The Senate

Environment and Communications Legislation Committee

Online Safety Amendment (Digital Duty of Care) Bill 2026

November 2026

© Commonwealth of Australia 2026

ISBN 978-1-86523-024-5 (Printed version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International License.



The details of this licence are available on the Creative Commons website: https://creativecommons.org/licenses/by-nc-nd/4.0/.

Printed by Printed by the Senate Printing Unit, Parliament House, Canberra

Members

Chair

Senator Varun Ghosh	ALP, WA

Deputy Chair

Senator Sarah Hanson-Young	AG, SA

Members

Senator Michelle Ananda-Rajah	ALP, VIC
Senator the Hon Carol Brown	ALP, TAS
Senator the Hon Sarah Henderson	LP, VIC
Senator Dean Smith	LP, WA

Substitute Member

Senator Tammy Tyrrell	ALP, TAS

(Substitute for Senator Ananda-Rajah on 10 November 2026)

Participating Members

Senator David Pocock	IND, ACT
Senator Tyron Whitten	ON, WA

Secretariat

Tas Larnach, Committee Secretary
Azrianne Rahman, Principal Research Officer
Monika Sheppard, Principal Research Officer
Kelly Yoon, Senior Research Officer
Elizabeth Hickey, A/g Research Officer
Hanna Duka, 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

Members ..... **iii**

Abbreviations ..... **ix**

Chapter 1—Introduction **1**

Conduct of the inquiry and acknowledgement 1

Structure of the report 2

Note on references 2

Purpose and context of the bill 2

The independent review of the Online Safety Act 3

Recent changes to Australia's online safety framework 3

Consultation on the bill 4

Amendments to the bill in the House of Representatives 5

Key proposals and provisions 5

Digital Duty of Care 5

Protection from seriously harmful material and conduct 7

Protections for children 8

Excluded material 9

Risk assessments 9

User empowerment tools 10

Age assurance and access control measures 11

Complaint and dispute processes 12

Transparency measures 12

Compliance and investigative powers 12

Research and data access 13

Data access schemes 13

Sock puppet identities 14

Take down notices 14

Removal notices for fake nude material 14

Removal notices for cyberbullying and adult cyber-abuse material 15

Link deletion notices 15

Increased penalties 16

Commencement 16
Examination by other parliamentary committees 17
Chapter 2—Digital Duty of Care and platform obligations 19
Support for a stronger regulatory approach 20
Digital Duty of Care 24
Clarity of the standard in proposed section 26 24
Matters to be taken into account under proposed section 26A 27
Privacy 27
Cost 28
Online services captured by the Digital Duty of Care 29
Harm definitions 32
Seriously harmful material and conduct 32
Material and conduct that is harmful to children 37
Proposed paragraph 25E(1)(c) 39
Proposed paragraph 25E(1)(d) 40
Proposed paragraph 25E(1)(f) 40
Departmental response 41
Excluded material 41
Public health and safety material and harm reduction material 42
Public interest material 43
Religious material 45
Departmental response 46
Design features with negative behavioural impacts 46
Expanded protections against harmful design features 46
Certain design features deemed to have negative behavioural impacts 48
Differential standards for children and adults 49
Risk assessments 50
Risks to be assessed 50
Strengthening the effectiveness of risk assessments 51
Concerns regarding regulatory burden 53
User empowerment tools 55
Potential implications for online service providers 57

Ministerial powers in relation to user empowerment tools 58
Age assurance and access control measures 59
Scope and proportionality of the measures 60
Privacy and data security implications 61
Potential impacts on access to lawful online services 62
Next chapter 62
Chapter 3—Regulatory oversight and enforcement 63
Compliance and investigative powers of the eSafety Commissioner 63
Removal notices for fake nude material 64
Research and data access 66
Data access schemes 66
Scope of researcher data access 67
Industry concerns 68
Sock puppet identities 69
Support for sock puppet provisions 69
The importance of safeguards 71
Complaint and dispute processes 72
External dispute resolution 74
Penalties and enforcement 75
Civil penalties 75
Calls for a private right of action 77
Committee view 80
Coalition Senators' Dissenting Report 85
Australian Greens' Additional Comments 107
Appendix 1—Submissions and additional information 111
Appendix 2—Public hearings and witnesses 121

Abbreviations

ACS	Australian Computer Society
ADM+S	ARC Centre of Excellence for Automated Decision-Making and Society
AHRC	Australian Human Rights Commission
AJA	Australian Jewish Association
ASU	Australian Services Union
BCA	The Business Council of Australia
bill	Online Safety Amendment (Digital Duty of Care) Bill 2026
committee	Environment and Communications Legislation Committee
COSBOA	Council of Small Business Organisations Australia
department	Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts
DIGI	Digital Industry Group Inc
Duty	Digital Duty of Care
EM	Explanatory Memorandum
FSU	Free Speech Union of Australia
Human Rights Committee	Parliamentary Joint Committee on Human Rights
ICS	internet carriage services
IGEA	Interactive Games & Entertainment Association
Minister	Minister for Communications

NATSIWA	National Aboriginal and Torres Strait Islander Women's Alliance
NFAW	National Foundation for Australian Women
OAIC	Office of the Australian Information Commissioner
Online Safety Act	*Online Safety Act 2021*
SANDAS	South Australian Network of Drug and Alcohol Services
Scrutiny of Bills Committee	Senate Standing Committee for the Scrutiny of Bills
TIO	Telecommunications Industry Ombudsman

Chapter 1
Introduction

1.1 On 15 October 2026, the Senate referred the provisions of the Online Safety Amendment (Digital Duty of Care) Bill 2026 (the bill) to the Environment and Communications Legislation Committee (the committee) for inquiry and report by 20 November 2026.[1]

1.2 The bill would amend the *Online Safety Act 2021* (Online Safety Act) to introduce a Digital Duty of Care aimed at addressing serious online harms and to implement a range of measures to strengthen Australia's online safety framework.[2]

Conduct of the inquiry and acknowledgement

1.3 In accordance with its usual practice, the committee advertised the inquiry on its website and called for submissions by 30 October 2026. The committee received 182 submissions, which are listed at Appendix 1.

1.4 The committee also received comments from individuals through various campaigns. A sample of these individual comments is available on the committee's website.

1.5 The committee held public hearings in Canberra on 9 and 10 November 2026. A list of the witnesses who appeared at the hearings is included at Appendix 2.

1.6 The committee thanks those individuals and organisations who contributed to the inquiry. The committee is particularly grateful to those who shared deeply personal accounts of the impacts and harms they and their loved ones have experienced online.

---

1 *Journals of the Senate*, No. 76, 15 October 2026, pp. 2768–2769.

2 Online Safety Amendment (Digital Duty of Care) Bill 2026 (the bill), Explanatory Memorandum (EM), p. 2.

Structure of the report

1.7 This report comprises three chapters:

- Chapter 1 provides contextual background to the bill, outlines key proposals and provisions, and notes any consideration of the bill undertaken by other parliamentary committees.
- Chapter 2 examines the bill's proposed duties and mechanisms directed to the identification, prevention and minimisation of online harms, including the Digital Duty of Care, protections against harmful design features, and requirements relating to risk assessments, user empowerment tools, and age assurance and access control.
- Chapter 3 explores issues relating to the proposed regulatory oversight and enforcement framework, including the powers of the eSafety Commissioner, the research and data access framework, complaint and dispute processes, and penalties and enforcement provisions. It also sets out the committee's views and recommendations.

Note on references

1.8 In this report, references to the *Committee Hansard* are to the proof (that is, uncorrected) transcript. Page numbers may vary between the proof and the official transcript.

Purpose and context of the bill

1.9 In her second reading speech on the bill, the Minister for Communications (the Minister), the Hon Anika Wells MP, explained that the bill's aims are to: provide a safe online environment for all Australians; give Australians choice about the content they view on social media; and protect children from harmful content. The Minister noted that the bill addresses the findings of an independent statutory review of the Online Safety Act.[3]

1.10 On 27 October 2026, the Prime Minister, the Hon Anthony Albanese MP, described some of the harms, stating:

> There is a growing body of research pointing to the reality that as a result of the deliberate design of its algorithmic features, social media is changing our society in harmful ways.
>
> Turbocharging anger to the detriment of our social cohesion and our democracy. It is promoting misogyny. Building an aggressive and sometimes frightening manosphere and driving a wedge between men and women, leading to an increase in gender based violence.[4]

---

3 The Hon Anika Wells MP, Minister for Communications, the bill, *Second Reading Speech*, pp. 6–7.

4 The Hon Anthony Albanese MP, Prime Minister, Speech, Digital duty of care, 27 October 2026.

The independent review of the Online Safety Act

1.11 On 31 October 2024, Ms Delia Rickard PSM provided the final report of her review of the Online Safety Act to the Australian Government. The Review found that Australia's current laws and regulatory settings are inadequate to address the scale and evolving nature of online harms and highlighted the need for a more systemic and preventative approach.[5]

1.12 The Review made 67 wide-ranging recommendations, chief among them the implementation of an overarching duty of care that would require online service providers to take reasonable steps to address and prevent foreseeable harms on their services.[6]

1.13 The Australian Government's response, published in April 2026, expressed the Government's commitment to legislating a duty of care as an immediate priority and to implement or further consider 64 of the 67 recommendations.[7] These include the Review's recommendations around providing the eSafety Commissioner with stronger enforcement options and additional powers in relation to investigations.[8]

Recent changes to Australia's online safety framework

1.14 The *Online Safety Amendment (Social Media Minimum Age) Act 2024* established a social media minimum age framework within the Online Safety Act. This framework requires providers of age-restricted social media platforms to take reasonable steps to prevent Australians under 16 years of age from holding accounts.

1.15 The enactment of the *Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Act 2026* in September 2026 strengthened the eSafety Commissioner's information-gathering powers and the maximum civil penalties for non-compliance with the social media minimum age framework.

---

5 Delia Rickard PSM, *Report of the Statutory Review of the Online Safety Act 2021*, October 2024, pp. 12, 39–41 and 136.

6 Delia Rickard PSM, *Report of the Statutory Review of the Online Safety Act 2021*, October 2024, pp. 20–25 and 136.

7 Australian Government, *Government Response to the Independent Review of the Online Safety Act 2021*, April 2026, p. 2.

8 Australian Government, *Government Response to the Independent Review of the Online Safety Act 2021*, April 2026, pp. 10 and 12–13.

1.16 The bill's Explanatory Memorandum notes that the bill would substantially build on the protections provided by the social media minimum age framework:

> The *Online Safety Amendment (Social Media Minimum Age) Act 2024* was a major step forward in protecting children and young people online. However, more needs to be done, particularly in respect of services not captured and to protect social media users over the age of 16. The [Digital] Duty [of Care] is complementary and will reinforce the growing expectation that platforms have a responsibility to protect the safety of their users and to address harm before it has occurred.[9]

1.17 The Minister stated that the bill represents the Government 'taking the next step following its world leading social media age ban to ensure Australians have more choice online'.[10]

1.18 The introduction of a digital duty of care is a substantive step toward a more holistic approach toward ensuring online safety.

Consultation on the bill

1.19 As set out in the Explanatory Memorandum, the bill was developed following public and targeted stakeholder consultation undertaken by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department) since 2024. This includes meetings with a range of stakeholders between late 2025 and early 2026 during the initial stages of designing the Digital Duty of Care model; further consultation throughout May and June 2026 following the release of an issues paper; and consultation on the exposure draft of the bill in September 2026.[11]

---

9 The bill, EM, p. 4.

10 The Hon Anika Wells MP, Minister for Communications, and The Hon Anthony Albanese MP, Prime Minister of Australia, 'My Feed, My Way', *Media Release*, 8 September 2026, https://minister.infrastructure.gov.au/wells/media-release/my-feed-my-way (accessed 20 October 2026).

11 The bill, EM, p. 5. See also, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department), *Submission 130*, pp. 3–4; The department, answer to question on notice SQ26-000594, Senate Environment and Communications Budget Estimates 2026–27, 27 May 2026 (received 14 October 2026); The department, *A Digital Duty of Care for Australia—Developing a duty of care framework for online services used by Australians*, 26 May 2026, https://www.infrastructure.gov.au/department/media/publications/digital-duty-care-australia-developing-duty-care-framework-online-services-used-australians (accessed 20 October 2026); The department, *Exposure Draft—Online Safety Amendment (Digital Duty of Care) Bill 2026*, 8 September 2026, https://www.infrastructure.gov.au/department/media/publications/exposure-draft-online-safety-amendment-digital-duty-care-bill-2026 (accessed 20 October 2026).

Amendments to the bill in the House of Representatives

1.20 On 28 October 2026, the bill was agreed to by the House of Representatives, with 15 Government amendments and eight crossbench amendments.[12]

1.21 The Government amendments were intended to 'make technical corrections and changes and provide additional clarity for provisions that exclude material from the scope of harms captured by the digital duty of care'.[13]

1.22 Crossbench amendments were made to the definition of material and conduct that is harmful to children (proposed section 25E) and the requirements relating to user empowerment tools (proposed Division 4 of Part 2).[14]

1.23 Amendments to the bill are discussed further below.

Key proposals and provisions

1.24 The bill comprises three schedules that propose amendments to the Online Safety Act and several other Commonwealth Acts,[15] with the key proposals and provisions set out in Schedules 1 and 2.

Digital Duty of Care

1.25 The bill's central proposal is the introduction of the Digital Duty of Care (Duty). The bill's Explanatory Memorandum states that the proposed Duty 'replaces the existing Basic Online Safety Expectations and Online Safety Codes and Standards framework with a single, clear and enforceable duty of care'.[16]

---

12 *House of Representatives Votes and Proceedings*, No. 93, 28 October 2026, pp. 1181–1186.

13 The bill, Supplementary Explanatory Memorandum, p. 3.

14 Amendments as circulated in the name of the Member for Curtin.

15 The bill proposes amendments to the *Age Discrimination Act 2004*, *Privacy Act 1988*, *Broadcasting Services Act 1992*, *Criminal Code Act 1995* and *Interactive Gambling Act 2001*.

16 The bill, EM, pp. 13–14.

1.26 The proposed Duty is an overarching obligation on persons responsible for online services[17] (hereafter referred to as 'online service providers') to take appropriate action to ensure a safe online environment for all Australians.[18] A 'safe online environment'[19] is defined as an online environment in which:

- persons in Australia are protected from seriously harmful material and conduct;[20] and
- children in Australia are protected from:
  - material and conduct that is harmful to children;[21] and
  - harms associated with access or exposure to design features of online services.

1.27 The bill recognises that the harm caused in online environments is not limited to children and that there are risks posed to all Australians.

1.28 A safe online environment is also defined as one in which children under 16 years of age do not have access to, and are not exposed to, design features of a social media service that have negative behavioural impacts.[22]

1.29 The bill states that taking appropriate action to ensure a safe online environment includes taking effective measures to mitigate risks identified in risk assessments conducted in accordance with proposed section 27 (discussed further below).[23] According to the Explanatory Memorandum:

> Individual instances of harmful material and conduct on a service will not necessarily be a breach of the digital duty of care. The relevant question is whether the provider has identified reasonably foreseeable risks and implemented and maintained effective systems and processes to mitigate the risk of the harm occurring on its platform.[24]

---

17 Proposed section 25B sets out the definition of an online service and a person responsible for an online service. The provision would empower the Minister, by legislative instrument, to exempt an online service, or a class of online services, from the operation of one or more provisions of proposed Part 2 of the Act, if the Minister is satisfied that the service, or class of services, pose little risk to users in Australia.

18 See Schedule 2 of the bill. The Digital Duty of Care is set out in proposed section 26.

19 Proposed section 25C sets out the definition of a safe online environment.

20 Proposed section 25D sets out the definition of seriously harmful material or conduct.

21 Proposed section 25E sets out the definition of material and conduct that is harmful to children.

22 Proposed section 25G provides a list of design features of an online service that are taken to have negative behavioural impacts.

23 Proposed subsection 26(1).

24 The bill, EM, p. 72.

1.30 Additionally, for the purposes of assessing compliance with the Duty, matters to be taken into account include the nature of the material, the extent to which exposure to the material would be inconsistent with a safe online environment and whether the action or measures are or would be proportionate to the level of risk. The cost of the action or measures must not be taken into account.[25]

1.31 Lawful communications occurring in private solely between consenting adults would be exempted from the application of the Duty.[26]

1.32 A range of graduated enforcement options would be available to the eSafety Commissioner to manage compliance with the Duty, including formal warnings, remedial directions, infringement notices, and applying to the courts for civil penalty orders or injunctions.[27] Failure to comply with the Duty could attract a maximum civil penalty of 60 000 units ($21.84 million).[28] The Explanatory Memorandum states that:

> This penalty amount brings the penalty in line with those under the *Competition and Consumer Act 2010* and reflects the significant revenue base and resources of the multinational platforms captured by the Duty. A penalty amount of 60,000 units also reflects the severity and scope of systemic harms that an unsafe online environment poses to the broader Australian community and wellbeing of its people.[29]

Protection from seriously harmful material and conduct

1.33 The Duty would require online service providers to take appropriate action to ensure an online environment in which all persons in Australia, regardless of age, are protected from seriously harmful material and conduct.[30] This would include, for example: material or conduct that depicts, encourages, promotes, incites or instructs child sexual exploitation or child sexual abuse; fake nude material created without consent; and material or conduct that encourages, promotes, incites or instructs gender-based violence.[31]

---

25 Proposed section 26A.

26 Proposed section 26B.

27 The bill, EM, p. 69.

28 Proposed section 26C. See, Parliamentary Library, Bills Digest No. 26, 2026–27, 23 October 2026, p. 13.

29 The bill, EM, p. 68.

30 The bill, EM, p. 53.

31 Proposed section 25D.

1.34 The definition of seriously harmful material or conduct in proposed section 25D is:

> … provided as an exhaustive list which is closely aligned with material and conduct that would likely be considered Class 1A material (content that is or would be refused classification in Australia) under the online content scheme in Part 9 of the Act, or is illegal under the Commonwealth *Criminal Code Act 1995*.[32]

1.35 However, as matters stand, the bill does not expressly include aspects of group-directed hate nor specifically cover those situations where online abuse is directed against groups based on protected characteristics. Submitters' views on this issue are discussed in Chapter 2.

Protections for children

Material and conduct that is harmful to children

1.36 The Duty would require online service providers to take appropriate action to ensure an online environment in which children in Australia are protected from material and conduct that is harmful to children. This would include, for example: pornography, abuse, harassment or bullying, and material or conduct that encourages, promotes or instructs disordered eating.[33]

1.37 A crossbench amendment agreed to by the House of Representatives inserted into the list of material and conduct harmful to children: 'material or conduct that simulates emotional intimacy and encourages or fosters a child's dependence on it in place of human relationships'.[34]

1.38 The list of harmful material and conduct in proposed section 25E is not exhaustive, and online service providers would be required to assess all potential risks to children through their services.[35]

Design features of a social media service that have negative behavioural impacts

1.39 Under the Duty, a provider of a social media service would be required to take appropriate action to ensure an online environment in which children in Australia under the age of 16 do not have access to, and are not exposed to, design features (such as recommender features and logged-in features) that have negative behavioural impacts. The Minister would be empowered to determine, by legislative instrument, that a design feature of an online service has negative behavioural impacts.[36]

---

32 The bill, EM, p. 54.

33 Proposed section 25E.

34 Amendments as circulated in the name of the Member for Curtin.

35 The bill, EM, p. 59.

36 Proposed section 25G.

1.40 According to the Explanatory Memorandum:

> Design features can be particularly harmful for children, especially addictive design elements, tools which facilitate communication with strangers, community driven reward systems, and algorithmic recommender systems that proliferate harmful material, or are used to amplify bullying and harassment.
>
> … There is … credible evidence that children and adolescents are more vulnerable than adults to engaging in addictive, disordered or problematic use of social media, artificial intelligence and online gaming.[37]

Excluded material

1.41 The bill provides that certain material is excluded from the definition of seriously harmful material and conduct (proposed section 25D) and material and conduct that is harmful to children (proposed section 25E).[38] This provision is:

> … intended to exempt lawful and legitimate communications related to matters such as news reporting, professionally produced entertainment, or the public interest, concerning the harms captured under sections 25D and 25E.[39]

1.42 Government amendments agreed to by the House of Representatives added to the list of excluded material media content provided by on-demand program services.[40]

Risk assessments

1.43 For the purposes of complying with the Duty, online service providers must ensure that written risk assessments are conducted at least annually, or at shorter intervals determined by the eSafety Commissioner, and before making any significant changes to the service that could introduce new or additional risks. Risk assessments must be made available to the eSafety Commissioner within 30 days upon request.[41]

---

37 The bill, EM, p. 53. See also, pp. 62–67.

38 Proposed section 25F.

39 The bill, EM, p. 59.

40 The bill, Supplementary Explanatory Memorandum, pp. 8–9.

41 Proposed section 27.

1.44 Risk assessments must identify reasonably foreseeable risks and the design features and other systems or processes that give rise to those risks; assess the likelihood and potential severity of those risks; and document the measures implemented to mitigate those risks and an assessment of the expected effectiveness of those measures.[42] In many cases, the design features that produce higher risks are likely to be known to online service providers or reasonably discernible.

1.45 The Commissioner would be empowered to determine, by legislative instrument, additional requirements relating to risk assessments.[43]

1.46 The Explanatory Memorandum notes that risk assessments are 'integral to the function of the Duty' and that:

> The risk assessment process is intended to ensure that online service providers are taking proactive and ongoing action to identify and assess risks … [and] provides an evidence base for the Commissioner to assess whether an entity has met its obligations under the Duty.[44]

User empowerment tools

1.47 Proposed subsection 27A(1) provides that the Minister may, by legislative instrument, require a specified online service to provide users in Australia with a specified user empowerment tool. The Minister may also prescribe requirements for, and in relation to, the tool. The bill defines a 'user empowerment tool' as a tool that 'allows a user of an online service to manage the way design features of the service operate for the user'.[45]

1.48 Before specifying a user empowerment tool by legislative instrument, the Minister must be satisfied that the tool is necessary to protect users in Australia from harms associated with access or exposure to a design feature of the service.[46]

---

42 Proposed section 27.

43 Proposed section 27.

44 The bill, EM, p. 70.

45 Proposed section 27A.

46 Proposed section 27A.

1.49 Upon the bill's introduction to the Parliament, the Australian Government released an exposure draft of the legislative instrument proposed to be made under subsection 27A(1)—the Online Safety (User Empowerment Tools) Determination 2026—for public consultation. The Determination is intended to give effect to the Government's My Feed, My Way initiative which would 'give Australians control over their social media algorithms'[47] by 'requir[ing] social media service providers to offer Australian logged-in users with a choice of a following-only content feed'.[48]

1.50 A crossbench amendment agreed to by the House of Representatives inserted proposed section 27BA which would require user empowerment tools to be accessible, easy to use, prominently available, functional, and available on an ongoing basis. It also states that use of the tool must not affect the general functionality of the service or reduce or impair user experience.[49]

Age assurance and access control measures

1.51 Proposed section 27D provides that where there is a reasonably foreseeable risk that a child could access, or be exposed to, pornography or material that describes or depicts specific fetish practices or fantasies, through an online service, the service provider must, where technically feasible and reasonably practicable, implement a choice of appropriate age assurance measures and implement access control measures.[50] The Explanatory Memorandum notes that preventing children from accessing such material would be 'consistent with the broader risk-based architecture of the Duty'.[51]

---

47 The Hon Anika Wells MP, Minister for Communications, and the Hon Anthony Albanese MP, Prime Minister of Australia, 'My Feed, My Way', *Media Release*, 8 September 2026, https://minister.infrastructure.gov.au/wells/media-release/my-feed-my-way (accessed 20 October 2026).

