - 001 additional information received on 5 November 2025.
2 15 Sample Submissions from Campaign - 26 November 2025.
3 Mr Henry Turnbull, Snap Inc., Correspondence clarifying evidence given at a public hearing on 28 October 2025 (received 28 October 2025).

Answer to Question on Notice

1 Answer to a question on notice asked by Senator Henderson at a public hearing on 13.10.2025 (received 28.10.2025)
2 Answer to a question on notice asked by Senator Henderson at a public hearing on 13.10.2025 (received 28.10.2025)
3 eSafety Commissioner - 001: Answer to a questions on notice asked by Senator Henderson, Senator Pocock and Senator Shoebridge at a public hearing on 13.10.2025 (received)
4 Answer to a question on notice asked by Senator Henderson at a public hearing on 13.10.2025 (received 29 October 2025)
5 Answer to a question on notice asked at a public hearing on 28.10.2025 (received 10 November 2025)

6 Answers to questions on notice asked by Senators Hanson-Young, D. Pocock and D. Smith at a committee hearing on 28 October 2025 (received 11 November 2025).
7 Answers to questions on notice asked by Senators D. Pocock and Henderson at a committee hearing on 28 October 2025 (received 13 November 2025).
8 Answers to written questions on notice asked by Senator D. Pocock asked on 6 November 2025 (received 18 November 2025)
9 Answer to a question on notice asked at a public hearing on 28.10.2025 (18.11.2025 received)
10 Answer to a question on notice asked at a public hearing on 28.10.2025 (27.10.2025 received)
11 Answer to a question on notice asked at a public hearing on 13.10.2025 (22.10.2025 received)
12 Answer to a question on notice asked by Senator Dean Smith at a public hearing on 13.10.2025 (22.10.2025 received)
13 Answer to a question on notice asked by Senator Dean Smith at a public hearing on 13.10.2025 (27.10.2025 received)
14 Answer to a question on notice asked by Senator Dean Smith at a public hearing on 13.10.2025 (27.10.2025 received)
15 Answer to a question on notice asked at a public hearing on 13.10.2025 (27.10.2025 received)
16 Answer to a question on notice asked by Senator Hanson-Young at a public hearing on 13.10.2025 (27.10.2025 received)
17 Answer to a question on notice asked by Senator Dean Smith at a public hearing on 13.10.2025 (27.10.2025 received)
18 Answers from several organisations to written questions on notice asked by Senator D. Pocock on 11 November 2025 (received between 11 – 18 November 2025).
19 Answer to a question on notice asked by Senator D. Smith at a committee hearing on 13 October 2025 (received 24 November 2025).
20 Answer to a question on notice asked by Senator D. Smith at a committee hearing on 13 October 2025 (received 24 November 2025).
21 Answers to written questions on notice asked by Senator D. Pocock on 6 November 2025 (received 25 November 2025).

Tabled Documents

1 Document tabled by eSafety Commissioner at a public hearing on 13.10.2025
2 Document tabled by eSafety Commissioner at a public hearing on 13.10.2025
3 Document tabled by eSafety Commissioner at a public hearing on 13.10.2025
4 Document tabled by eSafety Commissioner at a public hearing on 13.10.2025
5 Document tabled by eSafety Commissioner at a public hearing on 13.10.2025

Appendix 2
Public hearings and witnesses

Wednesday 24 September 2025
Parliament House, Committee Room 2S3
Canberra

Digital Industry Group inc

- Dr Jennifer Duxbury, Director Policy, Regulatory Affairs and Research
- Ms Sunita Bose, Managing Director

Monday 13 October 2025
Committee Room 2S3
Parliament House
Canberra

YouTube

- Ms Rachel Lord, Senior Manager , Government Affairs and Public Policy , YouTube AUNZ

Google

- Ms Kate Charlet, Director for Privacy, Safety and Security
- Ms Stefanee Lovett, Director of Government Affairs and Public Policy

Microsoft

- Ms Elizabeth Thomas, Senior Director of Public Policy, Digital Safety
- Mr Michael Golebiewski, Principal Product Manager
- Ms Elizabeth Thomas, Senior Director of Public Policy, Digital Safety

Yahoo

- Mr Logan Smith

Australia Child Rights Taskforce

- Mr James McDougall, Co-Chair

Project Rockit

- Ms Lucy Thomas OAM, Chief Executive Officer
- Ms Caitlin Blanch, Member of National Youth Collective

Headspace National Youth Mental Health Foundation

- Ms Nicola Palfrey, Head of Clinical Practice
- Ms Caroline Thain, Manager of Clinical Advice and Governance

6 News

- Mr Leo Puglisi, Founder and Chief Anchor

Youth Affairs Council of Victoria

- Ms Laura Pettenuzzo, Executive Assistant to Head of Youth Disability Advocacy Service
- Ms Lauren Frost, Advocacy Manager

Centre for Multicultural Youth

- Ms Harini Kasthuriarachchi, Policy Officer
- Ms Edmee Kenny, Senior Policy Advisor

Digital Rights Watch

- Ms Elizabeth O'Shea, Chair

Electronic Frontiers Australia Inc.

- Mr John Pane, Chair
- Mr Andrew Scott, Secretary

CitizenGo

- Mr Brian Marlow, Campaigner

Qoria

- Mr Tim Levy, Founder, Managing Director

The Age Verification Providers Association

- Mr Iain Corby, Executive Director

Tech Policy Design Institute

- Ms Zoe Hawkins, Co-Founder & Deputy Executive Director
- Ms Johanna Weaver, Co-Founder and Executive Director

Dr Rys Farthing, Private capacity

Office of the eSafety Commissioner

- Ms Julie Inman Grant, Commissioner
- Mr Richard Flemming, General Counsel
- Ms Heidi Snell, A/g General Manager, Regulatory Operations
- Ms Kelly Tallon, Executive Manager, Industry Compliance & Enforcement
- Ms Chole Bennett, Manager – Industry Codes

Department of Infrastructure, Transport, Regional Development, Communications and the Arts

- Ms Anthea Fell, Assistant Secretary, Online Safety Branch
- Mr James Chisholm, Deputy Secretary, Communications and Media Group
- Mr Nolan Noeng, Director, Online Safety Branch

- Ms Sarah Vandenbroek, First Assistant Secretary, Digital Platforms, Safety and Classification Division

Office of the Australian Information Commissioner

- Ms Carly Kind, Privacy Commissioner
- Ms Carly Kind, Privacy Commissioner

Tuesday 28 October 2025

Committee Room 2S3, Parliament House
Canberra

Meta

- Ms Mia Garlick, Regional Director Of Policy

Snap Inc.

- Ms Jennifer Stout, Senior Vice President, Global Policy and Platform Operations

TikTok

- Ms Ella Woods-Joyce, Public Policy Lead, Content and Safety