48 The department, *Choice of feeds on social media*, https://www.infrastructure.gov.au/have-your-say/choice-feeds-social-media (accessed 23 October 2026).

49 Amendments as circulated in the name of the Member for Curtin.

50 Proposed section 27D. Item 3 of Schedule 2 to the bill would insert definitions of 'age assurance measure' and 'access control measure' into the *Online Safety Act 2021* (Online Safety Act).

51 The bill, EM, p. 76.

Complaint and dispute processes

1.52 Proposed section 27G provides that a person responsible for a 'prescribed online service' must have complaint and dispute processes available equally to all individuals in Australia. The eSafety Commissioner may, by legislative instrument, designate that an online service falling within a particular class of services is a 'prescribed online service' and may determine requirements in relation to complaint and dispute processes.[52]

1.53 The Explanatory Memorandum clarifies that:

> By ensuring that all Australians have equal access to complaint and dispute processes, individuals who are not users of the service but have had content about them shared on the platform, such as deepfakes or cyberbullying material or other matters in breach of a platform's terms of service, can contact the service provider and seek remedy.[53]

Transparency measures

1.54 The bill proposes to insert a new Part 12A into the Online Safety Act to set out measures aimed at promoting transparency. The bill would empower the eSafety Commissioner to:

- require an online service provider to prepare and give the Commissioner transparency reports about the safety of the online service for Australians (proposed section 192B);[54] and
- require an online service provider to publish information about operations or activities relating to the online safety of users of the service in Australia (proposed section 192L).[55]

Compliance and investigative powers

1.55 The bill would insert a new Division 2 into Part 13 of the Online Safety Act which sets out the eSafety Commissioner's information-gathering powers. The new Division would replace Part 14 of the Act which currently sets out the Commissioner's investigative powers.[56]

---

52 Proposed section 27G.

53 The bill, EM, p. 78.

54 See proposed Division 2 of Part 12A for provisions related to transparency reports.

55 See proposed Division 3 of Part 12A for provisions related to information publication requirements.

56 Parliamentary Library, Bills Digest No. 26, 2026–27, 23 October 2026, p. 17.

1.56 The proposed Division would empower the Commissioner to require persons to give information or evidence, produce documents or answer questions that are relevant to certain investigations or to compliance with, or possible contraventions of, the Online Safety Act.[57] The Explanatory Memorandum notes that these powers are intended 'to support the effective administration of the Duty' and are 'based on similar provisions in the *Competition and Consumer Act 2010*'.[58]

Research and data access

1.57 The bill would insert a new Part 14 into the Online Safety Act to provide for a research and data access regime.

Data access schemes

1.58 Under the regime, the Minister would be empowered to make legislative rules (data access rules) requiring online service providers to give approved researchers access to data for the purposes of, or in connection with, undertaking online safety related research. In making the data access rules, the Minister must be satisfied that 'the access to data provided by the scheme would be reasonable in all of the circumstances'.[59]

1.59 An 'approved researcher' would be a person employed by an Australian university and designated as an approved researcher under the legislative rules, while 'online safety related research' would cover research that is relevant to the online safety of users of online services in Australia, approved by a human research ethics committee, and of a kind prescribed by the legislative rules to be in the public interest.[60] The Explanatory Memorandum states that by targeting university researchers, the bill would 'limit access to potentially sensitive data to suitably qualified researchers undertaking public interest research under appropriate safeguards'.[61]

---

57 Proposed Division 2 of Part 13.

58 The bill, EM, p. 92.

59 Proposed section 205C.

60 Proposed section 205B. The Minister would be empowered to make legislative rules specifying additional requirements that apply to approved researchers and online safety related research.

61 The bill, EM, p. 95.

Sock puppet identities

1.60 The bill would allow sock puppet identities (false or fictitious identities)[62] to be assumed by approved researchers for the purposes of undertaking online safety research[63] and by the eSafety Commissioner for the purposes of performing its functions or exercising its powers under the Online Safety Act.[64] Proposed section 205K sets out a list of authorised activities that may be undertaken using sock puppet identities, including creating and using an account to access an online service; observing, downloading or making a record of any material accessed using an online service; and testing features of an online service.[65]

1.61 The eSafety Commissioner would be required to publish an annual statement setting out its priorities and strategies for the year in relation to sock puppet activities and summarising, in general terms, its sock puppet activities during the previous year.[66] These statements are 'intended to provide public facing transparency over the use of the eSafety Commissioner's fictitious accounts'.[67]

Take down notices

1.62 The bill contains several measures in Schedule 1 aimed at 'strengthen[ing] protections against technology-facilitated abuse and the effectiveness of the complaints schemes under the [Online Safety] Act'.[68]

Removal notices for fake nude material

1.63 The bill would insert a new Part 6A into the Online Safety Act to empower the eSafety Commissioner to require providers of app distribution services or internet search engine services to remove apps or websites for end-users in Australia if those apps or websites are predominantly designed, or being used, for generating fake nude material.[69]

---

62 The definition of 'sock puppet identity' is set out in proposed section 205G.

63 Proposed section 205H.

64 Proposed section 205J.

65 Proposed section 205K.

66 Proposed section 205M.

67 The bill, EM, p. 98.

68 The bill, EM, p. 6.

69 Proposed Part 6A. The power to issue removal notices is contained in proposed section 86B. Government amendments 1 and 2 to the bill, agreed by the House of Representatives, replaced 'and' with 'or' to clarify that a removal notice could be issued under section 86B if the Commissioner is satisfied that the app or website either: was designed for the predominant purpose of generating fake nude material, or is predominantly used by end-users to generate fake nude material: The bill, Supplementary Explanatory Memorandum, p. 8.

Removal notices for cyberbullying and adult cyber-abuse material

1.64 The bill would amend the Online Safety Act to allow the eSafety Commissioner to issue removal notices to service providers in relation to cyberbullying and adult cyber-abuse material without requiring a prior complaint to have been made to the service provider. The Commissioner would be able to waive the requirement for a prior complaint if satisfied that the service does not have a functional or accessible complaints mechanism or that requiring the complaint would create a reasonably foreseeable risk of further harm.[70]

1.65 The bill would also shorten the period (from 48 hours to 24 hours) within which service providers have to respond to a user complaint before the eSafety Commissioner can issue a removal notice.[71]

Link deletion notices

1.66 The bill would expand the online content scheme under the Online Safety Act to empower the eSafety Commissioner to issue link deletion notices to internet search engine providers in relation to cyberbullying material targeted at an Australian child, non-consensually shared intimate image of a person and cyber-abuse material targeted at an Australian adult. Before issuing a link deletion notice, the Commissioner must be reasonably satisfied that giving the notice is appropriate in the circumstances, and a removal notice must have already been issued in relation to the material.[72]

1.67 The Explanatory Memorandum notes that the expansion of the link deletion notice powers would 'address the continued accessibility of harmful material through search engine results in the period between a removal notice being issued and compliance with that notice'.[73]

---

70 See Division 2 of Part 1 in Schedule 1 of the bill.

71 The bill, EM, p. 6.

72 See Division 3 of Part 1 in Schedule 1 of the bill.

73 The bill, EM, p. 6.

Increased penalties

1.68 The bill proposes to increase a range of civil penalties in the Online Safety Act from 500 penalty units ($182 000) to 6000 penalty units ($2.184 million). These include penalties for non-compliance with removal notices in relation to cyberbullying material, cyber-abuse material and non-consensual intimate images; non-compliance with removal notices, link deletion notices or app removal notices relating to class 1 material;[74] and posting, or threatening to post, non-consensual intimate images.[75]

1.69 Civil penalties for non-compliance with industry codes and standards would increase from 30 000 penalty units ($10.920 million) to 60 000 penalty units ($2.184 million).[76]

1.70 In addition, the bill would provide for higher penalties to apply to corporations for specified contraventions of the Online Safety Act. Proposed section 163AA would increase the penalties payable by bodies corporate for contraventions of specified provisions, from 60 penalty units ($21 840) to 600 penalty units ($218 400).[77]

Commencement

1.71 The bill provides that Schedule 1, including expanded powers for the eSafety Commissioner in relation to take down notices, would commence on the day after the Act receives Royal Assent.[78]

1.72 Schedule 2 of the bill, which, amongst other things, establishes the Duty and other requirements relating to risk assessments and user empowerment tools, and Schedule 3 of the bill, which provides for the repeal of online content scheme industry codes and standards, would commence 12 months after Royal Assent. This would mean that 'the delayed effect of the Duty … [would] coincide with the repeal of the Basic Online Safety Expectations, and industry codes and standards'.[79]

---

74 The definition of 'class 1 material' is set out in section 106 of the Online Safety Act.

75 See: Part 4 of Schedule 1 of the bill; Parliamentary Library, Bills Digest No. 26, 2026–27, 23 October 2026, p. 8.

76 Proposed subsections 143(2) and 146(1). Parliamentary Library, Bills Digest No. 26, 2026–27, 23 October 2026, p. 8.

77 The bill, EM, pp. 82–83.

78 Section 2 of the bill.

79 The bill, EM, p. 2.

Examination by other parliamentary committees

1.73 When examining a bill, the committee takes into account any relevant comments published by the Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) and the Parliamentary Joint Committee on Human Rights (Human Rights Committee).

1.74 At the time of writing, neither the Scrutiny of Bills Committee nor the Human Rights Committee have reported on the bill. However, the Explanatory Memorandum advises that the bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

1.75 The bill's Explanatory Memorandum acknowledges that the bill engages human rights under articles 14, 17, 19, 20 and 26 of the International Covenant on Civil and Political Rights, articles 2, 3, 12, 13, 16, 17, 19, 24 and 40 of the Convention on the Rights of the Child and articles 16, 21 and 22 of the Convention on the Rights of Persons with Disabilities.[80] According to the Statement of Compatibility with Human Rights:

> To the extent to which the measures in the Bill may engage the right to freedom of expression, the right to privacy, the right to certain minimum guarantees in criminal proceedings and the right to non-discrimination, any limitation is reasonable, necessary and proportionate to the goal of promoting and improving online safety for Australians.[81]

[80] The bill, EM, Statement of Compatibility with Human Rights, pp. 15–22.

[81] The bill, EM, Statement of Compatibility with Human Rights, p. 22.

Chapter 2
Digital Duty of Care and platform obligations

2.1 Submitters and witnesses to the inquiry expressed broad support for the objectives of the Online Safety Amendment (Digital Duty of Care) Bill 2026 (the bill), recognising the prevalence and severity of online harms and the importance of protecting Australians from these harms.

2.2 While many inquiry participants welcomed the strengthening of the online safety framework, concerns were raised regarding the scope and clarity of certain measures, and whether they are risk-based, proportionate, and appropriately calibrated to achieve the bill's objectives.

2.3 This chapter examines the proposed duties and mechanisms directed to the identification, prevention and minimisation of online harms. It considers issues raised in evidence to the inquiry relating to the scope of the Digital Duty of Care (the Duty) and definitions of online harms, protections against harmful design features, and the requirements relating to risk assessments, user empowerment tools, and age assurance and access control.

2.4 The following chapter examines key issues in relation to regulatory powers and oversight, enforcement and remedies.

Support for a stronger regulatory approach

2.5 Many inquiry participants supported a systemic, proactive and preventative regulatory approach to online safety, as proposed by the bill.[1] Ms Emma Mason, who lost her daughter to suicide following online bullying, gave powerful evidence on the first day of public hearings that illustrated the profound human consequences of online harms and the pressing need for stronger regulatory measures to hold technology platforms to account:

> At the end of these hearings and every day that there are no laws to hold these companies to account, three things will remain true: our children will still be gone. The online world will continue to harm more children, and some will die. And these big tech companies will continue to offer empty promises of future change. In the end, when protecting adults and children online, prevention should not be an aspiration; it must be an obligation.[2]

2.6 Likewise, Mr Wayne Holdsworth, who lost his son to suicide following sexual extortion online, emphasised the seriousness of the harms that can occur through exposure to harmful algorithms and stressed the urgency of reform:

> If we delay this, and every day we delay it, we're exposing more children to the harmful algorithms, with them subsequently becoming anxious, depressed and, potentially, taking their life. We don't want another child to go through what our children went through.[3]

2.7 Ms Mason argued that online services are an outlier in the commercial world as '[s]afety by design … [is] mandatory in every part of the commercial world except in the digital world'. Ms Mason linked the Duty to the foundational principle of the common law of torts: 'the idea that every provider of a good or service owes a duty of care to its consumer'.[4]

---

1 See, for example: Ms Mia Bannister, *Submission 7*, p. 2; Prevention United, *Submission 10*, p. 3; National Council of Women Australia, *Submission 30*, [p. 3]; With You We Can, *Submission 38*, p. 2; The Centre for Excellence in Child & Family Welfare, *Submission 52*, [p. 1]; Human Rights Law Centre, *Submission 57*, p. 4; Australian Human Rights Commission, *Submission 58*, p. 5; Tech Policy Design Institute, *Submission 69*, p. 1; Y Australia, *Submission 97*, [p. 2]; yourtown, *Submission 100*, p. 2; National Foundation for Australian Women (NFAW), *Submission 113*, p. 2; Maurice Blackburn, *Submission 161,* p. 1.

2 Ms Emma Mason, Private capacity, *Proof Committee Hansard,* 9 November 2026, p. 4.

3 Mr Wayne Holdsworth, Founder, SmackTalk, *Proof Committee Hansard,* 9 November 2026, p. 3.

4 Ms Emma Mason, Private capacity, *Proof Committee Hansard,* 9 November 2026, p. 3.

2.8 This view was reinforced by numerous child safety and gender equality advocates and organisations who welcomed the bill's emphasis on platform accountability.[5] Ms Mia Bannister, a mother who experienced the loss of her son to suicide following online harms, told the committee:

> We cannot continue to place the primary responsibility for managing online harm on children, parents and educators while the companies designing, operating and profiting from digital environments remain insufficiently accountable for the risks created by their services.
>
> A Digital Duty of Care provides an opportunity to shift that responsibility towards prevention, safer design and demonstrable accountability.[6]

2.9 Ms Chanel Contos told the committee that:

> It's about making tech platforms take proactive steps to prevent content like child sexual abuse material and content inciting violence. These things are already illegal, but tech platforms currently have no obligation to prevent them from spreading. The digital duty of care applies basic safety standards, as we have in every other industry, online and takes them out of the bubble of impunity that they currently sit in. If a tech company designs and profits from a harmful, addictive digital environment, that is not okay and it's on them to make it safer.[7]

2.10 The ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S), a cross-disciplinary national research centre, welcomed the introduction of a Digital Duty of Care which would address systemic design risks:

> We support the shift towards an outcomes-based duty to take appropriate action to ensure a safe online environment. This approach is much more capable of managing broader, systemic and emerging online harms than past "regulatory whack-a-mole" approaches focused only on narrow, specific risks.[8]

---

5 See, for example: ARACY - Australian Research Alliance for Children and Youth, *Submission 88*, [p. 6]; Y Australia, *Submission 97*, [p. 2]; yourtown, *Submission 100*, p. 2; Working with Women Alliance, *Submission 134*, p. 3.

6 Ms Mia Bannister, *Submission 7*, p. 2.

7 Ms Chanel Contos, Chief Executive Officer and Founder, Teach Us Consent Global, *Proof Committee Hansard*, p. 8.

8 ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, p. 3.

2.11 The significance of the proposed changes to Australia's regulatory approach was highlighted by the eSafety Commissioner:

> The Bill represents an evolutionary shift in regulatory approach from the current Online Safety Act, which will necessitate a change in enforcement approach.
>
> Whilst the introduction of an overarching digital duty of care provides a more flexible, durable and proactive framework for addressing online harms, this approach fundamentally changes the nature of regulatory oversight and enforcement compared to the current framework. Rather than assessing historical compliance breaches against specific obligations, as under the Online Safety Codes and Standards, eSafety will be required to evaluate whether providers have taken appropriate action to identify, assess, and effectively mitigate online safety risks from occurring in the first place.[9]

2.12 The Commissioner referred to the bill as a 'huge step change in the right direction' and explained that:

> To me, the digital duty of care is a clear evolution. We're really in the fourth wave of Online Safety Act reform. This uses safety by design as the primary scaffolding … I think it's reasonable that, as a regulator, you would want to have a suite of the best tools possible and grab those tools from each previous set of legislation while giving us really a new way to approach enforcement and put the onus back on the platforms to assess risk and build in rather than bolt on safety. Again, this builds on 11 years of experience and I think it's the right evolution.[10]

2.13 Ms Clare Chapple, First Assistant Secretary within the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department), remarked that the establishment of a broad Duty would:

> … mov[e] from a setting where there are 17 codes and standards that are fragmented and difficult to navigate—and we very much heard that feedback in consultation—to something that brings that together in a single duty of care that has the flexibility to be able to move with technology and the online experiences.[11]

2.14 Other inquiry participants similarly observed that the overarching nature of the Duty would represent a significant improvement on the current framework of prescriptive industry codes which have limited capacity to keep pace with

---

9 eSafety Commissioner, *Submission 129*, p. 9.

10 Ms Julie Inman Grant, Commissioner, Office of the eSafety Commissioner, *Proof Committee Hansard,* 10 November 2026, p. 61.

11 Ms Clare Chapple, First Assistant Secretary, Digital Policy, Online Safety and Classification Division, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department), *Proof Committee Hansard,* 10 November 2026, p. 72. See also, Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, the department, *Proof Committee Hansard,* 10 November 2026, p. 75.

evolving technologies and set less stringent safety requirements due to the industry co-design process through which they were developed.[12]

2.15 Mr Jamie Crosby, Chief Executive Officer of the Centre for Excellence in Child and Family Welfare, highlighted that the Duty's non-exhaustive approach to identifying harmful design features offers an important conceptual advantage by enabling the framework to respond to emerging design risks:

> It's important due to the rapidly evolving nature of online platforms and technologies in and of themselves. We don't know what next month might look like, and we don't know what next year might look like. Having appropriate safeguards that encompass evolving technologies in a non-exhaustive list is an important principle to include within the bill so that we can respond to technologies and their impacts upon children and young people as they evolve, ensuring that we keep children and young people in online environments as safe as we possibly can as technology grows and evolves over time.[13]

2.16 Multiple inquiry participants commended the proposed shift from reactive content removal to upstream prevention of online harms.[14] For example, Dr Rys Farthing, Chief Research Officer of Reset Tech Australia, outlined how the bill tackles harmful, addictive technology:

> I think this is core to what this bill is trying to do. It is attempting to move away from our current Online Safety Act, which by nature of its history and policy path, focuses on notice and takedown—so it focuses on types of content. And it moves us towards a model of legislation that's systemic, that's trying to move into a preventative mode, where companies have to risk-assess their services and prevent harms from occurring in the first instance, including harms from designs such as addictive design features[.][15]

---

[12] See: Dr Rys Farthing, Chief Research Officer, Reset Tech Australia, *Proof Committee Hansard,* 10 November 2026, p. 37; Ms Johanna Weaver, Co-founder and Executive Director, Tech Policy Design Institute, *Proof Committee Hansard,* 10 November 2026, pp. 48–49; Ms Julie Inman Grant, Commissioner, Office of the eSafety Commissioner, *Proof Committee Hansard,* 10 November 2026, p. 68; Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, the department, *Proof Committee Hansard,* 10 November 2026, p. 74.

[13] Mr Jamie Crosby, Chief Executive Officer, Centre for Excellence in Child and Family Welfare, *Proof Committee Hansard,* 9 November 2026, p. 16.

[14] See, for example: Dr Honni van Rijswijk, *Submission 6*, p. 1; With You We Can, *Submission 38*, p. 2; Bravehearts, *Submission 89*, [p. 1]; Center for Cybersecurity Policy and Law, *Submission 105,* [p. 1]; Ms Chanel Contos, Chief Executive Officer and Founder, Teach Us Consent Global, *Proof Committee Hansard,* 9 November 2026, p. 8; Mr David Braga, Chief Executive Officer, International Justice Mission Australia, *Proof Committee Hansard,* 9 November 2026, p. 17.

[15] Dr Rys Farthing, Chief Research Officer, Reset Tech Australia, *Proof Committee Hansard,* 10 November 2026, p. 34. See also, Ms Rinat Strahlhofer, Founder, Digital Readiness Lab, *Proof Committee Hansard,* 10 November 2026, p. 35.

2.17 In a similar vein, Associate Professor Honni van Rijswijk of the University of Technology Sydney submitted that:

> The Online Safety Amendment (Digital Duty of Care) Bill 2026 is a welcome Bill and it should be passed. It marks a genuine change of regulatory direction: away from a regime built on reactive takedown, in which harmful material must first be encountered, reported and complained about before anything happens, and towards a proactive and systemic duty that obliges the organisations which design and operate digital services to identify and mitigate the foreseeable risks their own products create. That shift is correct in principle and overdue in practice.[16]

2.18 Dr van Rijswijk provided a product safety analogy to argue that responsibility for preventing harm should rest with the corporations that design, operate and profit from digital products, just as manufacturers are required to ensure the safety of physical products:

> We do not respond to a car that somersaults at speed by issuing advice to drivers about careful steering. We require the vehicle to be designed so that it does not somersault, and we impose that requirement on the manufacturer, who is the party able to discharge it. The same logic should apply to digital products whose design foreseeably multiplies exposure to sexual assault, image-based abuse, grooming, eating disorder material and self-harm content. The Bill accepts that logic in principle.[17]

Digital Duty of Care

2.19 A number of inquiry participants commented on: the formulation of the Duty in proposed section 26; the matters to be taken into consideration under proposed section 26A when determining compliance with the Duty; and the definition of online services in proposed section 25B to which the Duty would apply.

Clarity of the standard in proposed section 26

2.20 The Digital Industry Group Inc (DIGI), an industry association representing major technology companies, called for greater clarity around the standard that online services must meet. Regarding the obligation in proposed section 26 to take appropriate action to 'ensure' a safe online environment, DIGI argued: 'This standard is uncertain and could mean that a service must prevent all exposure, or only that it must take reasonable steps to reduce the risk'.[18] DIGI continued that:

> The duty as drafted requires appropriate action "including" mitigating identified risks, so mitigating those risks may not be enough. The matters to

---

16 Dr Honni van Rijswijk, *Submission 6*, p. 1.

17 Dr Honni van Rijswijk, *Submission 6*, p. 3. See also, p. 10.

18 Digital Industry Group Inc (DIGI), *Submission 90*, p. 6.

> be weighed are not exhaustive, and the risk assessment must identify "reasonably foreseeable risks" without saying risks of what.[19]

2.21 Similar concerns regarding the lack of certainty in the standard required by the Duty were raised by other technology industry members.[20]

2.22 DIGI and others supported the inclusion of a 'reasonably practicable' qualifier to the Duty.[21] Snap Australia, for example, argued that the removal of the exposure draft's 'reasonably practicable' qualifier 'creates uncertainty about the relationship between the Duty, the requirement to take "effective measures" and the factors in section 26A'.[22] Further, the Business Council of Australia submitted that:

> Reasonable practicability is a well-understood standard in Australian safety law, including work health and safety law. A maximum civil penalty of 60,000 penalty units demands clear requirements. Improving clarity would give providers greater certainty about what the duty requires.[23]

2.23 Some inquiry participants suggested that the standard required by the Duty could be clarified by prescribing specific minimum obligations to comply with the Duty. International Justice Mission Australia recommended that a list of minimum mandatory standards applicable to all online services and all types of harm could be included in proposed section 26 and that the eSafety Commissioner should be empowered to develop enforceable rules specifying additional minimum standards for particular types of material and conduct.[24]

2.24 The eSafety Commissioner raised the possibility that:

> … should Parliament wish to provide further specificity in the Bill, the Bill could prescribe specific minimum obligations to comply with the digital duty of care under disallowable legislative instrument. Requirements in legislative instrument could draw on the obligations in the Online Safety Codes and Standards in a streamlined and simplified manner. This would reduce complexities in the existing framework but provide industry with sufficient clarity under the new framework.[25]

---

19 DIGI, *Submission 90*, p. 7.

20 See, for example: TikTok Australia, *Submission 28*, p. 3; Snap Australia, *Submission 40*, pp. 2–4; Match Group, *Submission 92*, pp. 2–3; Meta, *Submission 73*, p. 4; Bumble Inc., *Submission 107*, p. 3. For other industry groups, see also: Business Council of Australia (BCA), *Submission 34*, pp. 3–4; Interactive Games & Entertainment Association (IGEA), *Submission 93*, p. 5.

21 See, for example: BCA, *Submission 34*, p. 4; The Information Rights Project, *Submission 37*, p. 1; DIGI, *Submission 90*, pp. 8 and 19; Match Group, *Submission 92*, p. 1; IGEA, *Submission 93*, p. 5; Business Software Alliance, *Submission 104*, p. 5.

22 Snap Australia, *Submission 40*, p. 2.

23 BCA, *Submission 34*, p. 4.

24 International Justice Mission Australia, *Submission 50*, pp. 2–3.

25 eSafety Commissioner, *Submission 129*, p. 13.

2.25 Ms Johanna Weaver, Co-founder and Executive Director of the Tech Policy Design Institute, acknowledged the desire for the Duty to be more prescriptive but pointed out that the Online Safety Act already contains guidance in interpreting the Duty and that there are benefits to a non-prescriptive approach:

> The [A]ct does define, in 26A, what is 'appropriate and effective'. So there is guidance there which is quite extensive. It also allows for what is appropriate and effective to evolve over time. What is appropriate and effective to respond to a harm today will be very different in six months because the technology will evolve. And I think we want to avoid a situation where we have to come back to parliament every time the technology changes. I think this is actually well drafted and will allow for us to evolve over time, and I don't say that lightly.[26]

2.26 Additionally, the department's Ms Chapple explained that greater specificity in legislative definitions can give rise to unintended consequences:

> … we have been watching the evidence and some calls for specificity around definitions. When you provide that specificity, it can have the opposite effect and it can actually provide a floor rather than a ceiling. What you can see sometimes is very strict compliance with that black letter, but perhaps they're not taking that broader duty of care for harms that exist beyond that, which is very much the intent of this bill.[27]

2.27 The Explanatory Memorandum to the bill notes that under proposed section 28 the eSafety Commissioner would have the power to publish guidelines to:

> … assist persons responsible for online services to meet their digital duty of care. The guidelines will not be binding; however, they are intended to give service providers practical information about how they can meet their obligations under the Duty, and about eSafety's compliance expectations.[28]

---

[26] Ms Johanna Weaver, Co-founder and Executive Director, Tech Policy Design Institute, *Proof Committee Hansard*, 10 November 2026, p. 49.

[27] Ms Clare Chapple, First Assistant Secretary, Digital Policy, Online Safety and Classification Division, the department, *Proof Committee Hansard*, 10 November 2026, p. 72.

[28] Online Safety Amendment (Digital Duty of Care) Bill 2026 (the bill), Explanatory Memorandum (EM), p. 79.

Matters to be taken into account under proposed section 26A

2.28 A range of suggestions were put forward in evidence regarding the list of matters to be taken into account under proposed section 26A in determining what is appropriate and effective for the purposes of complying with the Duty. For instance, DIGI supported the addition of technical feasibility, privacy, impacts on lawful expression, and cost to the list of matters to be taken into account.[29] Other suggestions raised by inquiry participants included human rights considerations[30] and impacts on service security.[31]

2.29 A selection of comments is provided below in relation to privacy and cost considerations.

Privacy

2.30 Several inquiry participants queried the omission of privacy from the list of considerations in proposed section 26A.[32] The Office of the Australian Information Commissioner (OAIC) mentioned that under the bill's current wording there is a risk that:

> … online services may argue that the collection of additional personal information is required to comply with clause 26A within the Digital Duty of Care. The OAIC notes that the increased collection of personal information can create risks to individual's privacy and lead to serious adverse consequences where mishandled, for instance due to insufficient privacy practices or a data breach.[33]

2.31 The OAIC suggested that there may be a need to provide clearer 'direction to online services implementing actions and measures as to what is reasonably necessary and proportionate for compliance with the Bill and the Privacy Act'.[34]

---

29 DIGI, *Submission 90*, pp. 8 and 19.

30 Scarlet Alliance, National Sex Workers Association, *Submission 121*, p. 3.

31 Snap Australia, *Submission 40*, p. 3.

32 See, for example: Privacy 108, *Submission 25*, p. 2; Google, *Submission 27*, p. 2; FamilyVoice Australia, *Submission 36*, p. 2; NSW Council for Civil Liberties (NSWCCL), *Submission 55*, p. 3; Institute of Public Affairs, *Submission 56*, p. 5; Match Group, *Submission 92*, pp. 2–3; IGEA, *Submission 93*, p. 3; Bumble Inc., *Submission 107*, p. 3; liber-net, *Submission 108*, [p. 2].

33 Office of the Australian Information Commissioner (OAIC), *Submission 48*, p. 2.

34 OAIC, *Submission 48*, p. 2.

2.32 The Australian Human Rights Commission (AHRC) expressed concern regarding the lack of an express requirement to consider privacy impacts when determining measures necessary to comply with the Duty. The AHRC stated that, given the potential privacy implications of age assurance measures in the bill, the Explanatory Memorandum should clarify that section 26A requires consideration of broader human rights impacts, including the right to privacy.[35]

2.33 The bill's Statement of Compatibility with Human Rights notes that:

> To the extent that obligations in the Bill would require the collection of personal information and limit a user's right to privacy, any such limitation is reasonable, necessary and proportionate to achieving a safe online environment for Australians.[36]

Cost

2.34 The bill's exclusion of cost from the matters to be considered under proposed section 26A was raised as a particular concern by some submitters.[37]

2.35 The Business Council of Australia submitted that the exclusion of financial and operational costs as a consideration is 'inconsistent with proportionality and may create prohibitive barriers for smaller businesses or deter beneficial product development'.[38] Likewise, the Interactive Games & Entertainment Association (IGEA) noted that the exclusion of cost considerations is a 'particular concern for the many SMEs [Small and Medium Enterprises] and independent studios in the Australian video games industry'.[39]

---

35 Australian Human Rights Commission, *Submission 58*, p. 7.

36 The bill, EM, Statement of Compatibility with Human Rights, p. 18.

37 See, for example: Australians for Science and Freedom, *Submission 32*, p. 3; Snap Australia, *Submission 40,* p. 3; Consumer Choice Center, *Submission 78,* [p. 3]; Business Software Alliance, *Submission 104*, p. 5; Association for Competitive Technology (ACT), *Submission 106*, p. 2; Bumble Inc., *Submission 107*, p. 3; Internet Association of Australia, *Submission 127*, p. 4; Consumer Electronics Suppliers Association, *Submission 160,* p. 3.

38 BCA, *Submission 34*, p. 4.

39 IGEA, *Submission 93*, p. 17.

2.36 In comparison, several inquiry participants commended the stipulation that cost must not be taken into consideration under proposed section 26A.[40] The Women's Legal Service NSW, for instance, 'particularly welcome[d]' the inclusion of the provision:

> … that precludes cost from being a justification for duty holders *not* to take action. We recommend that this provision remains in the Bill as a safeguard to prevent online service providers from circumventing their duty of care because of potential implications on profit.[41]

2.37 Dr van Rijswijk similarly praised the 'principled drafting choice' in proposed subsection 26A(3) that should be 'preserved without qualification', adding that:

> Cost is relevant to how an obligation is discharged; it should not be permitted to determine whether safety is owed at all. Where cost is allowed to enter the standard of care, the standard becomes a function of the duty-holder's willingness to spend, which is precisely the inversion the Bill is designed to correct.[42]

2.38 The department noted that proposed subsection 26A(3) 'recognises that there are serious harms which platforms must take effective measures to address'.[43]

Online services captured by the Digital Duty of Care

2.39 Numerous inquiry participants commented on the breadth of the bill's definition, in proposed section 25B, of online services that would be captured by the Duty.[44]

---

40 See, for example: With You We Can, *Submission 38*, p. 2; The Centre for Excellence in Child & Family Welfare, *Submission 52*, [p. 2]; Older Women's Network NSW, *Submission 76*, [p. 6]; Associate Professor Joel Scanlan, Professor Jeremy Prichard, Dr Rachel Baird and Dr Nina Hudson, *Submission 84*, [p. 1]; Gender Justice Australia, *Submission 85*, p. 1; ARACY – Australian Research Alliance for Children and Youth, *Submission 88*, [p. 3].

41 Women's Legal Service NSW, *Submission 95*, p. 4.

42 Dr Honni van Rijswijk, *Submission 6*, p. 2.

43 The department, *Submission 130,* pp. 6–7.

44 See, for example: Australian Human Rights Commission, *Submission 58*, pp. 15–16; IGEA, *Submission 93*, pp. 3–4; Business Software Alliance, *Submission 104*, p. 4; Internet Association of Australia, *Submission 127*, p. 4; SBS, *Submission 133,* pp. 1–3.

2.40 Dr van Rijswijk praised the 'decision to impose a single overarching duty across the whole technology stack rather than a patchwork of service-specific obligations', and added that:

> Proposed s 25B(1) extends the duty to social media services, relevant electronic services and designated internet services, but also to artificial intelligence generation services, app distribution services, internet carriage services, hosting services, search engine services and equipment manufacturers and suppliers. That breadth matters, because harm in the digital environment is produced by the interaction of layers, and a duty that stops at the application layer invites the displacement of risk to the layers below it.[45]

2.41 In comparison, DIGI expressed concern about the breadth of entities that would be captured by the Duty and the potential impacts on business systems and small businesses:

> The duty reaches almost every business online. The duty applies to every "online service", including internet carriage, messaging, websites and apps, hosting, search, app stores, AI services and equipment suppliers. It will reach almost every Australian business with a website, app, customer accounts or connected devices, many of which are already extensively regulated.[46]

2.42 DIGI advocated for greater clarity on how the Duty applies to business systems and low-risk services, such as workplace collaboration tools, private cloud storage and enterprise AI tools, which 'have a very different risk profile' from consumer platforms and services.[47]

2.43 Likewise, the Business Council of Australia supported risk-based exclusions for 'low-risk informational and transactional websites, enterprise, business-to-business and infrastructure services'. It also emphasised the need to avoid regulatory duplication, for example in relation to '[f]inancial service providers [who] already face extensive prudential, conduct, complaints-handling, scams, anti-money laundering and fraud requirements'.[48]

2.44 Along similar lines, the Australian Retail Council argued that online retail platforms, e-commerce marketplaces and commercial retail websites are 'fundamentally different from higher-risk digital services' and should be expressly excluded from the bill.[49]

---

45 Dr Honni van Rijswijk, *Submission 6*, p. 2.

46 DIGI, *Submission 90*, p. 25.

47 DIGI, *Submission 90*, pp. 3 and 25.

48 BCA, *Submission 34*, p. 7.

49 Australian Retail Council, *Submission 155*, p. 1.

2.45 Concerns were also raised by submitters and witnesses regarding the application of the Duty to churches and other religious organisations, charities and schools which may operate websites and other online services.[50]

2.46 The department stated that the breadth of the scope of online services subject to the Duty would be 'balanced by the proportional design of the Duty', explaining that:

> Under the Duty, the measures online services will be required to take will vary – in proportion both to the extent to which a service could give rise to harm, and the extent to which actions or measures by the service will or may reasonably be expected to reduce those risks. Services that carry a lower risk of harm, or which have a less direct or more remote responsibility for the provision of harmful material or conduct than other services, will necessarily have less responsibility and fewer obligations under the Duty. This proportionality will be supported where necessary by the ability of the Minister to exempt a low-risk online service or class of online services from the operation of the Duty or related provisions.[51]

2.47 In response to concerns about the impact of the bill on small businesses and low-risk online services, departmental officer Ms Chapple stated that the bill is 'proportional by design' and noted that the services captured by the proposed framework are already subject to existing codes and standards. She argued that the bill would simplify the regulatory framework by consolidating obligations in a single scheme.[52]

2.48 Mr Andrew Hyles, Assistant Secretary within the department, also told the committee that the vast majority of websites would be low-risk entities because they do not host the types of harmful content or features targeted by the bill. He indicated that risk assessments for such services would be straightforward and limited in scope:

> The reality of it is that the vast majority of websites don't contain this content. They don't contain the seriously harmful content that's identified. They don't contain the harmful content that's identified. They don't contain the features that are problematic. From that perspective, the vast majority of entities will be low-risk entities. ESafety in their own submission has identified that, for the form of the risk assessment, it will be a very simple, checkbox kind of process.[53]

---

50 See, for example: National Catholic Education Commission, *Submission 35*, p. 2; Coptic Orthodox Diocese of Sydney & Affiliated Regions, *Submission 46*, pp. 1–2; Anglican Church, Diocese of Sydney, *Submission 63*, p. 4.

51 The department, *Submission 130,* p. 4.

52 Ms Clare Chapple, First Assistant Secretary, Digital Policy, Online Safety and Classification Division, department, Proof Committee Hansard, 10 November 2026, p. 74.

53 Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, department, *Proof Committee Hansard*, 10 November 2026, p. 74.

Harm definitions

2.49 The committee received a wide range of evidence on the appropriateness of the definitions of seriously harmful material and conduct (proposed section 25D), and material and conduct that is harmful to children (proposed section 25E).

Seriously harmful material and conduct

2.50 Inquiry participants expressed support for the bill's inclusion of particular categories of seriously harmful material and conduct in proposed section 25D, including:

- fake nude material created without consent;
- posting, or threatening to post, an intimate image of another person without consent; and
- material and conduct that encourages, promotes, incites or instructs gender-based violence.[54]

2.51 The AHRC noted that positive changes had been made since the release of the exposure draft 'to rightly narrow the definitions to be both more workable and better calibrated to protect freedom of expression'.[55]

2.52 Additionally, the AHRC and others welcomed the removal of the ministerial power to determine, by legislative instrument, additional categories of seriously harmful material and conduct, which had featured in the bill's exposure draft.[56] The AHRC stated that:

> Given the potential restrictions on lawful expression, access to information and rights to protest, any expansion of the scope of seriously harmful material and conduct should be made through primary legislation and subject to full parliamentary scrutiny. This provides greater certainty about the scope of the [Duty] and ensures that proposed restrictions can be assessed for their necessity, proportionality and human rights implications.[57]

---

54 See, for example: Dr Honni van Rijswijk, *Submission 6*, p. 2; Associate Professor Andrew Moshirnia and Dr Amanda Selvarajah, *Submission 9*, [p. 1]; Protocol Policy Lab Ltd, *Submission 17*, [p. 1]; Teach Us Consent, *Submission 29*, [p. 5]; Australian Human Rights Commission, *Submission 58*, p. 8; Equality Australia, *Submission 59*, p. 5; ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, pp. 4–5; Working with Women Alliance, *Submission 134*, p. 4.

55 Australian Human Rights Commission, *Submission 58*, p. 8.

56 See, for example: Teach Us Consent, *Submission 29*, [p. 4]; Coptic Orthodox Diocese of Sydney & Affiliated Regions, *Submission 46*, p. 1; Australian Human Rights Commission, *Submission 58*, p. 10; Australian Jewish Association, *Submission 61*, [p. 1]; Anglican Church, Diocese of Sydney, *Submission 63*, p. 2; Bravehearts, *Submission 89*, [p. 8]; Dr Rob Nicholls, *Submission 103*, p. 3; Canberra Declaration, *Submission 124*, p. 7; Anne Twomey, Professor Emerita, *Submission 132*, p. 1.

57 Australian Human Rights Commission, *Submission 58*, p. 10.

2.53 Some organisations suggested that further categories should be added to the list of seriously harmful material and conduct.[58] Several submitters called for stronger measures to address group-based hatred and vilification directed at people on the basis of characteristics including race.

2.54 For example, Mr Peter Wertheim, Co-Chief Executive Officer of the Executive Council of Australian Jewry, highlighted the absence of a provision in the bill 'for dealing with content that promotes hatred on the basis of race or other inherent characteristics', and raised concerns that social media platforms and large technology companies currently amplify the promotion of that hatred.[59]

2.55 Mr Leon Zwier, Partner at Arnold Bloch Leibler, similarly argued that stronger measures were needed to combat hate speech directed at protected groups and to enable its swift removal from social media platforms:

> The difficulty that we all have in taking on platforms…—is the disproportionate power. They have vast resources and incredible capability to retain lawyers, including senior counsel, in vast numbers. Therefore, we need to find a way to combat hate speech—knowing, of course, that the propagation of hate speech is connected to violence.
>
> … We need, therefore, to find a very cost-effective, speedy way of removing hate speech from social media platforms.[60]

2.56 Mr Tom Sulston, Head of Policy at Digital Rights Watch, also pointed to the commercial incentives for large digital platforms—particularly social media platforms—to promote and elevate hateful and extremist content:

> … because those very fringe views—the hateful, extremist content—are very engaging and users do pay a lot of attention to them, there's an incentive for the social media companies to pay the creators of that content. They revenue share, so they generate yet more of it. There is a drive by creators to create ever more extreme content that gets more engagement that gets paid out by the social media companies, who in turn monetise us receiving that through advertisements.[61]

---

[58] See, for example: Dr Honni van Rijswijk, *Submission 6*, p. 37; With You We Can, *Submission 38*, p. 4; Relationships Australia, *Submission 39*, p. 2; Our Watch, *Submission 51*, pp. 4–5; Gender Justice Australia, *Submission 85*, p. 7; Women's Legal Service NSW, *Submission 95*, p. 3; NFAW, *Submission 113*, p. 5.

[59] Mr Peter Wertheim, Co-Chief Executive Officer, Executive Council of Australian Jewry, *Proof Committee Hansard*, 10 November 2026, p. 19.

[60] Mr Leon Zwier, Partner, Arnold Bloch Leibler, *Proof Committee Hansard*, 10 November 2026, p. 19.

[61] Mr Tom Sulston, Head, Policy, Digital Rights Watch, *Proof Committee Hansard*, 9 November 2026, p. 26.

2.57 Inquiry participants argued that online attacks based on protected characteristics should be expressly recognised within proposed section 25D, consistent with Recommendations 21 and 22 of Ms Delia Rickard PSM's review of the *Online Safety Act 2021* (Online Safety Act).[62] The Human Rights Law Centre argued that this category should cover:

> … material or conduct that encourages, promotes, incites or instructs hatred against a person or group on the basis of race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality, or national or ethnic origin, where it is reasonably likely to lead to serious harm.[63]

2.58 Our Watch, an organisation working on the primary prevention of violence against women and their children, highlighted the prevalence of technology facilitated abuse directed at women and LGBTQIA+ communities.[64] Dr Romy Listo of Our Watch argued for the definition of harm to be expanded to include gender hostile attitudes towards women and gender equality, for both adults and children, because:

> … there has been this relationship drawn between adherence to what Our Watch calls the gender drivers of violence—which include the condoning of violence against women, men's control over decision-making and women's independence, rigid gender stereotypes and dominant forms of masculinity and male peer relations and cultures of masculinity that emphasise aggression, dominance and control—and violence against women downstream. It's our view regarding that this content that there's an opportunity, through the digital duty of care, to require online services to regulate the risks arising from this content, for both young people as well as adults.[65]

---

62 See, for example: Human Rights Law Centre, *Submission 57*, pp. 6 and 11; Equality Australia, *Submission 59*, p. 3; Gender Justice Australia, *Submission 85*, p. 7; Trans Justice Project, *Submission 101*, p. 2; Older Women's Network NSW, *Submission 76*, [p. 2]; Women's Services Network, *Submission 82*, p. 5; National Aboriginal and Torres Strait Islander Women's Alliance (NATSIWA), *Submission 83*, [p. 6]; Arnold Bloch Leibler, ECAJ, ZFA, NSW JBOD, NCJWA, JCCV, Dor Foundation & AIJAC, *Submission 128*, pp. 1–2; Australian Muslim Advocacy Network, *Submission 157*, pp. 5–6.

63 Human Rights Law Centre, *Submission 57*, p. 6.

64 Our Watch, *Submission 51*, pp. 2 and 4; Dr Romy Listo, Manager, Prevention Strategy and Policy Development, Our Watch, *Proof Committee Hansard,* 9 November 2026, p. 22.

65 Dr Romy Listo, Manager, Prevention Strategy and Policy Development, Our Watch, *Proof Committee Hansard,* 9 November 2026, p. 22. See also: Dr Gemma Killen, Executive Director, Working with Women Alliance, *Proof Committee Hansard,* 10 November 2026, p. 3.

2.59 On the other hand, some inquiry participants argued that the existing categories in proposed section 25D are too broad and made suggestions for narrowing or removing them.[66] For example, Dr Rob Nicholls, Senior Research Associate at the University of Sydney, suggested that each category should correspond to conduct that amounts to an identifiable criminal offence in at least one Australian jurisdiction.[67]

2.60 The Free Speech Union of Australia (FSU) submitted that the definition of seriously harmful material and conduct would capture a wide range of online content and lead to extensive censorship. Accordingly, the FSU argued that the provisions should be removed from the bill.[68]

2.61 Conversely, Mr Zwier from Arnold Bloch Leibler addressed apprehensions about the reach of the bill and its impacts on free speech, arguing that some limitations on free speech are necessary and appropriate:

> There is no perfect free speech here. We have defamation laws. We have laws that prohibit misleading and deceptive conduct. We have all sorts of constraints—section 18C. It's not pure. What this is about is hate speech leading to terrorism and violence in Australia, and we have to fight that. We have to fight it with every available resource that we have because this is the beginning. This is the beginning, and we have to stamp it out. We have to stamp it out quickly.[69]

---

66 See, for example: Libertarian Party (WA), *Submission 12*, [p. 2]; Dr. Alexander Hatzikalimnios, *Submission 45,* pp. 4–6.

67 Dr Rob Nicholls, *Submission 103*, pp. 2–6.

68 Free Speech Union of Australia, *Submission 54,* pp. 2–5.

69 Mr Leon Zwier, Partner, Arnold Bloch Leibler, *Proof Committee Hansard,* 10 November 2026, p. 20.

2.62 The department explained that the definition in proposed section 25D:

> … capture[s] the most serious forms of online harm experienced by Australians … This definition is based on relevant criminal statutes, and concepts of harmful online material currently within scope of the Online Safety Act 2021. … The very serious and abhorrent nature of the material and conduct captured under this definition make it appropriate for application to all Australians, regardless of age.
>
> … It targets serious harm to a person's physical or mental health, with the legislation defining specific harms, based on unlawful conduct and material under Australian law. Serious harm is a legally high threshold for harm and requires more than ordinary distress, upset or transient adverse consequences, which means that taking offence, having hurt feelings or being subject to political disagreement would not meet this threshold. Instead, serious harm requires indicators such as medically recognised psychological or physical injury, significant impairment of a person's ordinary functioning, substantial economic consequences, or other objectively significant and demonstrable effects.[70]

2.63 Both the Office of the eSafety Commissioner and the department advised that there was no evidence that platforms were over-censoring content. When questioned about whether the Duty may have a chilling effect or whether the regulator may overregulate, the eSafety Commissioner responded:

> … what I would say is that the most overblocking we're seeing is in some of these companies eviscerating their trust and safety teams, not keeping humans in the loop and exclusively using AI for content moderation. I think it's a stretch to say that there would be a chilling effect here. I haven't seen any indication, particularly over the past two years, that companies are overcensoring. In fact, we in the Classification Review Board are being fought—and we've put in a submission against this—to make available to share and monetise online some of the postmortem Bondi footage and to reduce the classification. So what I would say is companies today are trying to show the maximum amount of material, no matter how harmful or hurtful it is to the Australian community.[71]

---

[70] The department, *Submission 130*, p. 5.

[71] Ms Julie Inman Grant, Commissioner, Office of the eSafety Commissioner, *Proof Committee Hansard*, 10 November 2026, p. 69.

2.64 Mr Richard Fleming, General Counsel, Office of the eSafety Commissioner, told the committee that overblocking and overcompliance were not its experience as a regulator:

> Overblocking and overcompliance aren't our experience at eSafety. That's just not what we see. The example I point to is that, as everyone on the committee would be aware, each of the digital platforms has an online hate policy in their terms of service, and there's been a whole lot of evidence presented to the royal commission around how they take either little or no action under that policy. If you look at those real-life examples as opposed to broader concerns, I think we can find that overblocking and overcompliance certainly are not what we see.[72]

2.65 The department similarly emphasised that the proposed Duty was not a duty to broadly remove content:

> … [I]t's not about deleting this content from the internet; it's about ensuring that children, while they're in their formative years, are protected from being exposed to content that could be harmful to them.[73]

Material and conduct that is harmful to children

2.66 Submitters and witnesses put forward various perspectives on the definition of material and conduct that is harmful to children, in proposed section 25E.

2.67 Ms Bannister supported the bill's acknowledgement of the diverse harms that can affect children, submitting that:

> I particularly welcome the Bill's recognition of harms that extend beyond material that may be obviously unlawful.
>
> Young people can experience serious psychological harm through repeated exposure to content and interactions that, when viewed individually, may not appear to meet a high threshold of severity.
>
> These can include bullying, humiliation, appearance-based comparisons, harmful body image messaging, disordered eating content and repeated exposure to material that normalises self-harm.
>
> The cumulative nature of these experiences is important.
>
> A child may not be harmed by one isolated comment, image or recommendation. However, repeated exposure over weeks or months, combined with peer relationships, personal vulnerabilities and offline circumstances, can contribute to substantial distress.[74]

---

[72] Mr Richard Fleming, General Counsel, Office of the eSafety Commissioner, *Proof Committee Hansard*, 10 November 2026, p. 69.

[73] Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, department, *Proof Committee Hansard*, 10 November 2026, p. 77.

[74] Ms Mia Bannister, *Submission 7*, p. 3.

2.68 Several inquiry participants advocated for the list of material and conduct that is harmful to children in proposed section 25E to be expanded.[75]

2.69 While reflecting positively on the bill's inclusion of 'categories of harm that children are protected from, in recognition of the unique vulnerabilities that children face in digital spaces', UNICEF Australia recommended expanding the categories to include 'risks from compulsive and/or addictive design, overuse, cumulative harms, and unforeseen and emerging harms from features or content'.[76]

2.70 Dr van Rijswijk suggested the inclusion of 'contact and solicitation risks, compulsive use, gambling-like mechanics, manipulative artificial intelligence companions and appearance-related harms'.[77] Additionally, the Alliance for Gambling Reform proposed that material or conduct that 'incites, encourages or grooms a child to gamble' and material containing 'simulated gambling' should be explicitly mentioned in proposed section 25E.[78]

2.71 Other inquiry participants expressed concern about the breadth of the categories of material and conduct in proposed section 25E and argued that they lacked clarity.[79] Concerns were raised regarding the following categories in particular—these are discussed below in turn:

- 'material or conduct that encourages or promotes hostile attitudes towards women or gender equality' (proposed paragraph 25E(1)(c));
- 'material or conduct that glorifies crime or encourages dangerous stunts or seriously harmful practices' (proposed paragraph 25E(1)(d)); and
- 'any other material or conduct, or combination of material and conduct, that may cause serious harm to children' (proposed paragraph 25E(1)(f)).

---

75 See, for example: Relationships Australia, *Submission 39*, p. 2; NATSIWA, *Submission 83*, [p. 6]; Trans Justice Project, *Submission 101*, p. 3; NFAW), *Submission 113*, p. 2; Working with Women Alliance, *Submission 134*, p. 9.

76 UNICEF Australia, *Submission 120*, pp. 1 and 2.

77 Dr Honni van Rijswijk, *Submission 6*, p. 38.

78 Alliance for Gambling Reform, *Supplementary Submission 60.1*, pp. 5–6. See also: Alliance for Gambling Reform, *Submission 60*, p. 1; Relationships Australia, *Submission 39*, p. 2.

79 See, for example: Google, *Submission 27*, [p. 5]; Consumer Choice Center, *Submission 42*, [p. 2]; Institute of Public Affairs, *Submission 56*, p. 4; Information Technology and Innovation Foundation (ITIF), *Submission 80*, p. 3; DIGI, *Submission 90*, p. 2; Australian Christian Lobby, *Submission 99*, p. 4; Canberra Declaration, *Submission 124*, p. 8; Liberty Victoria, *Submission 143*, [p. 4].

Proposed paragraph 25E(1)(c)

2.72 The committee heard concerns that the terms 'hostile attitudes' and 'gender equality' are undefined in the bill, creating uncertainty.[80] Meta acknowledged the importance of 'protecting young people from harmful misogynistic abuse, harassment and violence', but noted that:

> The challenge is to distinguish that harmful conduct from legitimate discussion about women's rights, religious beliefs and public policy … That broad formulation [in proposed paragraph 25E(1)(c)] does not itself explain when a contested political or religious view, or criticism of a social practice, crosses the line into harmful hostility. Without a clearer boundary, providers may face uncertainty about whether protecting children requires restricting their access to lawful debate.[81]

2.73 Several organisations voiced concerns that religious teachings and content may be captured by proposed paragraph 25E(1)(c).[82] For example, the Australian Catholic Bishops Conference submitted that:

> There is a real risk that longstanding religious teachings on matters of ethics and morality, human relationships and a whole range of other issues could be characterised by some as falling within this definition, notwithstanding that such teachings are well-established elements of a number of religious traditions, and form part of legitimate public discourse.[83]

2.74 Canberra Declaration, an organisation promoting Judaeo-Christian beliefs, cautioned that 'Christian teaching on marriage, sexuality, the sanctity of human life, and the created distinction between male and female' could be captured.[84]

2.75 On the other hand, members of the gender-based violence prevention sector expressed support for the inclusion of proposed paragraph 25E(1)(c). Teach Us Consent, an Australian charity committed to consent education and the prevention of sexual violence, submitted that the provision 'is crucial as it acknowledges how harmful it is to expose children to content or behaviours that are hostile toward women or the goal of gender equality'.[85]

2.76 Our Watch, an organisation working to support the prevention of violence against women and their children, stated that:

> Given the significant amount of time Australians spend online, reducing exposure to the promotion of gender inequality and hostile attitudes to

---

80 See, for example: DIGI, *Submission 90*, p. 15; Australian Catholic Bishops Conference, *Submission 62*, p. 5; Anglican Church, Diocese of Sydney, *Submission 63*, p. 12.

81 Meta, *Submission 73*, p. 8.

82 See, for example: Australian Catholic Bishops Conference, *Submission 62*, p. 5; Anglican Church, Diocese of Sydney, *Submission 63*, p. 3; Canberra Declaration, *Submission 124*, p. 11.

83 Australian Catholic Bishops Conference, *Submission 62*, p. 5.

84 Canberra Declaration, *Submission 124*, p. 11.

85 Teach Us Consent, *Submission 29*, [p. 5].

> women on online platforms is a critical opportunity for primary prevention of violence against women among people of all ages.[86]

2.77 The department explained the rationale behind proposed paragraph 25E(1)(c):

> Material or conduct that encourages hostile attitudes towards women and gender equality was specifically added to the Bill as a harm to children to address a growing body of evidence and feedback from stakeholders that this form of harm has long term social consequences linked to radicalisation and violence towards women.[87]

2.78 Departmental officer Mr Hyles similarly referred to a 'growing body of evidence' linking 'adolescent exposure to misogynistic attitudes to support for various forms of violent extremism'.[88] He emphasised that harmful online content can contribute to broader social harms, stating:

> Such content targets the promotion of hostility during a child's development rather than disagreeing over politics or policy and leads to the impacts of normalising of gender-based violence during schooling and physical and mental health concerns for Australians, particularly Australian girls and women.[89]

Proposed paragraph 25E(1)(d)

2.79 The AHRC noted that material and conduct that 'glorifies crime' within the meaning of proposed paragraph 25E(1)(d) 'could extend to material supporting peaceful protest where an aspect of the protest may constitute an offence under Commonwealth, state or territory law'. It also warned that '"seriously harmful practices" is too broad and may impose a disproportionate impact on freedom of expression'.[90]

2.80 DIGI submitted that proposed paragraph 25E(1)(d) 'could capture crime drama, true crime podcasts, some music genres and extreme sports content'.[91]

Proposed paragraph 25E(1)(f)

2.81 Some submitters expressed reservations about the phrase 'may cause serious harm to children' in proposed paragraph 25E(1)(f), with the AHRC stating that it 'does not clearly explain which practices are covered or how likely they must be to cause serious harm', thereby 'leav[ing] platforms to make those judgments,

---

86 Our Watch, *Submission 51*, p. 5.

87 The department, *Submission 130,* p. 5.

88 Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, the department, *Proof Committee Hansard,* 10 November 2026, p. 76.

89 Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, the department, *Proof Committee Hansard,* 10 November 2026, pp. 76–77.

90 Australian Human Rights Commission, *Submission 58*, pp. 20 and 22.

91 DIGI, *Submission 90*, p. 15.

creating a risk that they will restrict lawful expression based on unclear understandings of harm'.[92]

Departmental response

2.82 The department acknowledged that, in comparison to the 'legally high threshold' for seriously harmful material and conduct, the bill 'sets a lower bar for harms to children, recognising they are particularly vulnerable to online harm and require greater protections'.[93]

2.83 Mr Hyles of the department indicated that the proposed definition of material and conduct that is harmful to children reflects the views expressed during the department's stakeholder consultations:

> The general sense of the feedback that we've had from a range of advocates and industry groups et cetera was really around that idea that children do need to be protected online, they do need to have the opportunity to develop in a safe environment, and those kinds of platforms clearly aren't creating that opportunity at the moment.[94]

Excluded material

2.84 Inquiry participants were broadly supportive of the bill's provision (in proposed section 25F) for certain material to be excluded from the harm definitions in proposed sections 25D and 25E.[95] The AHRC, for example, stated, 'The exclusions in s 25F are a substantial improvement [from the exposure draft] and provide important safeguards for freedom of expression'.[96]

2.85 Bravehearts, a non-government organisation combating child sexual abuse and exploitation, highlighted the importance of having exclusions for particular material:

> Exclusions for research, educational material, public health and safety information, and content in the public interest is critical. These protections are particularly important for organisations working in child sexual abuse prevention and victim-survivor support. Educational resources addressing grooming, sexual exploitation, consent, harmful sexual behaviour and help-seeking may necessarily discuss sensitive or confronting subjects.[97]

---

92 Australian Human Rights Commission, *Submission 58*, p. 23. See also, DIGI, *Submission 90*, p. 15; Anne Twomey, Professor Emerita, *Submission 132*, p. 4.

93 The department, *Submission 130*, p. 5.

94 Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, the department, *Proof Committee Hansard*, 10 November 2026, p. 72.

95 See, for example: Dr Honni van Rijswijk, *Submission 6*, p. 67; With You We Can, *Submission 38*, pp. 2 and 10; Our Watch, *Submission 51*, pp. 5–6; Australian Human Rights Commission, *Submission 58*, p. 7; NATSIWA, *Submission 83*, [p. 4].

96 Australian Human Rights Commission, *Submission 58*, p. 7.

97 Bravehearts, *Submission 89*, [p. 5].

2.86 Evidence to the inquiry largely focused on the following categories of excluded material:

- material that is necessary for, or of assistance in, protecting or promoting public health and safety (proposed paragraph 25F(1)(g));
- material that is necessary for, or of assistance in, reducing harms to individuals (proposed paragraph 25F(1)(h)); and
- material that is in the public interest (proposed paragraph 25F(1)(i)).

2.87 Inquiry participants also commented on the omission of an exclusion for religious material.

Public health and safety material and harm reduction material

2.88 While submitters and witnesses welcomed the bill's exclusion of public health and safety material and harm reduction material from the harm definitions, they called for further measures to protect access to this material.[98]

2.89 Members of the alcohol and other drugs sector gave evidence of the current challenges involving public health information being suppressed on online platforms due to automated content moderation, and expressed concern that the exclusion in proposed section 25F will not do enough to safeguard against over-capture.[99]

2.90 The National Centre for Clinical Research on Emerging Drugs which coordinates the Prompt Response Network, a national project bringing together early warning networks regarding emerging drugs of concern, submitted that:

> Network members are already having their content restricted or removed, or are self-censoring and therefore obfuscating clear public health messaging in order to evade detection by over-reaching automated moderators. As one member described, this has "significantly impacted our ability to spread the reach of essential public health warnings". This highlights how moderation can disrupt public health communications and create additional work for organisations with limited resources.[100]

---

[98] See, for example: National Drug Research Institute, Curtin University, *Submission 42*, [pp. 1–2]; Alcohol and Drug Foundation, *Submission 49*, pp. 1–3; Australian Alcohol and Other Drugs Council, *Submission 87*, [pp. 1–2]; ARACY - Australian Research Alliance for Children and Youth, *Submission 88*, [p. 6]; National Association of People with HIV, *Submission 114*, pp. 1–6; The Matilda Centre for Research in Mental Health and Substance Use, *Submission 115*, p. 3; Alcohol Tobacco and Other Drug Association ACT, *Submission 119*, [p. 1]; Your Community Health, *Submission 122*, pp. 1–3; South Australian Network of Drug and Alcohol Services (SANDAS), *Submission 152*, [pp. 1–2].

[99] See, for example: Alcohol and Drug Foundation, *Submission 49*, pp. 2–4; Bluelight Communities Ltd, *Submission 91*, [pp. 1–2]; Australian Alcohol and Other Drugs Council, *Submission 87*, [p. 2]; Alcohol Tobacco and Other Drug Association ACT, *Submission 119*, [p. 1].

[100] National Centre for Clinical Research on Emerging Drugs, *Submission 117*, [p. 2].

2.91 The Penington Institute cautioned that the bill's current settings may 'incentivise platforms to err on the side of removing content whenever its subject matter is considered sensitive', which may lead to 'material intended to help people make safer decisions, prevent overdose or access health services … be[ing] restricted alongside genuinely harmful content'.[101]

2.92 These concerns were echoed by health, harm reduction, LGBTQIA+ advocacy, sex worker and civil liberties organisations and researchers.[102] For example, the Scarlet Alliance, the national peak body for sex workers, argued that platforms would be incentivised to remove more content because while they face large penalties for failing to remove or restrict harmful material, there are no penalties for removing lawful material and no requirements to offer any right of appeal against content-removal decisions. The Scarlet Alliance continued:

> The excluded material set out in s 25F is a definition, not a protection. It tells platforms what they are not required to act against. It does not oblige them to leave that material up, or give anyone whose 'excluded material' is removed a way to get it back.[103]

2.93 Proposals to strengthen protections in the bill for public health and harm reduction material include the establishment of a positive duty of care requiring platforms to protect access to such material and requiring platforms to offer clear and effective appeal and complaints mechanisms.[104]

Public interest material

2.94 A number of inquiry participants commented on the uncertainty of the meaning of 'material that is in the public interest' for the purposes of the exclusion in proposed section 25F.[105]

---

101 Penington Institute, *Submission 86*, [p. 1].

102 See, for example: QNews, *Submission 77*, [pp. 1–4]; Trans Justice Project, *Submission 101*, pp. 2–3; Health Equity Matters, *Submission 112*, [pp. 1–2]; National Association of People with HIV, *Submission 114*, pp. 1–5; Scarlet Alliance, National Sex Workers Association, *Submission 121*, pp. 7–8; Repro Uncensored, *Submission 125*, [pp. 2–5]; The Twelve (HIV, STI and BBV joint sector submission), *Submission 164*, pp. 1–12.

103 Scarlet Alliance, National Sex Workers Association, *Submission 121*, pp. 7–8.

104 See, for example: National Drug Research Institute, Curtin University, *Submission 42*, [p. 2]; Alcohol and Drug Foundation, *Submission 49*, pp. 1–4; QNews, *Submission 77*, [pp. 2 and 4]; Penington Institute, *Submission 86*, [p. 2]; Australian Alcohol and Other Drugs Council, *Submission 87*, [p. 2]; National Association of People with HIV, *Submission 114*, pp. 1–6; The Matilda Centre for Research in Mental Health and Substance Use, *Submission 115*, p. 3; Alcohol Tobacco and Other Drug Association ACT, *Submission 119*, [pp. 1–2]; Your Community Health, *Submission 122*, pp. 1–5.

105 See, for example: The Information Rights Project, *Submission 37*, p. 3; Australian Human Rights Commission, *Submission 58*, p. 7; Australians vs. The Agenda, *Submission 98*, p. 3; Anne Twomey,

2.95 TikTok Australia expressed concern that that the exclusion framework could result in different treatment of substantially similar content depending on who publishes it, providing the following example:

> A professional news provider may benefit from a clearly identified statutory exclusion, while an individual creator publishing substantially similar commentary may need to rely on more general exclusions, including the public interest provision.[106]

2.96 TikTok Australia added that the lack of a detailed test for determining when material is 'in the public interest' means that 'services will initially need to make these judgments, and apply them for their machine-learning moderation models'.[107]

2.97 The Women's Services Network, while welcoming the exclusion for public interest material, recommended that the term should be defined, and accompanied by guidance and examples. It also recommended that online services should be required to:

> … explain how automated moderation systems will apply to material in the public interest to ensure they do not disproportionately restrict the content or accounts of individuals and communities experiencing systemic discrimination.[108]

2.98 A departmental representative observed that the Online Safety Act already contains a reference to material that is 'in the public interest' and noted that the bill would simply carry over that term.[109]

Professor Emerita, *Submission 132*, p. 3; Australian Muslim Advocacy Network, *Submission 157*, p. 17.

106 TikTok Australia, *Submission 28*, p. 4.

107 TikTok Australia, *Submission 28*, p. 4.

108 Women's Services Network, *Submission 82*, pp. 13–14. See also, Bravehearts, *Submission 89*, [p. 5].

109 Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, the department, *Proof Committee Hansard*, 10 November 2026, p. 77.

Religious material

2.99 Several submitters drew the committee's attention to the omission of religious material from the list of excluded material in proposed section 25F.[110] While some organisations noted that the exclusions for educational or public interest material may cover religious teaching, they raised concerns that the protection is not guaranteed.[111] The Coptic Orthodox Diocese of Sydney & Affiliated Regions, for example, stated that:

> It is not clear to us whether the matters listed in s 25F would, in practice, cover worship, sermons and scripture. Lawful preaching and religious education deserve the same certainty as other excluded material.[112]

2.100 The Anglican Church, Diocese of Sydney highlighted the risk of over-censorship of religious teaching and content as a result of platforms using 'AI Agents to comply with a digital duty to moderate content'. In addition, it argued that:

> To avoid massive regulatory fines, platforms will inevitably default to extreme caution. Being commercially incentivised to do so, they will proactively take down completely lawful, benign speech that looks even remotely controversial, as has been evidenced in the UK under a similar 'digital duty of care'. The legislation thus sets up in competition the interests of religious freedom as opposed to the private commercial interests of business owners, placing into the hands of the latter the obligation to police permissible speech in the online forum according to broad, imprecise standards of harm.[113]

---

110 See, for example: Coptic Orthodox Diocese of Sydney & Affiliated Regions, *Submission 46*, p. 1; Australian Catholic Bishops Conference, *Submission 62*, p. 4; Anglican Church, Diocese of Sydney, *Submission 63*, pp. 13–14; Australian Christian Lobby, *Submission 99*, p. 7; Freedom for Faith, *Submission 109*, [p. 2]; Canberra Declaration, *Submission 124*, p. 11.

111 Anglican Church, Diocese of Sydney, *Submission 63*, p. 14; Australian Christian Lobby, *Submission 99*, p. 7.

112 Coptic Orthodox Diocese of Sydney & Affiliated Regions, *Submission 46*, p. 1.

113 Anglican Church, Diocese of Sydney, *Submission 63*, pp. 4–5.

2.101 Representing the Anglican Church, Diocese of Sydney at a public hearing, Dr Michael Stead, Bishop of South Sydney, explained the concerns around the breadth of harm definitions in the bill and the absence of an explicit protection for religious communication:

> We're very concerned that the scheme of content moderation is going to have the effect of censoring religious teaching, especially biblical teaching, on contentious social issues about sexual ethics, gender identity, which we think will come within the definitions in section 25E and potentially within 25D—the breadth of the definitions there—combined with the absence of any other recognitions of the importance of religious freedom and free speech more broadly in the exemptions in 25F and the new 26A overriding principles.[114]

Departmental response

2.102 The department explained that the list of excluded material in proposed section 25F is intended 'to ensure that lawful and informative communications are not captured by the Duty of Care'. The department noted that the categories were:

> … informed by stakeholder feedback on the Exposure draft and drew from exclusions in other legislative frameworks such as the *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021* which informed the definition of news material and professional news material.[115]

Design features with negative behavioural impacts

2.103 The committee heard a variety of views on proposed section 25G regarding design features that have negative behavioural impacts.

Expanded protections against harmful design features

2.104 Some inquiry participants argued for the list of design features to be expanded to capture additional types of harmful features and for stronger prohibitions against these features.

2.105 Consumer policy and advocacy groups recommended that 'dark patterns' (design features used by online platforms purely to steer people's choices and experiences), such as forced continuity and scarcity cues, 'can play a significant role in impeding a consumer's control and choice online' and should therefore be explicitly recognised in proposed section 25G.[116]

---

[114] Dr Michael Stead, Bishop of South Sydney, Anglican Church, Diocese of Sydney, *Proof Committee Hansard*, 10 November 2026, p. 15.

[115] The department, *Submission 130*, p. 6.

[116] Consumer Policy Research Centre, CHOICE and Consumer Action, *Submission 53*, pp. 1–2.

2.106 Submitters also proposed that the list of design features in proposed section 25G should include 'endless scrolling, likes and follower counts, and disappearing content'[117] and 'autoplay, re-engagement prompts, contact recommendation, location sharing, live-streaming, simulated companionship features and variable rewards'.[118]

2.107 The committee heard proposals that recommender algorithms should be switched off by default for children. Ms Bannister, for example, stated:

> I support algorithmically personalised feeds being switched off by default for children, with age-appropriate safeguards that do not rely on a child identifying risks and navigating complex settings.
>
> Children should not have to opt out of potentially harmful engagement-driven systems.[119]

2.108 The Wellbeing and Prevention Coalition in Mental Health went further to suggest that engagement-maximising algorithms should be prohibited for users under 16 years of age, to reflect that 'young people are still developing impulse control, emotional regulation, and identity, which can make them more susceptible to persuasive and engagement-based service features'. It also suggested that 'service features that exploit vulnerabilities in children and young people: autoplay without stopping points, variable-ratio reinforcement (streaks, engagement rewards), social comparison metrics (likes, follower counts), notification cadence designed for re-engagement' should be prohibited for users under 16.[120]

2.109 Under proposed subsection 25G(2), the Minister would have the power to determine by legislative instrument that additional design features have negative behavioural impacts, beyond those features specifically listed in proposed subsection 25G(1). The bill's Explanatory Memorandum notes that this would:

> … allow the Minister to capture additional social media services which are not to operate for children in Australia under the age of 16, if they incorporate features that have negative behavioural impacts.[121]

---

117 Women's Services Network, *Submission 82*, p. 15.

118 Dr Honni van Rijswijk, *Submission 6*, p. 40.

119 Ms Mia Bannister, *Submission 7*, p. 5. See also, Dr Honni van Rijswijk, *Submission 6*, p. 41; Women's Services Network, *Submission 82*, p. 15.

120 Prevention United, *Submission 10*, p. 9.

121 The bill, EM, p. 62.

Certain design features deemed to have negative behavioural impacts

2.110 Some inquiry participants argued that design features should not be presumed to be harmful and pointed out their potential positive uses.[122] Snap Australia, for example, argued that recommender and logged-in features can support safety by recommending child-safe content or safety and wellbeing resources and by providing parental alerts to minors.[123]

2.111 Duolingo submitted that design features such as streaks, notifications, and gamification can be used positively to motivate learning, and proposed that an exclusion for solely or primarily educational services be applied to the bill's provisions concerning design features.[124]

2.112 SBS raised concerns that the bill 'could impact the effectiveness of design features through which audiences discover SBS content, including recommendation tools' and undermine the 'availability and discoverability of public service media'.[125] Similarly, Free TV Australia called for an exclusion in the bill for recommendation functions of broadcaster online services which 'help audiences find programs relevant to them from within substantial content catalogues'.[126] Further, Streaming for Australia expressed concern that logged-in features could be at risk, noting that users generally need to log in to access content and enable certain essential parental safeguards, including Kids Profiles, maturity restrictions and PIN protection.[127]

---

122 See, for example: TikTok Australia, *Submission 28*, p. 6; BCA, *Submission 34*, p. 5; DIGI, *Submission 90*, pp. 2, 8–9 and 11; IGEA, *Submission 93*, pp. 2 and 6; Consumer Electronics Suppliers Association, *Submission 160*, pp. 4–5.

123 Snap Australia, *Submission 40*, p. 5.

124 Duolingo, *Submission 79*, [pp. 1 and 6].

125 SBS, *Submission 133*, p. 2. See also, pp. 5–6.

126 Free TV Australia, *Submission 67*, pp. 1–2. See also, Ms Bridget Fair, Chief Executive Officer, Free TV Australia, *Proof Committee Hansard*, 10 November 2026, pp. 25 and 28; Mr Michael Coonan, Director, Public Policy, Free TV Australia, *Proof Committee Hansard*, 10 November 2026, pp. 25–26.

127 Streaming for Australia, *Submission 131*, [pp. 2–3]; Mr Paul Muller, Convener, Streaming for Australia, *Proof Committee Hansard*, 10 November 2026, pp. 27 and 29.

2.113 DIGI argued that rather than presuming certain design features are harmful, they should be assessed through risk assessments:

> Section 25G should be removed and design features assessed through each service's risk assessment.
>
> … If section 25G is retained, design feature obligations should be met through risk assessment, guidelines should take the same approach after public consultation, and the Explanatory Memorandum should confirm that services need not restrict features or establish users' ages unless their risk assessment shows this is needed.[128]

2.114 The bill's Explanatory Memorandum recognises that:

> While design features can be agnostic or neutral aspects of a service, their design and interface can incentivise users to engage with the service in ways that may be harmful to themselves or others.[129]

2.115 The Explanatory Memorandum cites evidence that recommender systems 'may expose end-users to harmful material, including self-harm, suicidal ideation, incitement to violence, negative body image and eating disorder material and behaviours', while feedback features 'can impact self-acceptance and trigger ruminative and anxious behaviours'.[130]

Differential standards for children and adults

2.116 Some inquiry participants queried whether differential standards regarding design features should apply to children and adults.

2.117 The ADM+S posited, 'A person's vulnerability to harms arising from design features does not cease automatically upon reaching adulthood' and recommended that the bill should 'require that all persons in Australia are protected from serious harms associated with access or exposure to design features of online services'.[131]

2.118 Dr van Rijswijk made a similar point, arguing that limiting the protection from harmful design features to children under the age of 16 is 'an arbitrary line' and that the protection should be extended to all persons in Australia:

> A recommender system that amplifies suicide and self-harm content does not become benign on a user's sixteenth birthday, and the engagement-optimising architecture that produces the harm is identical across age groups.[132]

---

128 DIGI, *Submission 90*, p. 11.

129 The bill, EM, p. 62.

130 The bill, EM, pp. 63–66.

131 ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, p. 4.

132 Dr Honni van Rijswijk, *Submission 6*, pp. 36–37. See also, Gender Justice Australia, *Submission 85*, p. 7.

2.119 In comparison, the AHRC supported an adult-child bifurcated model of digital regulation because 'the online experiences of children and adults are different'. The AHRC added that a 'bifurcated model will avoid the application of restrictive child-settings to adults'.[133]

2.120 The department noted that the application of the bill's provisions regarding design features to children under the age of 16 'reinforces the social media minimum age framework'.[134]

Risk assessments

2.121 Submitters and witnesses provided evidence on the requirements relating to risk assessments as set out in proposed section 27.

Risks to be assessed

2.122 Inquiry participants put forward suggestions regarding the risks that online service providers should be required to assess as part of risk assessments. These included risks to human rights, children's rights and groups sharing protected characteristics, and risks of gender-based violence and cumulative harms.[135]

2.123 The Human Rights Law Centre, for instance, recommended that:

> Section 27 of the Bill is amended to require that Risk Assessments explicitly consider risks to human rights, including harms arising from online attacks based on protected characteristics.[136]

2.124 The AHRC also argued in favour of human rights-based risk assessments, stating that:

> The Bill should be amended to expressly require that risk assessments must address cumulative and contextual factors that may contribute to harm, including the interaction between content, amplification mechanisms and platform design features. Human rights-based criteria or principles should guide proportionate risk mitigation, including respect for privacy, safety and freedom of expression (which includes the right to seek and receive information).[137]

---

133 Australian Human Rights Commission, *Submission 58*, p. 12.

134 The department, *Submission 130,* p. 6.

135 See, for example: International Justice Mission Australia, *Submission 50*, p. 7; Human Rights Law Centre, *Submission 57*, pp. 10-11; Australian Human Rights Commission, *Submission 58*, p. 25; Women's Services Network, *Submission 82*, p. 10; NATSIWA, *Submission 83*, [p. 6]; Gender Justice Australia, *Submission 85*, p. 2; Bravehearts, *Submission 89*, [p. 2]; UNICEF Australia, *Submission 120*, p. 3; Arnold Bloch Leibler, ECAJ, ZFA, NSW JBOD, NCJWA, JCCV, Dor Foundation & AIJAC, *Submission 128*, p. 2; Working with Women Alliance, *Submission 134,* p. 5.

136 Human Rights Law Centre, *Submission 57*, p. 11.

137 Australian Human Rights Commission, *Submission 58*, p. 25.

2.125 The National Foundation for Australian Women (NFAW), an organisation committed to protecting the interests and human rights of Australian women, observed that proposed section 27:

> … does not expressly require providers to assess whether particular groups are more exposed to that risk or likely to experience more severe impacts. A formally neutral risk assessment may overlook the gendered operation of online harm. It may also fail to identify how gender-based violence or discrimination affects people differently because of disability or race.[138]

2.126 The NFAW and others argued that an assessment of reasonably foreseeable risks of gender-based violence should be mandatory.[139] Ms Anna Brown, Chief Executive Officer of Equality Australia, also put forward an argument for a broadening of what constitutes seriously harmful conduct:

> We absolutely see the need to strengthen and address the online harm that our communities experience, with some modifications to this bill. Our proposal is that the bill be amended so that, in the list of seriously harmful conduct, we include, in section 25D—at the moment there's no express capture of targeted attacks against our communities, so it's actually failing to respond adequately to the escalating and deeply concerning situation for our communities. We're proposing that we add—and this is obviously in our submission. Section 25D could be amended to include an additional provision, and that is—we've got a couple of options there—material or conduct that vilifies or dehumanises a targeted group. There we're actually suggesting that it's not just LGBTQI+ people but other communities as well—race, religion, disability, nationality, national ethnic origin—and, importantly, we're proposing that the threshold still be required that it's reasonably likely that material or conduct may lead to serious harm. I just wanted to point out that threshold issue.[140]

Strengthening the effectiveness of risk assessments

2.127 The committee heard various proposals for strengthening the effectiveness of risk assessments, including through ensuring the competency of assessors and requiring transparency and independent auditing.

---

138 NFAW, *Submission 113*, p. 6.

139 See, for example: Older Women's Network NSW, *Submission 76*, [p. 2]; Women's Services Network, *Submission 82*, p. 10; NATSIWA, *Submission 83*, [p. 5]; Gender Justice Australia, *Submission 85*, p. 2; NFAW, *Submission 113*, p. 2; Working with Women Alliance, *Submission 134*, pp. 5–6; Dr Gemma Killen, Executive Director, Working with Women Alliance, *Proof Committee Hansard*, 10 November 2026, p. 3.

140 Ms Anna Brown, Chief Executive Officer, Equality Australia, *Proof Committee Hansard*, 10 November 2026, p. 4.

2.128 The Australian Computer Society (ACS), the professional society for Australia's technology profession, noted that particular expertise, for example in cyber security, privacy, data governance and ethics, may be required to assess digital systems. The ACS stated that:

> Where assessments involve complex technologies, including AI, algorithmic systems and recommender systems, organisations should be able to demonstrate that relevant assessments have been undertaken by people with appropriate technical competencies and professional expertise.[141]

2.129 The ACS argued that the eSafety Commissioner should be empowered to 'recognise relevant professional standards and certifications [for risk assessors], while allowing equivalent assurance through other approaches'.[142]

2.130 Dr van Rijswijk expressed concern that the absence of a requirement for risk assessments to be published or independently audited may result in 'cosmetic compliance' whereby regulated entities are encouraged simply 'to produce a document' rather than genuinely change its systems and processes. Dr van Rijswijk claimed that, conversely, 'Publication and audit convert the assessment into a document the provider must be prepared to defend'.[143]

2.131 UNICEF Australia similarly suggested that risk assessments could be made subject to 'independent, neutral third-party audits or verification to strengthen the integrity of online service providers' self-assessments'.[144]

2.132 The eSafety Commissioner, while supporting the bill's proposed risk assessment framework, remarked:

> eSafety is concerned that services may maliciously comply with the risk assessment framework by providing lengthy risk assessments without meaningful substance, minimising or mischaracterising risk ratings and effectively delaying safety uplift.[145]

---

141 Australian Computer Society (ACS), *Submission 43*, p. 2.

142 ACS, *Supplementary Submission 43.1*.

143 Dr Honni van Rijswijk, *Submission 6*, p. 47.

144 UNICEF Australia, *Submission 120*, p. 4.

145 eSafety Commissioner, *Submission 129*, p. 15.

2.133 To guard against malicious compliance and address inadequate risk assessments, the eSafety Commissioner submitted that it 'would greatly benefit from the clear power to require reassessment, an independent audit, and to seek authorisation for remote viewing powers'.[146] Referring to the potential power to require third-party audits, the eSafety Commissioner stated:

> eSafety is committed to ensuring this does not impose unnecessary regulatory burden or expenses on regulated entities who are complying with their obligations but provides a critical tool to further validate platform claims and provide platforms an additional mechanism to demonstrate compliance.[147]

Concerns regarding regulatory burden

2.134 Several inquiry participants raised concerns regarding the regulatory burden imposed by the risk assessment requirements in proposed section 27.

2.135 For example, Independent Schools Australia, the national peak body for the independent school sector, called for schools to be exempted from risk assessment obligations, arguing that they would:

> … create significant compliance work. A routine change to a learning platform, student portal or artificial intelligence tool might potentially trigger a new assessment. The additional workload on schools, particularly smaller, regional and remote schools would be disproportionate and divert resources away from teaching and learning for little, if any, benefit.[148]

2.136 The Internet Association of Australia, whose members include small to medium sized internet service providers who provide internet carriage services (ICS), claimed that ICS should be 'explicitly carved out from s 27' because:

> … imposing obligations for ISPs to conduct annual risk assessments have little end-user benefit, compared to the cost for providers. Conducting annual risk reviews is no small task for resourced [sic] constrained telco operators, many of whom also face overlapping risk assessment obligations under the *Security of Critical Infrastructure Act 2021*.[149]

---

146 eSafety Commissioner, *Submission 129*, p. 15.

147 eSafety Commissioner, *Submission 129*, p. 7.

148 Independent Schools Australia, *Submission 116*, p. 10.

149 Internet Association of Australia, *Submission 127*, p. 4.

2.137 Other inquiry participants argued for exemptions for low-risk small business online services[150] and internet access services and SMS/MMS services.[151] In arguing for a statutory exemption, the Council of Small Business Organisations Australia (COSBOA) submitted that the preparation of formal written risk assessments may involve 'external advice, additional costs and ongoing administrative work' for small businesses without dedicated compliance or legal resources which are disproportionate to the risks that the service presents.[152]

2.138 Noting the potential compliance burdens for small independent studios in the Australian video games industry, IGEA recommended that 'eSafety should be able to prescribe streamlined assessments for low-risk services'.[153]

2.139 In relation to the eSafety Commissioner's power under proposed section 27 to make a legislative instrument outlining additional risk assessment requirements, the department submitted that it:

> … expects that the Commissioner will determine the form or forms of risk assessments that will prescribe requirements for low through to high-risk entities. This is expected to mitigate the regulatory burden on very low and low-risk entities, which is intended to be minimal and will likely only require answering a small number of questions to confirm they do not host or enable higher risk material, conduct or features.[154]

2.140 The eSafety Commissioner confirmed that it envisaged:

> … the framework would take a risk-based and proportionate approach, enabling services to tailor their risk assessment processes to the nature and level of risk presented by their service. This could include differentiated expectations for lower-risk services, while requiring additional assessment and mitigation measures where services incorporate higher-risk features, functionalities or design elements. This approach would reduce unnecessary compliance burdens on lower-risk services, and ensure that regulatory obligations are commensurate with the likelihood of harm.[155]

---

150 Council of Small Business Organisations Australia (COSBOA), *Submission 65*, pp. 1 and 3–4.

151 Australian Telecommunications Alliance, *Submission 66*, pp. 6–7.

152 COSBOA, *Submission 65*, p. 3. See also, Mrs Skye Cappuccio, Chief Executive Officer, COSBOA, *Proof Committee Hansard*, 9 November 2026, pp. 56–58.

153 IGEA, *Submission 93*, p. 6.

154 The department, *Submission 130*, p. 7.

155 eSafety Commissioner, *Submission 129*, p. 16.

2.141 At the hearing, the eSafety Commissioner provided further detail:

> Essentially, risk assessments are really important. We want to make sure that we're learning from the templating that we've done and the manner and form of the transparency reports. We want to make sure that any risk assessments we get aren't unduly burdensome on the particular regulatory target but don't end up being administrative nightmares for us, so that we can actually focus on enforcement. And, of course, as a small regulator we always focus on the high-risk, high-harm targets. If you look at the universe of websites, platforms and services that our codes and standards currently cover, they're literally in the millions. So what I would say to you is we're not focused on small businesses that may have a web presence, or religious institutions and the like. We're concerned about those high-risk, high-harm sites, like those that are nudifying or chat roulette sites—
>
> … We've met with some small-business groups to give them a degree of comfort, but we've also already thought about how we might make clearer in regulatory guidance the criteria we would be looking at in terms of capture.[156]

2.142 Mr Fleming added:

> As you would have seen from the bill and the EM, the whole idea is to have a general uplift in terms of online harm. Getting to that point requires a balance of a whole range of issues, and part of that, as you say, is making sure that those that are lower risk face the least amount of red tape possible. The first thing that we will be doing is bringing out guidance, and that's how we interpret some of the provisions of the act, and that will facilitate compliance. The second thing we'll be doing, as is required by the act, is putting out a statement of monitoring and enforcement priorities. That's something that's required, as I say, in the act. And we'll be focusing on some of the lower risk features to try and identify for people what we expect for the lowest risk platforms. The kinds of criteria we're looking at, and it's early days, are where there's no user interaction, where there's no user messaging, where there's no interaction between adults and children—those kinds of features—and where there are no AI chatbots. They're the kinds of things we'll be looking at to point towards the lowest risk. We'll be engaging through a consultation process and we'll be engaging with small business again to make sure that we get those settings right.[157]

User empowerment tools

2.143 The committee heard a range of perspectives on the provisions in proposed section 27A regarding user empowerment tools.

---

[156] Ms Julie Inman Grant, Commissioner, Office of the eSafety Commissioner, *Proof Committee Hansard*, 10 November 2026, pp. 62–63.

[157] Mr Richard Fleming, General Counsel, Office of the eSafety Commissioner, *Proof Committee Hansard*, 10 November 2026, p. 63.

2.144 An Assistant Secretary within the department explained that the provisions would facilitate the implementation of the Australian Government's My Feed, My Way initiative which aims to offer users more choice over content recommended by their social media feeds:

> The government has … announced its 'My Feed, My Way' initiative. That's squarely allowed for and built into the legislation to give users choice. We've currently got a draft out at the moment and are doing consultation on that. We're getting feedback through that process. That is a legislative instrument, so in turn it will be subject to parliamentary scrutiny. But we're hearing messages that people want control. They want choice.[158]

2.145 Teach Us Consent commended the provision in the bill for user empowerment tools, noting that an 'opt-in feature for algorithms on social media platforms' would be a 'world-first reform'. Teach Us Consent added that:

> The user empowerment tool proposed in this bill, if adopted, will be one of the first consent-based frameworks for online safety.[159]

2.146 Similarly, the QUT Digital Media Research Centre articulated strong support for user empowerment tools:

> … which present an important opportunity to give Australians greater understanding of and control over their experiences of online platforms, apps and services, including how user behaviour interacts with platform systems.[160]

2.147 The QUT Digital Media Research Centre supported the inclusive definition of 'user empowerment tool' in proposed subsection 27A(5), noting that:

> In principle, as part of providers' overarching responsibility for safety-by-design, user empowerment tools should relate to the full range of providers' obligations under the duty of care. Given the range of online safety issues to be addressed, the scope of design features to which user empowerment tools would relate must extend beyond content feeds to automated content moderation and reporting, user engagement mechanisms, safety features, and advertising systems.[161]

2.148 Nonetheless, submitters and witnesses held differing views on whether the requirements regarding user empowerment tools are proportionate, considering the potential implications for online service providers, and on the scope of ministerial powers in relation to these tools.[162]

---

158 Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch, the department, *Proof Committee Hansard,* 10 November 2026, p. 74.

159 Ms Chanel Contos, Chief Executive Officer and Founder, Teach Us Consent Global, *Proof Committee Hansard,* 9 November 2026, p. 8.

160 QUT Digital Media Research Centre, *Submission 70*, [p. 7].

161 QUT Digital Media Research Centre, *Submission 70*, [p. 8].

162 See, for example: Relationships Australia, *Submission 39*, pp. 12–13; GetUp, *Submission 149*, pp. 2–3.

Potential implications for online service providers

2.149 Some inquiry participants commented that proposed section 27A may have unintended consequences for online service providers. SBS registered its concern that 'the provision could impose significant implementation costs', through requiring changes to recommendation systems and user interfaces, 'while inadvertently reducing the discoverability of public service media'.[163] SBS observed that:

> … tools that significantly alter or disable recommendation systems could reduce the visibility of SBS journalism, educational content and programming, including content delivered through SBS's multilingual services for audiences with limited English proficiency.
>
> … Safeguards should therefore be included to ensure user empowerment measures do not inadvertently diminish the discoverability, prominence or accessibility of public service media content, including content and services provided by SBS.[164]

2.150 The potential commercial impacts of user empowerment tools on small businesses were also raised in evidence to the inquiry, with COSBOA noting the importance of social media, search and online marketplaces as channels for small businesses to reach customers:

> Depending on [the] design and uptake [of user empowerment tools], controls could change organic reach, referral traffic, advertising expenditure or the relative visibility of established and emerging businesses. The magnitude and distribution of these effects have not been established.[165]

2.151 Match Group, the company behind online dating services such as Tinder and Hinge, argued that personalisation through recommender systems is a 'central feature' of dating services and that '[r]equiring a generic opt-out or non-personalised alternative without regard to functionality could substantially reduce utility without a corresponding safety benefit'.[166] Match Group recommended amendments to proposed section 27A to distinguish between 'recommender systems that amplify potentially harmful material' and 'systems that help users discover content or people they actively seek, including personalised streaming recommendations and dating matches'.[167]

---

163 SBS, *Submission 133*, p. 6.

164 SBS, *Submission 133*, p. 7.

165 COSBOA, *Submission 65*, p. 2. See also, Snap Australia, *Submission 40*, p. 9.

166 Match Group, *Submission 92*, p. 4.

167 Match Group, *Submission 92*, p. 5.

Ministerial powers in relation to user empowerment tools

2.152 Several inquiry participants raised concerns about the proposed breadth of the Minister's power to make legislative instruments requiring online service providers to offer user empowerment tools and prescribing requirements in relation to these tools.[168]

2.153 The FSU, for example, argued that proposed section 27A 'provides far too much power to the Minister to control the operation of individual platforms, as well as to engage in censorship'.[169] Academics from RMIT University also criticised the extent of 'discretionary policymaking power' vested in the Minister.[170]

2.154 Google recommended removing the Minister's rule-making power in proposed section 27A, arguing that the Australian Government's My Feed, My Way initiative could instead be implemented through direct amendments to the Online Safety Act. Google considered that future user empowerment tools could also be established in primary legislation to allow for appropriate scrutiny.[171]

2.155 Other submitters proposed additional safeguards should the Minister's power to prescribe user empowerment tools be retained. For example, it was suggested that public consultation should be made a statutory requirement for legislative instruments made under proposed section 27A,[172] and that instruments should be 'backed by published evidence of effectiveness'.[173]

---

168 See, for example: Institute of Public Affairs, *Submission 56*, pp. 5–6; DIGI, *Submission 90*, pp. 10–11; Mrs Mia Garlick, Regional Director, Policy, Meta, *Proof Committee Hansard*, 9 November 2026, p. 45; Mr Chris Merritt, Vice President, Rule of Law Institute of Australia, *Proof Committee Hansard*, 9 November 2026, p. 71.

169 Free Speech Union of Australia, *Submission 54*, p. 8.

170 Associate Professor Darcy W. E. Allen and Professor Chris Berg, *Submission 118*, [p. 1].

171 Google, *Submission 27*, [p. 3]. See also, Australian Human Rights Commission, *Submission 58*, p. 24.

172 See, for example: Snap Australia, *Submission 40*, p. 9; Australian Human Rights Commission, *Submission 58*, p. 24; DIGI, *Submission 90*, p. 11; Internet Association of Australia, *Submission 127*, p. 6.

173 DIGI, *Submission 90*, p. 11.

2.156 In comparison, the ADM+S strongly supported the Minister's proposed powers to make legislative instruments, arguing that the flexibility to prescribe and tailor user empowerment tools to different kinds of online services is critical to respond to evolving technologies.[174] The ADM+S explained that:

> … technologies shift over time, and the ability to respond through legislative instruments can (1) ensure user empowerment tools are accessible, flexible and powerful; (2) specify user empowerment tools which address issues beyond algorithmic feeds.[175]

2.157 The department's submission noted the safeguards contained in the bill in respect of user empowerment tools:

> To make an instrument under this power, the Minister must be satisfied that the tool is necessary to protect users of the service in Australia from harms associated with access or exposure to a design feature of the service. This establishes a clear scope of the power and ensures the best interests of Australian users are considered. The Minister must not take into account any material that has been, is or will be accessible to, or delivered to, a user using the service. This provision ensures that the material available on the service is not a relevant factor when designing user empowerment tools, and cannot be used to target a specific service based on the content it provides. This follows feedback from stakeholders on the Exposure Draft Bill and will ensure that the Minister cannot attempt to apply a User Empowerment rule to supress a particular political view or perspective. User empowerment tools made under this provision will also be subject to a mandatory period of disallowance when tabled in Parliament.[176]

Age assurance and access control measures

2.158 The committee received a range of commentary on the requirement in proposed section 27D for online service providers to implement age assurance and access control measures for Australian users if there is a reasonably foreseeable risk that a child could access, or be exposed to, pornography or material that describes or depicts specific fetish practices or fantasies.

2.159 ARACY, the Australian Research Alliance for Children and Youth, outlined the potential positive impacts on children's wellbeing of implementing age assurance for pornography:

> These measures may help reduce children's exposure to pornography and support healthy development. Age assurance should form part of a broader approach to protecting children online, alongside safer design, effective risk management and the other protections established through the Digital Duty of Care framework.[177]

---

174 ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, pp. 7–8.

175 ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, p. 9.

176 The department, *Submission 130,* p. 8.

177 ARACY - Australian Research Alliance for Children and Youth, *Submission 88*, [p. 4].

2.160 While there was broad recognition of the importance of protecting children from exposure to harmful online material, inquiry participants presented differing views on the scope and proportionality of the proposed requirements, their implications for privacy and security, and potential impacts on access to lawful online services.

Scope and proportionality of the measures

2.161 Several inquiry participants noted that the terms 'pornography' and 'fetish practices or fantasies' are undefined in the bill, creating uncertainty regarding the scope of the requirements.[178]

2.162 The Business Council of Australia argued that age assurance obligations should be proportionate to demonstrated risks and recommended that the terms 'pornography' and 'fetish practices or fantasies' be defined by reference to established classification arrangements and, where appropriate, existing online safety codes and standards.[179]

2.163 Other submitters proposed that the bill's age assurance and access control measures could be strengthened by expanding the scope of harms captured. The Alliance for Gambling Reform suggested extending the measures to cover children's access or exposure to online services for placing bets, where the online service's terms of use do not permit a child to open a betting account, place a bet or have a bet accepted.[180] Additionally, the eSafety Commissioner mentioned that age assurance could be used to prevent children's access or exposure to harms such as 'high impact sexually explicit material, self-harm and suicide material, high impact violence material and violent instruction material'.[181]

2.164 The department explained that the material covered by proposed section 27D 'equates to Class 1C and X18+ Class 2 material under the current age restricted material codes' and the provision would 'continue the existing age assurance and access control requirements established in those codes'.[182]

---

178 See, for example: DIGI, *Submission 90*, p. 16; Scarlet Alliance, National Sex Workers Association, *Submission 121*, p. 9; SBS, *Submission 133*, p. 7.

179 BCA, *Submission 34*, p. 5.

180 Alliance for Gambling Reform, *Supplementary Submission 60.1*, pp. 1–3.

181 eSafety Commissioner, *Submission 129*, p. 11.

182 The department, *Submission 130*, p. 8.

Privacy and data security implications

2.165 The committee heard concerns about the potential privacy and data security implications of age assurance and access control measures, with inquiry participants calling for further safeguards.[183]

2.166 The AHRC noted that age assurance should use the least privacy-intrusive effective method, minimise the collection and retention of personal information and prevent its unrelated use.[184]

2.167 Likewise, the OAIC outlined the importance of privacy safeguards:

> Privacy safeguards for age assurance are necessary when considering that such technologies may require the collection of sensitive information such as biometric templates or the use of Government-issued identification documents. Protections also ensure that Australians can trust that their personal information will be protected when they engage with online services when completing age checks.[185]

2.168 Accordingly, the OAIC recommended that consideration be given to introducing privacy safeguards in the bill to ensure alignment with Part 4A of the Online Safety Act (relating to the social media minimum age framework) and the *Interactive Gambling Amendment (Gambling Reform) Act 2026* which set out destruction, purpose limitation and consent requirements. The OAIC also suggested that Digital ID could provide a safe, high-confidence and privacy-respecting method of age assurance 'as an 18+ age token can be easily provided without the need for any other personal information to be shared and does not carry the same privacy risks as Government-issued identification documents'.[186]

2.169 Other submitters echoed the suggestion that the bill should incorporate privacy safeguards equivalent to those in the social media minimum age provisions.[187]

2.170 The eSafety Commissioner noted that the regulator would 'continue to work very closely with the OAIC and Commissioner Kind' and take expert advice from Commissioner Kind in relation to any privacy concerns in relation to age assurance measures.[188]

---

183 See, for example: Privacy 108, *Submission 25*, [p. 1]; OAIC, *Submission 48*, p. 3; Australians vs. The Agenda, *Submission 98*, p. 5; Scarlet Alliance, National Sex Workers Association, *Submission 121*, p. 9.

184 Australian Human Rights Commission, *Submission 58*, p. 13.

185 OAIC, *Submission 48*, p. 3.

186 OAIC, *Submission 48*, p. 3

187 Privacy 108, *Submission 25*, [p. 2]; Scarlet Alliance, National Sex Workers Association, *Submission 121*, pp. 4 and 9.

188 Ms Julie Inman Grant, Commissioner, Office of the eSafety Commissioner, *Proof Committee Hansard*, 10 November 2026, pp. 66–67.

Potential impacts on access to lawful online services

2.171 Some inquiry participants highlighted the potential for age assurance and access control measures to affect access to lawful content and services, including services that are not principally directed towards children.

2.172 For example, the FSU argued that:

> … there is the risk that large numbers of adults will be treated as children (because they cannot or will not prove their age) and will still be subject to extensive censorship.[189]

2.173 The FSU noted that proposed section 27D applies to particular classes of content and does not address what is specifically required to protect children from 'material and conduct that is harmful to children' for content that is not pornography or material that describes or depicts specific fetish practices or fantasies. The FSU continued: 'We are concerned that this will incentivise platforms to provide a range of inappropriate age gating measures' to comply with the Duty.[190]

2.174 The Scarlet Alliance proposed amendments to the bill to ensure that protections for children do not restrict adults' access to lawful material, expressing the concern that:

> … in practice, the likely result is that every adult must verify their age before they can see material that could meet these terms on any service, and that sexual health information, kink education and sex worker content will be placed behind age checks for all users.[191]

2.175 SBS similarly commented that the risk that age assurance and access control measures may capture 'professionally produced content, including drama, film and documentary programming that may contain sexual themes, and news and current affairs coverage'.[192]

Next chapter

2.176 The next chapter examines key issues raised in evidence regarding the bill's proposed regulatory oversight and enforcement framework, before outlining the committee view and recommendations.

---

189 Free Speech Union of Australia, *Submission 54*, p. 6.

190 Free Speech Union of Australia, *Submission 54*, p. 6.

191 Scarlet Alliance, National Sex Workers Association, *Submission 121*, p. 9. See also, p. 4.

192 SBS, *Submission 133*, p. 7.

Chapter 3
Regulatory oversight and enforcement

3.1 This chapter examines the proposed regulatory oversight and enforcement framework established by the Online Safety Amendment (Digital Duty of Care) Bill 2026 (the bill). It discusses key issues raised in evidence regarding the compliance and investigative powers of the eSafety Commissioner, the removal notice regime for fake nude material, and provisions for research and data access. It also considers mechanisms for complaints and dispute resolution, and penalties and enforcement measures available to ensure compliance with the proposed obligations and promote accountability among online platforms. It concludes with the committee's views and recommendations.

Compliance and investigative powers of the eSafety Commissioner

3.2 Several inquiry participants addressed the proposed expansion of the eSafety Commissioner's compliance and investigative powers under Division 2 of Part 13 of the *Online Safety Act 2021* (Online Safety Act) and in other provisions throughout the bill. Concerns were raised regarding the scope of the proposed powers, the adequacy of governance and accountability arrangements, and the potential implications for the operational independence of online service providers.

Some submitters argued that the bill would substantially expand the eSafety Commissioner's powers and questioned whether there were adequate checks on these powers.[1]

3.3 The Digital Industry Group Inc (DIGI) noted that the bill would enable the Commissioner to determine requirements for risk assessments, direct online service providers to take specified actions to ensure compliance with the bill, and require information about algorithms and systems. DIGI also observed that the Commissioner would be able to '[s]hape the content and standards of the [digital] duty [of care] itself' through its role in advising the Minister for Communications (the Minister) on harmful design features, categories of harm and the application of regulatory requirements to particular services.[2]

3.4 DIGI expressed concern that these functions would be concentrated in a single office holder and argued that the eSafety Commissioner's expanded powers

---

1 See, for example: Business Council of Australia (BCA), *Submission 34*, p. 3; Digital Industry Group Inc (DIGI), *Submission 90*, pp. 2 and 12–14; Consumer Choice Center, *Submission 78*, [p. 6]; Interactive Games & Entertainment Association (IGEA), *Submission 93*, pp. 7–8 and 25–26.

2 DIGI, *Submission 90*, p. 12.

warrant stronger institutional governance and accountability arrangements, particularly given their potential implications for children, privacy and freedom of expression.[3]

3.5 Along similar lines, the Business Council of Australia called for regulatory discretion to be 'bounded by objective criteria, transparent processes, appropriate consultation and mechanisms for accountability',[4] while the Interactive Games & Entertainment Association (IGEA) advocated for '[g]reater transparency regarding the intended use and operation of these powers, together with clearer safeguards protecting confidential and commercially sensitive information'.[5]

3.6 Additionally, SBS raised concerns about the potential implications of the eSafety Commissioner's proposed powers for the operational and editorial independence of public service broadcasters.[6]

3.7 The Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department) explained that the exercise of the eSafety Commissioner's information gathering powers under Division 2 of Part 13 would be subject to the satisfaction of certain preconditions:

> In exercising these information gathering powers, the Commissioner must have reason to believe that a person is capable of giving information or evidence, producing documents or answering questions and that the information or evidence or documents are relevant to compliance with, or a possible contravention of, the Act or in relation to an investigation, as per current provisions.[7]

3.8 The department added that the provisions in that Division are 'necessary for the effective investigation and enforcement of compliance with the Act, and especially the [Digital Duty of Care (the Duty)]', considering the 'highly opaque' internal operations of digital platforms.[8]

Removal notices for fake nude material

3.9 While inquiry participants generally welcomed the bill's proposed measures in Part 6A to address apps and websites used to generate fake nude material, the committee heard some concerns that the proposed provisions are too narrowly

---

3 DIGI, *Submission 90*, pp. 12–14.

4 BCA, *Submission 34*, p. 3.

5 IGEA, *Submission 93*, p. 26.

6 SBS, *Submission 133*, p. 8.

7 Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department), *Submission 130*, p. 13.

8 The department, *Submission 130*, p. 13.

drafted to address the range of technologies used to facilitate image-based abuse.

3.10 Monash University academics, Associate Professor Andrew Moshirnia and Dr Amanda Selvarajah, were supportive of the proposed powers in Part 6A, describing nudification technology as a 'longstanding and worsening problem'. They added:

> We regard the new section 86B power allowing the Commissioner to direct app distribution services and search engines to remove or delist an app or website involved in the generation of fake nude material as a welcome intervention, and a marked improvement on relying on the Commissioner's informal engagement with individual providers.[9]

3.11 Nonetheless, several submitters expressed concern that the term 'fake nude material' is undefined in the bill and could exclude forms of non-consensual sexualised material that do not depict a person as nude.[10] Gender Justice Australia recommended defining fake nude material by reference to the existing definition of 'intimate image' in section 15 of the Online Safety Act, to ensure the removal notice powers 'capture the full range of sexualised synthetic material'.[11] Other submitters suggested broadening the provisions to 'fake private sexual material', drawing on the existing definition in section 5.[12]

3.12 Submitters also raised concerns that the proposed removal notice powers may not adequately address multipurpose apps and websites, as well as emerging technologies capable of generating non-consensual sexualised material.[13]

3.13 The eSafety Commissioner suggested that proposed section 86B could be strengthened by allowing removal notices to be issued to a broader range of services, such as internet service providers, hosting service providers and pass-through services. The Commissioner explained that:

> With regards to nudify websites, as currently drafted, the removal notice powers would only require search engine services to remove links to the nudify website. While this may reduce the accessibility of the website, the website would still remain available to those who know its URL. Additionally, eSafety has observed that providers of nudify services often 'phoenix', including by duplicating substantially identical services under new domain names, URLs or other online locations. Providing eSafety with

---

9 Associate Professor Andrew Moshirnia and Dr Amanda Selvarajah, *Submission 9*, [p. 2].

10 See, for example: With You We Can, *Submission 38*, pp. 2–3 and 6; Ms Noelle Martin, *Submission 75*, [p. 2].

11 Gender Justice Australia, *Submission 85*, p. 6. See also, Ms Noelle Martin, *Submission 75*, [p. 2].

12 Associate Professor Andrew Moshirnia and Dr Amanda Selvarajah, *Submission 9*, [p. 5].

13 Associate Professor Andrew Moshirnia and Dr Amanda Selvarajah, *Submission 9*, [p. 1]; Ms Noelle Martin, *Submission 75*, [pp. 3–4].

> the ability to direct internet service providers, hosting service providers and pass-through services to cease supporting identified nudify services would enable more timely and durable disruption of harmful services, and ensure that responsibility for addressing these harms is more appropriately shared across the entities that facilitate their operation and availability.[14]

3.14 According to the department, the proposed removal notice powers 'will provide an efficient and targeted mechanism to complement the Duty'. The department observed that the Duty itself would also require online services to 'take appropriate and effective action to prevent the generation or distribution of fake nude material created without the consent of the person depicted'.[15]

Research and data access

3.15 The committee received a range of evidence on the bill's research and data access framework (proposed Part 14 of the Online Safety Act), including the provisions allowing approved researchers and the eSafety Commissioner to use sock puppet identities when investigating online services.

Data access schemes

3.16 Multiple inquiry participants welcomed the establishment of a statutory framework for researcher access to data on online services, arguing that independent research is essential to understanding online harms and assessing the effectiveness of regulatory interventions.[16]

3.17 The QUT Digital Media Research Centre strongly supported the bill's protections for researcher data access and highlighted that limited access to platform data remains a significant barrier to studying the online information environment:

> Decades of research experience has confirmed the insufficiency of platform-provided data access. Provider-controlled research environments are presented by industry as solutions to transparency concerns, but in practice can impose substantial technical and methodological constraints, restrict extraction and interoperability, limit reproducibility, and leave researchers dependent on tools and interfaces controlled by the companies being scrutinised.[17]

3.18 Professor Daniel Angus welcomed the proposed protections for researchers conducting online safety research, observing that researchers currently bear significant legal risks when conducting research on online platforms:

---

14 eSafety Commissioner, *Submission 129*, p. 9.

15 The department, *Submission 130*, p. 8.

16 See, for example: Dr Honni van Rijswijk, *Submission 6*, p. 2; QUT Digital Media Research Centre, *Submission 70*, [pp. 2–5]; ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, pp. 10–12; Reset.Tech Australia, *Submission 167*, p. 6.

17 QUT Digital Media Research Centre, *Submission 70*, [p. 5].

> … the legal protection in this bill is one of the first times that we've actually gained some kind of standing and protection against forms of recourse from platforms. We do much of this research at our own risk. We know that, when we do the research we do, that platforms could perhaps come after us … That's why we welcome any form of expansion of those protections for researchers working under the strict auspices of the Australian Code for Responsible Conduct of Research. We get those protections afforded to us for doing that because we do so in the public interest.[18]

3.19 The department outlined that:

> Data access schemes are a crucial part of the regulatory framework and will facilitate greater independent scrutiny of whether online services are meeting their duty of care obligations to Australian users.[19]

Scope of researcher data access

3.20 Several inquiry participants argued that the definition of an 'approved researcher' under proposed section 205B should extend beyond those employed by an Australian university, to encompass the independent and civil society researchers, accredited journalists and international collaborators who contribute to online safety research.[20]

3.21 Researchers from the University of Tasmania submitted that the proposed eligibility requirements for an 'approved researcher' are narrower than existing research practices. They noted that online safety research frequently involves collaboration between Australian universities, overseas institutions and non-government organisations, including organisations providing child protection and prevention services.[21] This was reinforced by the Australian Human Rights Commission (AHRC), who pointed out that civil society and other advocacy groups are responsible for much of the online safety research and advocacy that has been done since the introduction of the Online Safety Act.[22]

3.22 Further, the QUT Digital Media Research Centre emphasised the importance of ensuring that researcher access is 'genuinely independent and fit-for-purpose' and recommended that proposed section 205C establish clear principles

---

18 Professor Daniel Angus, Private capacity, *Proof Committee Hansard,* 10 November 2026, p. 56.

19 The department, *Submission 130,* p. 9.

20 See, for example: Dr Honni van Rijswijk, *Submission 6*, pp. 3 and 60; Associate Professor Joel Scanlan, Professor Jeremy Prichard, Dr Rachel Baird and Dr Nina Hudson, *Submission 84*, [pp. 1–3 and 6]; Equality Australia, *Submission 59*, p. 7.

21 Associate Professor Joel Scanlan, Professor Jeremy Prichard, Dr Rachel Baird and Dr Nina Hudson, *Submission 84*, [pp. 1–2 and 6].

22 Australian Human Rights Commission, *Submission 58*, pp. 13–14.

requiring data access schemes to facilitate independent, reproducible and methodologically appropriate research.[23]

Industry concerns

3.23 Industry stakeholders raised concerns about the potential privacy, security and commercial implications of researcher access to sensitive information, particularly where the framework could require disclosure of proprietary systems or information about platform safety mechanisms.

3.24 DIGI claimed that the proposed data access framework lacks sufficient safeguards regarding independent oversight and the scope of data that online service providers could be required to provide. DIGI argued that in the absence of a materiality threshold, the proposed requirements could impose a significant compliance burden on small Australian businesses.[24]

3.25 DIGI also raised concerns about the potential disclosure of information relating to algorithms used for content moderation systems and safety protections. It argued that detailed information about systems used to detect or prevent harmful activity might be exploited by malicious actors.[25]

3.26 The Business Council of Australia similarly emphasised the need to protect algorithms and other proprietary or commercial-in-confidence information, arguing that safeguards are 'particularly important where access could expose trade secrets, intellectual property or security vulnerabilities, including vulnerabilities that could be exploited in ways that affect user safety'.[26]

3.27 Match Group raised particular concerns about the application of mandatory researcher data access to online dating services, noting that these services hold highly sensitive information about users, the inappropriate disclosure of which could expose users to serious privacy and personal safety risks.[27]

3.28 Industry stakeholders made recommendations for amending the data access framework to have researcher access overseen by an independent body,[28] and to account for confidentiality, legal privilege, privacy and data-protection obligations.[29]

---

23 QUT Digital Media Research Centre, *Submission 70*, [p. 5].

24 DIGI, *Submission 90*, pp. 22–23.

25 DIGI, *Submission 90*, p. 23.

26 BCA, *Submission 34*, p. 6.

27 Match Group, *Submission 92*, p. 7.

28 DIGI, *Submission 90*, p. 24.

29 BCA, *Submission 34*, p. 6.

3.29 On the other hand, the ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S) considered that the requirement for researchers to operate within established university research ethics provides a 'strong framework for appropriate ethics and data governance'.[30]

3.30 The department also noted that 'the data that is accessed must be relevant to the online safety of users of online services in Australia, the scheme cannot be used to investigate other matters'. Additionally, the data access rules made pursuant to proposed section 205C would specify adequate safeguards for data access, including the privacy, data storage and security conditions that must be met. The rules would be legislative instruments, subject to disallowance and separate consultation requirements.[31]

Sock puppet identities

3.31 Submitters and witnesses made a range of comments on the provisions in proposed Division 3 of Part 14 regarding the use of sock puppet identities.

Support for sock puppet provisions

3.32 The Tech Policy Design Institute highlighted the importance of the ability to use sock puppet identities for regulatory and enforcement purposes:

> Sock puppet identities can provide an important means for the eSafety Commissioner to conduct 'secret shopper' investigations to understand how services operate in practice, investigate potential harms and test whether regulated services are meeting their obligations.[32]

3.33 At a public hearing, the Co-founder and Executive Director of the Tech Policy Design Institute, Ms Johanna Weaver, gave further evidence in relation to the importance of sock puppet accounts for assessing platforms' compliance with the Duty:

> They're really important because, at the moment, we don't currently have any other means to be able to test … whether the companies are actually complying with the digital duty of care. This is a way that researchers—like our institute, but also many others—could be able to conduct research to see whether companies are complying with their obligations. There are transparency obligations here as well, but without the ability to have sock puppet accounts we really are leaving the tech companies to mark their homework or we're having to conduct enforcement actions. This is a method in between that allows us to help hold those companies to account.[33]

---

30 ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, p. 11.

31 The department, *Submission 130*, p. 9.

32 Tech Policy Design Institute, *Submission 69*, p. 3.

33 Ms Johanna Weaver, Co-founder and Executive Director, Tech Policy Design Institute, *Proof Committee Hansard*, 10 November 2026, p. 50.

3.34 The eSafety Commissioner expressed strong support for the inclusion of sock puppet provisions to support the Commissioner's effective performance of its functions and exercise of its powers under the Online Safety Act. Its submission explained that:

> It is vital that the Online Safety Act provides express authority for eSafety to use [sock puppet] accounts so eSafety can appropriately test, investigate and gather admissible, first-hand evidence with respect to a service's compliance or non-compliance with their legislative obligations. This provision is essential to enable eSafety to verify the availability of certain features on services and test their functionality, to ascertain if a provider is complying with their obligations under the digital duty of care. This is the most practical approach to begin assessing a platform's compliance. Without this coverage eSafety must rely solely on the information and claims provided to it by the platforms themselves, with no mechanism to effectively validate or verify those claims.[34]

3.35 The eSafety Commissioner's submission outlined an example of the current limitations on its ability to obtain accurate information about online platforms, demonstrating the need for sock puppet provisions:

> As an example of current limitations in practice, in April 2026, eSafety undertook an exercise to write to 9 providers to request eSafety declared accounts to confirm if content was available to an end-user on the service under complaint scheme investigations. Only 3 providers agreed to eSafety's request, while the remaining 6 either declined or did not respond to eSafety's request.
>
> Without this coverage eSafety must rely solely on information and claims provided to it by the platforms themselves, with no mechanism to effectively validate or verify those claims.[35]

3.36 The QUT Digital Media Research Centre and ADM+S also gave evidence in support of allowing researchers and the eSafety Commissioner to use sock puppet accounts. The QUT Digital Media Research Centre explained that sock puppet accounts are a 'well-established method of algorithmic auditing' that enables researchers to examine how systems behave in practice when recommending content, displaying advertisements and applying safety measures.[36] ADM+S highlighted that sock puppet accounts would provide important legal protection for researchers and the Commissioner who seek to observe and test how online services operate.[37]

---

34 eSafety Commissioner, *Submission 129*, p. 10.

35 eSafety Commissioner, *Submission 129*, p. 21.

36 QUT Digital Media Research Centre, *Submission 70*, [p. 6].

37 ARC Centre of Excellence for Automated Decision-Making and Society, *Submission 71*, p. 12.

The importance of safeguards

3.37 Several inquiry participants recommended clearer safeguards around the use of sock puppet accounts to ensure their appropriate use and protect users from potential interference.[38]

3.38 The AHRC recommended that the bill expressly limit the use of sock puppet accounts to investigating, observing and testing compliance with the Duty, and prohibit their use to influence or participate in online debate or information-sharing activities.[39]

3.39 DIGI raised concerns about the interaction between authorised sock puppet accounts and the systems used by online services to detect and remove fake accounts. It submitted that platforms invest significant resources in identifying and removing fake accounts associated with scams, impersonation, disinformation and other harmful conduct, and that online service providers should not face liability for removing fake accounts in good faith, especially when authorised sock puppet accounts would be indistinguishable from malicious accounts.[40]

3.40 DIGI recommended removing the sock puppet account provisions once an appropriately safeguarded researcher data access scheme is established. Alternatively, DIGI proposed arrangements to require confidential notification to online services, limitations on the use of sock puppet accounts for observation, protections for services acting in good faith and agreed protocols for testing illegal output.[41]

3.41 Dr Rys Farthing, Chief Research Officer at Reset Tech Australia, addressed 'misconceptions around sock puppets', pointing out that they are 'remarkably ineffective' at spying on what the public says online as '[s]ock puppets have no inherent ability to collect or scrape content … [or] record what people have said'. Dr Farthing added that 'sock puppet protections in the bill won't allow researchers to run inauthentic networks or bot farms for influence'.[42]

3.42 The eSafety Commissioner pointed out the safeguards built into the bill's sock puppet provisions:

---

38 See, for example: Dr Aashish Srivastava, *Submission 11*, pp. 9–10; Digital Defence, *Submission 13*, [p. 3]; Relationships Australia, *Submission 39*, pp. 19–20; Ms Zara Cooper, Chief Executive Officer, Digital Defence, *Proof Committee Hansard*, 9 November 2026, p. 37.

39 Australian Human Rights Commission, *Submission 58*, p. 15.

40 DIGI, *Submission 90*, p. 24.

41 DIGI, *Submission 90*, p. 25. See also, Dr Jennifer Duxbury, Interim Managing Director, DIGI, *Proof Committee Hansard*, 9 November 2026, p. 35.

42 Dr Rys Farthing, Chief Research Officer, Reset Tech Australia, *Proof Committee Hansard*, 10 November 2026, pp. 38–39. See also, Reset.Tech Australia, *Submission 167*, pp. 3–5.

> Testing accounts can only be used for the sole purpose of performing the Commissioner's functions or exercising the Commissioner's powers under the Act. Accordingly, there is no mechanism for testing accounts to be misused, such as to conduct covert operations. The Bill also provides mechanisms for public transparency and external accountability. For example, eSafety would be required to prepare annual statements which summarise what the testing accounts were used for the previous year and explicitly set out the priorities and strategies for the year ahead. eSafety would also be required to consult the Commissioner of the Australian Federal Police in determining the policies to follow in using testing accounts.[43]

3.43 The eSafety Commissioner acknowledged that it 'does not have a remit under the Online Safety Act to undertake covert operations' and that proposed section 205K limits the use of sock puppet accounts to engage with a user of an online service only to the extent necessary to prevent closure of an account with the service.[44]

3.44 The department similarly clarified in its submission that:

> These powers [relating to sock puppet identities] do not allow the Commissioner or independent researchers to engage in political activity, post comments (except where it is specifically necessary to stop an account being automatically closed) or undertake surveillance of users. The Commissioner and authorised researchers may only use a sock puppet account for the purposes of performing their functions and exercising their powers under Section 205K of the Act.[45]

Complaint and dispute processes

3.45 While the committee heard support for the requirement in proposed section 27G that prescribed online service providers must have complaint and dispute processes available to all individuals in Australia, there were calls for its scope to be broadened and for access to external dispute resolution to be provided for in the bill.

3.46 The Telecommunications Industry Ombudsman (TIO) emphasised the need for 'dispute resolution for digital platform users, who currently have no avenue to resolve complaints when the platforms are unresponsive or unable to assist users to their satisfaction'.[46] The TIO outlined the extent of the demand for access to dispute resolution:

> Since January 2023, the TIO has received over 2,500 requests for help from digital platform users, which we are unable provide. These complaints include people who have been locked out of email, cloud storage and social

---

43 eSafety Commissioner, *Submission 129*, pp. 10–11.

44 eSafety Commissioner, *Submission 129*, pp. 21–22.

45 The department, *Submission 130*, p. 9.

46 Telecommunications Industry Ombudsman, *Submission 41*, [p. 2].

> media accounts for allegedly breaching community standards, without clear explanations or avenues for resolution.
>
> … People who contact us describe exhausting online forms, chatbots and email channels, receiving automated or generic responses without clear explanations or processes, and being unable to escalate to human support.[47]

3.47 Dr Vivi Tan, a lecturer at RMIT University, supported the inclusion of proposed section 27G, noting that internal dispute resolution is 'the first point of contact for almost every person with a grievance'. Nonetheless, Dr Tan pointed out that the provision: only applies to services within a class that the eSafety Commissioner prescribes; contains no substantive standards beyond the requirement of equal availability; and leaves 'complaint and dispute processes' undefined. Accordingly, Dr Tan recommended that consideration be given to the inclusion of minimum dispute resolution standards, for example, regarding accessibility, timeliness and human review.[48]

3.48 The AHRC similarly recommended that proposed section 27G 'expressly address accessibility', noting the importance of complaint pathways and information being easy to locate and use, available in accessible formats and written in plain English. However, the AHRC supported the power in proposed section 27G for the eSafety Commissioner to determine, by legislative instrument, the classes of online services to which the obligation applies and the requirements those processes must satisfy.[49]

3.49 The Centre for Media Transition at the University of Technology Sydney called for complaints processes to 'explicitly include appeals processes for content moderation and other actions taken by platforms'.[50]

3.50 The department indicated that proposed section 27G would enable individuals to contact online service providers and seek remedy for harms experienced as a result of content available on those services. Further, the eSafety Commissioner would be empowered to make a legislative instrument setting out additional requirements regarding complaint and dispute processes to which an online service must adhere.[51]

---

47 Telecommunications Industry Ombudsman, *Submission 41*, [p. 3].

48 Dr Vivi Tan, *Submission 24*, pp. 7–8.

49 Australian Human Rights Commission, *Submission 58*, p. 17.

50 Centre for Media Transition, *Submission 123*, p. 3.

51 The department, *Submission 130,* pp. 10–11.

External dispute resolution

3.51 A number of inquiry participants argued that internal complaint and dispute resolution processes should be complemented by external dispute resolution processes.[52]

3.52 The TIO supported an independent external dispute resolution scheme as a direct avenue for consumers to seek redress and hold platforms to account:

> An EDR [external dispute resolution] scheme is a practical avenue for consumers to access redress, including restoring account access, ensuring a user's choices about their algorithms are implemented, reversing an incorrect charge, reconsidering a decision, requiring an explanation or directing appropriate compensation.[53]

3.53 The Ombudsman, Ms Cynthia Gebert, indicated that such a scheme is needed to 'giv[e] people a free, fair and independent place to go when things go wrong online'.[54]

3.54 Similarly, the Human Rights Law Centre argued that while internal complaints and dispute resolution should be available to individuals seeking redress in the first instance, independent dispute resolution should also be available:

> Where a complaint is not resolved satisfactorily or within prescribed timeframes, individuals should be able to escalate the matter to an independent, accessible and specialist dispute resolution body with powers to investigate complaints, make determinations and order appropriate remedies.[55]

3.55 Several inquiry participants proposed that external dispute resolution could take the form of an ombudsman scheme.[56] For instance, Dr Tan observed that '[t]he Australian ombudsman model, in which determinations bind the provider, offers a stronger form of redress [than the European Union Digital Services Act] and is already familiar to industry'. Dr Tan recommended that designated online service providers should be required to be members of an external dispute resolution scheme that is

---

52 See, for example: Consumer Policy Research Centre, CHOICE and Consumer Action, *Submission 53*, pp. 1 and 3; Australian Human Rights Commission, *Submission 58*, p. 18; QNews, *Submission 77*, [p. 4]; Penington Institute, *Submission 86*, [p. 2]; Centre for Media Transition, *Submission 123*, pp. 5–6; Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 9 November 2026, p. 16; Ms Chandni Gupta, Deputy Chief Executive Officer and Director, Digital Policy, Consumer Policy Research Centre, *Proof Committee Hansard*, 9 November 2026, p. 32.

53 Telecommunications Industry Ombudsman, *Submission 41*, [p. 4]. See also, [p. 5].

54 Ms Cynthia Gebert, Ombudsman, Telecommunications Industry Ombudsman, *Proof Committee Hansard*, 10 November 2026, p. 41.

55 Human Rights Law Centre, *Submission 57*, p. 14.

56 Dr Vivi Tan, *Submission 24*, pp. 10–12; Dr Rob Nicholls, *Submission 103*, p. 7; Centre for Media Transition, *Submission 123*, p. 6.

empowered to make determinations binding on providers if accepted by the complainant and to order remedies.[57]

3.56 Ms Gebert envisaged that online platforms could be required to join a scheme like the TIO, which would be industry-funded, and 'push the liability for the costs of their harms back onto them in the handling of complaints'.[58]

Penalties and enforcement

3.57 Inquiry participants expressed a range of views on the bill's proposed penalty and enforcement arrangements, including the adequacy of civil penalties and the merits of introducing a private right of action for individuals and representative organisations.

Civil penalties

3.58 A number of inquiry participants questioned whether the proposed maximum civil penalties would provide an adequate deterrent for the largest online service providers.[59]

3.59 The Privacy Commissioner reflected on the relative power of the online platforms and the challenges in regulating this space:

> I do think that enhanced enforcement powers are necessary to ensure that this legislation and any other legislation in the online realm is effective, given the nature of digital platform power. Speaking from firsthand experience about how challenging it is to bring Australian legislation to bear on foreign major tech companies, I appreciate the motivations behind much of the powers that are contained in this bill.[60]

3.60 Teach Us Consent recommended that maximum penalties be calculated as a percentage of a company's global revenue, arguing that a revenue-based approach would provide a stronger incentive for major platforms to comply with the Duty:

> Tech companies have astronomically high profits and very large profit margins, meaning the incentive to comply is not as strong as a penalty that deducts global revenue.[61]

3.61 Teach Us Consent considered that a revenue-based approach would also align Australia's framework more closely with comparable democratic nations such

---

57 Dr Vivi Tan, *Submission 24*, p. 12.

58 Ms Cynthia Gebert, Ombudsman, Telecommunications Industry Ombudsman, *Proof Committee Hansard*, 10 November 2026, pp. 43–44.

59 See, for example: Teach Us Consent, *Submission 29*, [p. 6]; International Justice Mission Australia, *Submission 50*, p. 9; GetUp, *Submission 149*, p. 3.

60 Ms Carly Kind, Privacy Commissioner, Office of the Australian Information Commissioner, *Proof Committee Hansard*, 10 November 2026, pp 58–59.

61 Teach Us Consent, *Submission 29*, [p. 6].

as the European Union, New Zealand and Canada which are considering introducing fines as a percentage of companies' global revenue.[62]

3.62 Similar arguments in favour of revenue-based penalties were made by other inquiry participants.[63] Associate Professor Honni van Rijswijk, for instance, highlighted comparisons with the maximum corporate penalties under the United Kingdom Online Safety Act, the European Union Digital Services Act and Australian Consumer Law, to argue that:

> … penalty provisions [should] be recast to provide for the greater of a fixed amount, a multiple of the benefit obtained, and a percentage of adjusted turnover, consistently with both the Australian Consumer Law and the comparable overseas regimes[.][64]

3.63 On the other hand, the committee heard concerns from other inquiry participants that the bill's significant penalties could incentivise online platforms to remove lawful content as a precautionary measure.[65]

3.64 This was reinforced by DIGI who argued that online platforms would err on the side of caution by removing lawful material, when faced with high penalties and uncertain standards:

> A service faces penalties of up to $109.2 million, and the Bill does not ask services or the Commissioner to weigh freedom of expression. Faced with an uncertain standard, the rational response is to treat borderline material as harmful and resolve doubt in favour of removal, which could affect lawful debate on matters of public interest, including political communication.[66]

3.65 The Business Council of Australia argued that the penalty framework should distinguish between substantive safety failures and minor administrative errors or documentation breaches. It expressed concern that the bill 'retains the same stated maximum penalty for duty breaches and minor breaches in documentation, such as risk assessments', and recommended lower maximum penalties for minor documentation breaches.[67]

3.66 The department advised that failure to comply with the Duty, risk assessment and user empowerment tool obligations, and age assurance and access control

---

62 Teach Us Consent, *Submission 29*, [p. 6].

63 See, for example: International Justice Mission Australia, *Submission 50*, p. 9; GetUp, *Submission 149*, p. 3.

64 Dr Honni van Rijswijk, *Submission 6*, p. 27. See also, pp. 21 and 26.

65 See, for example: Digital Defence, *Submission 13*, [p. 4]; FamilyVoice Australia, *Submission 36*, p. 4; liber-net, *Submission 108*, [p. 1]; Liberty Victoria, *Submission 143*, [p. 5]; Youth Support and Advocacy Service, *Submission 147*, p. 3.

66 DIGI, *Submission 90*, p. 7.

67 BCA, *Submission 34*, p. 4.

requirements, would attract a maximum civil penalty of 60 000 penalty units. The department indicated that this represented a maximum penalty of $109.2 million for companies.[68] The department explained that:

> A penalty amount of 60,000 units is appropriate to signal a strong deterrent for non-compliance and ensure compliance. It is the maximum amount imposable by a court, and must be imposed by a court only following consideration of the seriousness of the contravention.
>
> This amount brings the penalty in line with those under the *Competition and Consumer Act 2010* and the *Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Act 2026*. Increased penalties reflect the severity and scope of systemic harms that an unsafe online environment poses to the Australian community and wellbeing of Australians.[69]

3.67 The department noted that most other measures would attract a maximum of 6 000 penalty units ($10.9 million for companies). It observed that the current maximum penalty for most offences under the Online Safety Act is 500 penalty units, and noted that this is inadequate when considering the size and resources of major platforms, the maximum penalties available to comparable overseas regulators and the maximum penalties which can be imposed on companies under other Australian laws.[70]

Calls for a private right of action

3.68 A significant number of submitters and witnesses expressed support for the introduction of a private right of action to enable individuals and representative organisations who have experienced online harms to seek redress.[71]

---

68 The department, *Submission 130,* pp. 11–12.

69 The department, *Submission 130,* p. 12.

70 The department, *Submission 130,* p. 12.

71 See, for example: Dr Honni van Rijswijk, *Submission 6*, pp. 3 and 53; Australian Services Union, *Submission 47*, [pp. 2–3]; FamilyVoice Australia, *Submission 36*, p. 3; Older Women's Network NSW, *Submission 76*, [p. 8]; QNews, *Submission 77*, [p. 5]; Ms Noelle Martin, *Submission 75*, [p. 5]; Teach Us Consent, *Submission 29*, [p. 6]; Women's Services Network, *Submission 82*, p. 8; National Aboriginal and Torres Strait Islander Women's Alliance (NATSIWA), *Submission 83*, [p. 5]; The Australia Institute, *Submission 68*, pp. 2 and 4–6; GetUp, *Submission 149*, p. 3; Working with Women Alliance, *Submission 134,* p. 7; Ms Mia Bannister, Private capacity, *Proof Committee Hansard,* 9 November 2026, p. Ms Chanel Contos, Chief Executive Officer and Founder, Teach Us Consent Global, *Proof Committee Hansard*, 9 November 2026, pp. 8–9; Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 9 November 2026, pp. 17–18; Mr Jamie Crosby, Chief Executive Officer, Centre for Excellence in Child and Family Welfare, *Proof Committee Hansard*, 9 November 2026, pp. 17–18; Mr Arif Hussein, Senior Lawyer, Human Rights Law Centre, *Proof Committee Hansard*, 9 November 2026, p. 68; Dr Gemma Killen, Executive Director, Working with Women Alliance, *Proof Committee Hansard*, 10 November 22026, pp. 2–3; Ms Darcie Newland, Senior Policy Officer, Working with Women Alliance, *Proof Committee Hansard,* 10 November 2026, p. 2; Ms Anna Brown, Chief Executive Officer, Equality Australia, *Proof Committee Hansard,* 10 November 2026, p. 3;

3.69 Teach Us Consent supported a private right of action, arguing that it would provide individuals with a direct means of seeking redress and create an additional incentive for online services to comply with the Digital Duty of Care.[72] Ms Chanel Contos, Chief Executive Officer and Founder of Teach Us Consent, told the committee:

> Yes, we strongly support a private right of action. We think it will add to giving more Australians autonomy. Again, many other industries are held to a standard, but, for some reason, tech companies sit in this different level. We've also seen in the US very recently how a private right of action can positively create systemic change in how platforms function and what they offer users.[73]

3.70 Digital Rights Watch argued that regulatory enforcement alone would be insufficient to address the range of online harms likely to arise. It noted that the eSafety Commissioner would not be able to seek or obtain compensation on behalf of individuals under the proposed arrangements, and recommended establishing an express statutory right of action for individuals who have suffered harm as a result of a service provider's failure to comply with the Duty.[74]

3.71 Mr Tom Sulston, Head of Policy at Digital Rights Watch, explained that introducing a private right of action would ease the burden on the regulator that must currently handle all complaints:

> Adding the courts into the regulatory regime means that we will be able to handle more complaints against big tech than just through the regulator. Australian regulators have struggled, being small organisations, coming up against the legal departments of very large organisations.[75]

3.72 Mr Peter Wertheim, Co-Chief Executive Officer of the Executive Council of Australian Jewry, pointed to the evidence of the eSafety Commissioner during the Royal Commission on Antisemitism and Social Cohesion, indicating that the regulator is struggling to handle the rising volume of complaints:

Alex Lia, Senior Legal Policy Advisor, Equality Australia, *Proof Committee Hansard,* 10 November 2026, p. 3; Mr Josh Bornstein, Director, Corporate Regulation, Australia Institute, *Proof Committee Hansard,* 10 November 2026, pp. 33–34.; Ms Johanna Weaver, Co-founder and Executive Director, Tech Policy Design Institute, *Proof Committee Hansard,* 10 November 2026, p. 46; Professor Kimberlee Weatherall, Chief Investigator, ARC Centre of Excellence for Automated Decision-Making and Society, *Proof Committee Hansard,* 10 November 2026, p. 47.

72 Teach Us Consent, *Submission 29*, [p. 6].

73 Ms Chanel Contos, Chief Executive Officer and Founder, Teach Us Consent Global, *Proof Committee Hansard,* 9 November 2026, p. 9.

74 Digital Rights Watch, *Submission 64,* p. 12.

75 Mr Tom Sulston, Head, Policy, Digital Rights Watch, *Proof Committee Hansard,* 9 November 2026, p. 25.

> … the regulator herself, in the course of her evidence in the royal commission, said that her office is swamped and they cannot cope. They have fewer than 40 assessors on their books, and yet the number of complaints has more than doubled in two years and shows every sign of continuing to grow.[76]

3.73 Arnold Bloch Leibler, the Executive Council of Australian Jewry and other joint submitters also raised concerns about the capacity of the eSafety Commissioner to enforce the Duty effectively in the context of an increasing complaints caseload and the resources available to major technology companies to contest regulatory action.[77] The joint submitters recommended establishing a 'private right to enforce the duty at the systemic level', with designated entities (such as non-profit community representative bodies) able to:

> … seek declarations of systemic breach, compliance orders, orders for disclosure of the platform's risk assessments and enforcement data, damages and civil penalties payable to the Commonwealth.[78]

3.74 Mr Leon Zwier, Partner at Arnold Bloch Leibler, expanded on how this would work in practice:

> If a judge is satisfied that there is a reasonable issue for trial, two things will then occur. Firstly, the onus of proof will reverse and it will fall upon the platforms to prove compliance. Secondly, the court could make an order requiring the platform to pay all the legal costs of the fight thereafter for the group that's taken them on.
>
> That changes the commerce of the problem. It is no longer financially in their interest to propagate hate leading to violence, but what will be in their financial interest, if there's a serious issue there, is to remove that material. The beauty of it is that it will save hundreds of millions of dollars for a regulator to go about enforcement. It's speedy, it's fast and it's simple, and, of course, it also weeds out those claims which have no merit. If a judge or registrar decides there's no reasonable issue for trial, there's no reversing of the onus, and the applicant would have to bear the cost and take the risk. So t's a very cost-effective way of dealing with it, and it's directed only to pull-down, not damages—not money. Again—I should say this too—it won't be a feeding frenzy for lawyers. It won't generate a massive amount of work for lawyers. If the platforms want to have a fight, they'll pay for it. If they don't want to have a fight, they'll remove it. It may be the quickest,

---

[76] Mr Peter Wertheim, Co-Chief Executive Officer, Executive Council of Australian Jewry, *Proof Committee Hansard,* 10 November 2026, p. 20.

[77] Arnold Bloch Leibler, ECAJ, ZFA, NSW JBOD, NCJWA, JCCV, Dor Foundation & AIJAC, *Submission 128*, pp. 3–4. See also: Mr Peter Wertheim, Co-Chief Executive Officer, Executive Council of Australian Jewry, *Proof Committee Hansard,* 10 November 2026, p. 20; Mr Josh Bornstein, Director, Corporate Regulation, Australia Institute, *Proof Committee Hansard,* 10 November 2026, p. 34.

[78] Arnold Bloch Leibler, ECAJ, ZFA, NSW JBOD, NCJWA, JCCV, Dor Foundation & AIJAC, *Submission 128*, pp. 3–4.

> fastest, speediest way, without government having to fund a way through it, and, as I said, it won't lead to a proliferation of complicated litigation.[79]

3.75 The Australian Services Union (ASU) similarly called for the ability to bring individual and collective complaints under the Duty, including for example complaints 'brought by unions on behalf of groups of workers'.[80] The ASU argued that:

> Given the widespread harms being caused by social media, both eSafety and individual workers should have the right to bring complaints to cover all circumstances. Without this, individuals remain stuck in social media companies' own reporting mechanisms, which only seek to protect the platform.[81]

3.76 Conversely, DIGI argued that a 'new right to sue is premature' and noted that 'Australians can already sue in negligence, under the statutory privacy tort and the Australian Consumer Law, and use the Commissioner's removal schemes'. DIGI stated that further redress should be a question left for the next statutory review once the Duty has been 'bedded down and there is evidence of how it operates'.[82]

3.77 The department stated that the Duty would be:

> … enforceable through regulatory action and litigation by the Commissioner. The Duty will strengthen the basis for individuals to make a common law claim of negligence against online services on the grounds that the service owed them a Duty of care, breached that Duty, and as a result of the breach, caused them to suffer damage.[83]

Committee view

3.78 The committee acknowledges the large and growing body of evidence demonstrating the serious, pervasive and often pernicious harms experienced by Australians in online environments, particularly on social media platforms. These harms can have devastating consequences for individuals, families and communities. For young and vulnerable Australians, exposure to harmful online content and platform practices can have catastrophic and, in some cases, fatal consequences.

3.79 The committee considers that, although the current regulatory framework was an important progression towards creating a safer online ecosystem, it has not adequately addressed the scale, nature and evolving character of online harms. In particular, an approach that relies heavily on industry-developed codes is

---

79 Mr Leon Zwier, Partner, Arnold Bloch Leibler, *Proof Committee Hansard*, 10 November 2026, p. 20.

80 Australian Services Union, *Submission 47*, [pp. 2–3].

81 Australian Services Union, *Submission 47*, [p. 2].

82 DIGI, *Submission 90*, p. 27.

83 The department, *Submission 130*, p. 13.

insufficient to ensure that online service providers take meaningful responsibility for the risks their services create. The committee therefore welcomes the bill as an important and necessary reform.

3.80 The bill seeks to change the regulatory framework at a fundamental level by establishing a Digital Duty of Care which would apply to online service providers. In the committee's view, this is a significant improvement on the existing regulatory approach. A holistic, principle-based duty of care has the potential to establish a more effective and enduring framework for online safety, capable of responding to changing technologies, platform practices and patterns of harm. Rather than relying primarily on sector-specific industry codes and standards, the proposed framework would impose a systemic duty on online service providers to take responsibility for identifying, assessing and mitigating or avoiding the risks associated with their services.

3.81 The committee particularly welcomes the bill's shift towards a more preventative and proactive approach to online safety. The proposed Digital Duty of Care appropriately places responsibility on online service providers to identify and address the risks arising from the design, operation and delivery of their services, rather than placing the onus on individual users to protect themselves from harm. The committee considers this a crucial shift in regulatory responsibility. The bill rightly recognises that online safety cannot depend solely on individual users exercising caution or navigating harmful online environments, but requires platforms themselves to take responsibility for the safety of the services they provide and profit from.

3.82 The committee recognises that inquiry participants raised legitimate concerns about the potential implications of the bill for freedom of speech and expression, including the risk that obligations could restrict adults' access to lawful material online. Concerns were also raised that the proposed requirements could impose excessive compliance burdens on small or low-risk online service providers. The committee takes these concerns seriously. Freedom of expression and access to lawful information are important principles that must be protected, and regulatory obligations must be appropriately calibrated to the nature and level of risk posed by different services.

3.83 However, the committee considers that the bill contains important safeguards to address these concerns. Its requirements for proportionality and reasonableness, together with appropriate thresholds for harm, provide a basis for ensuring that any limitations on freedom of expression are justified and proportionate to the objectives of preventing and reducing online harm. The bill also provides for exemptions and exclusions from certain requirements, including through the making of legislative instruments. These mechanisms will allow obligations to be tailored to the circumstances and risk profiles of different online services, avoiding a one-size-fits-all approach.

3.84 The committee also considers that the compliance obligations imposed by the bill must be understood in the context of the scale and resources of the businesses to which they apply. Major online platforms generate substantial revenues and profits from their operations in Australia and internationally, and have the resources and capacity to meet meaningful regulatory obligations. It is reasonable to expect these businesses to invest in the safety of the services they provide and to take responsibility for the harms that their products and practices may cause. The committee considers that serious and significant penalties for breaches of the Digital Duty of Care and other requirements of the bill are appropriate and necessary to ensure that compliance is treated as a genuine business obligation, rather than simply a cost of doing business.

3.85 The committee also acknowledges suggestions from inquiry participants that the bill should go further in addressing online hate directed at individuals and groups on the basis of protected characteristics, including race, religion, sex, and sexual orientation. The committee considers that online hate and vilification can cause significant harm and undermine the safety and participation of individuals in online environments. The committee is persuaded that the concept of protected characteristics is sufficiently familiar to Australian law, having long been recognised in Commonwealth anti-discrimination legislation, such that its inclusion in the proposed framework is unlikely to give rise to significant legislative uncertainty. The committee therefore considers that the Australian Government should give further consideration to including an express provision addressing group-directed hate on the basis of protected characteristics.

3.86 The committee further notes the significant support expressed during the inquiry for the introduction of a private right of action. Such a mechanism could empower individuals, and representative organisations acting on their behalf, to seek urgent removal of harmful material from online platforms and, where appropriate, compensation for loss or damage suffered. The committee considers that providing affected individuals with an avenue to seek redress would be an important complement to the regulatory powers of the eSafety Commissioner. It would also reinforce the central principle underpinning the bill: that online service providers must be accountable for preventing and addressing harm arising from their services. The committee considers that the Government should consider examining how a private right of action could be incorporated into the bill, including for breaches of the Digital Duty of Care that occasion harm or loss.

3.87 Ultimately, the committee considers that the bill represents a substantial and welcome improvement to Australia's online safety regulatory framework. It would move the regulatory approach away from an over-reliance on industry codes and towards a framework in which online service providers have clear obligations to prevent harm, assess the risks associated with their services and

take appropriate steps to mitigate or avoid those risks. This is a significant shift in the responsibilities expected of online service providers and one that is long overdue. The committee commends this reform and considers that the proposed Digital Duty of Care has the potential to deliver meaningful and lasting improvements to the safety of Australians online.

Recommendation 1

3.88 The committee recommends that the Australian Government introduce amendments to the bill to establish a civil right of action for individuals in respect of breaches of the Digital Duty of Care that cause harm or loss.

Recommendation 2

3.89 The committee recommends that the Australian Government, as part of the statutory review, consider the effectiveness of the Digital Duty of Care in addressing online hate and vilification directed at individuals or groups on the basis of protected characteristics.

Recommendation 3

3.90 The committee recommends that the Australian Government amend the bill to clarify the scope of application, specifically to confirm:

- **the bill's intention to regulate digital communication platforms, such as social media platforms; and**
- **that the bill is not intended to apply to low-risk websites or online services, such as small business websites, online market places, booking platforms, or religious websites focused on education or doctrinal instruction.**

Recommendation 4

3.91 Subject to consideration of Recommendations 1 and 3, the committee recommends that the Senate pass the bill.

Senator Varun Ghosh
Chair

Coalition Senators' Dissenting Report

Introduction

1.1 The Online Safety Amendment (Digital Duty of Care) Bill 2026 (bill) is so deeply flawed and so ill-conceived that it should never have seen the light of day.

1.2 While Coalition senators strongly support measures as necessary to protect Australians, particularly children, from online harm, the bill, if passed, would seriously compromise the free speech of Australians as well as undermine existing online safety protections enshrined in the *Online Safety Act 2021* (Online Safety Act).

1.3 It is most regrettable that the Albanese Government has determined to use the cover of child safety to enact what can only be described as a blank cheque for political censorship. In conferring sweeping powers on the Minister for Communications (Minister) and the eSafety Commissioner (Commissioner), relying on dangerously vague definitions of harm and imposing poorly defined and onerous obligations on online service providers, the bill creates powerful incentives to suppress lawful speech, including legitimate political debate.

1.4 Compounding these fundamental flaws, the bill exposes small businesses, charities, faith groups and other low-risk online services to a potentially crippling regulatory burden while dismantling mandatory industry codes and standards designed to protect Australians from some of the most egregious forms of online harm.

Enforcing our current laws is vital

1.5 Beyond the Online Safety Act, the online safety of Australians is also governed by extensive Commonwealth, state and territory laws, including criminal laws dealing with child sexual abuse, grooming, terrorism, incitement to violence and harassment, as well as defamation, privacy, anti-discrimination and vilification laws.

1.6 Coalition senators believe the Government should be focusing much more on enforcing Australia's current laws than embarking on its Digital Duty of Care folly. Why are bomb-making videos available on YouTube[1] and self-harm material being disseminated on Tik Tok?[2] Where is the enforcement action that is desperately required? We note with concern Meta's landmark US settlement worth up to US$17.1 billion over allegations that it deliberately designed

---

1 'Online bomb guides fuel rising teen terror threat', *The Australian*, https://www.theaustralian.com.au/business/media/bombmaking-guides-remain-on-youtube-after-teenager-convicted-over-sydney-opera-house-plot/news-story/a525888e8de7a5b1803909ecea077e2c (accessed 20 November 2026).

2 Senator David Pocock, *Proof Committee Hansard*, 9 November 2026, pp. 48–49.

Facebook and Instagram to addict children and mislead parents about the risks. Given the inherent risks, it is extremely worrying for Australian parents and their children that the Government's social media minimum age law is, on the whole, not working.

Putting parents and families first

1.7 With a strong focus on putting parents and families first, Coalition senators believe more needs to be done to hold digital platforms to account for the harm they cause, particularly to children. With the rapid changes in technology and artificial intelligence, governments must be prepared to respond quickly to address and combat emerging, serious online harms as the Coalition did in the wake of the abhorrent Christchurch terrorist attack which was live-streamed, in part, by the perpetrator.[3]

1.8 The Coalition has strongly advocated for access to parental safety tools which would apply across all devices, giving parents choice over what their children say and see online. Parents should be free to choose the tools they trust to block harmful content, restrict apps and websites, manage screen time and keep their kids safe online. This is about a simple principle: families should have the choice in relation to their children's safety, not big tech.

1.9 As prosecuted by the Free Speech Union, the Coalition has also proposed that all social media platforms should follow in the steps of X Corp which has delivered algorithmic transparency for its For You feed. This would require all social media companies to disclose the key factors and signals driving their recommendation and moderation systems, while protecting source code, personal information, and legitimate security interests.

1.10 This gives anyone the opportunity to better scrutinise whether platforms are pushing harmful material, manipulating users, censoring legitimate views, or applying their own rules unfairly. Big tech should not be able to operate a black box which shapes what millions of Australians see every day without proper scrutiny.

1.11 Even after the Prime Minister boasted about his visit to Apple headquarters in the United States to discuss the importance of digital safety tools, it is a poor indictment on the Minister and her Government that neither parental safety tools or algorithmic transparency have been addressed in this bill.

---

[3] In 2019, following the Christchurch terrorist attack, the Coalition introduced the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, making it a criminal offence for online content and hosting service providers to fail to expeditiously remove material produced by perpetrators or their accomplices depicting terrorist acts, murder, attempted murder, torture, rape or violent kidnapping. The legislation also imposed mandatory reporting obligations to the Australian Federal Police in relation to such conduct occurring in Australia.

Labor's insidious censorship agenda

1.12 The Albanese Government's insidious agenda underpinning this bill was laid bare by the Prime Minister during a speech on the sidelines of the United Nations General Assembly in New York on 22 September 2026. In describing the Digital Duty of Care as an 'inevitable next stage', the Prime Minister canvassed his concerns about 'misinformation, disinformation' and increasing political polarisation, with people moving 'more and more to the extremes, be they of the left or the right'.

1.13 Despite his subsequent attempts to walk back these comments, the Prime Minister exposed the Government's ambitions to regulate online discourse well beyond the protection of children from serious harms.

1.14 Further evidence of the Government's disturbing agenda to control what Australians say and see online can be seen in a social media video posted in recent days by West Australian Labor senator, Ellie Whiteaker.

1.15 In the video, Senator Whiteaker takes issue with 'trad wife' online content, including images of a woman at home cooking alongside her child. Senator Whiteaker states that 'being told to give up their independence, to submit to a man, to obey their husbands …[are] things that women just shouldn't be exposed to online in 2026,' and that the Digital Duty of Care will hold digital platforms accountable by 'giving the power back to you to decide whether you want the algorithm or not'.[4]

1.16 The senator's suggestion that Australian women should be shielded from lawful content about marriage and family life because she considers it objectionable goes to the heart of the dangers posed by this bill: who determines what is harmful, according to whose values and on what basis?

1.17 The Greens' Senator David Shoebridge also exposed the dark underbelly of these proposed laws when he claimed they were all about 'having an algorithm that doesn't actually promote and generate hate'. He cited both the so-called offensive views of Senator Pauline Hanson and the Coalition, saying 'we need digital duty of care so that those messages aren't amplified and they don't become the content that kids are digesting when they flip open their phone and wonder what's happening in the world'.[5]

---

[4] Please note the Online Safety Amendment (Digital Duty of Care) Bill 2026 (bill) confers no express right on Australians to turn off content recommendation algorithms. Rather, it provides a broad discretion to the Minister for Communications to make rules in relation to user empowerment tools.

[5] Laurence Karacsony and Oscar Godsell, 'Greens Senator David Shoebridge claims Digital Duty of Care is needed to stop 'amplifying' One Nation, Coalition rhetoric', *News24*, 17 September 2026, https://www.news24.com.au/politics/australian-politics/greens-senator-david-shoebridge-claims-digital-duty-of-care-is-needed-to-stop-amplifying-one-nation-coalition-rhetoric/news-story/b7127733162a422542e97eadd712f8b2 (accessed 20 November 2026).

1.18 It is certainly not the role of government to determine which lawful opinions Australians should be permitted to express or encounter online, whether about politics, religion, gender, marriage or any other matter. The right to express unpopular, controversial or even offensive views is fundamental to a free and democratic society.

1.19 Yet the powers conferred on the Minister and the Commissioner are so far-reaching, the concepts of harm so ill-defined and the penalties so punitive that online service providers will be heavily incentivised to censor lawful speech rather than risk regulatory action.

1.20 No government should be entrusted with such extraordinary powers to shape public discourse, suppress dissent or determine the boundaries of acceptable opinion. The prospect of government-sanctioned political censorship under the guise of online safety is neither remote nor theoretical. This bill presents a genuine and frightening threat to the democratic freedoms of all Australians.

Coalition's online safety record

1.21 Before we discuss the many defects with the bill, it is important to reiterate the Coalition's exceptionally strong record on online safety.

1.22 In 2015, the Coalition established the world's first Commissioner, introducing a complaints and removal scheme to combat the serious cyberbullying of children and strengthening Australia's capacity to combat child sexual abuse material online.

1.23 In 2017, the Coalition expanded the remit of the Commissioner to encompass the online safety of all Australians, not just children. In 2018, the Coalition legislated to combat the non-consensual sharing of intimate images and, in 2019, introduced laws to combat the online dissemination of abhorrent violent material following the Christchurch terrorist attack.

1.24 In 2021, the Coalition enacted the landmark Online Safety Act, substantially strengthening protections against child cyberbullying, image-based abuse and illegal and age-restricted online content. The Act also established the world's first Adult Cyber Abuse Scheme, empowering the Commissioner to investigate complaints and order the removal of seriously abusive online material targeting Australian adults.

1.25 The Online Safety Act also established the Basic Online Safety Expectations to drive greater transparency and accountability from online services, as well as the legislative framework for mandatory industry codes and standards.

1.26 There are now 17 mandatory industry codes and standards regulating eight sectors of the online industry, including social media platforms, messaging services, online gaming services, AI chatbots, websites, search engines, app stores, hosting services, internet service providers and manufacturers and suppliers of internet-connected devices.

1.27 These codes and standards provide extensive online safety protections:

- Six Unlawful Material Codes and two Unlawful Material Standards, which came into effect progressively between December 2023 and December 2024, combat Class 1A and Class 1B material, including child sexual abuse and exploitation, pro-terror material, extreme violence, sexual violence, cruelty, serious criminal activity and certain material promoting illicit drug use.
- Nine Age-Restricted Material Codes, which came into effect progressively from December 2025, protect children under 18 from Class 1C and Class 2 material, including pornography, high-impact violence, simulated gambling and material which encourages, promotes or provides instructions for suicide, self-harm or eating disorders.

1.28 Depending on the nature and risk profile of the online service, these codes and standards impose specific obligations in relation to the detection and removal of unlawful material, age assurance, parental controls, content moderation, complaints handling, risk assessments and safety measures, including safeguards against harmful content generated by AI chatbots.

Parliament is being asked to 'legislate blind'

1.29 One of the most fundamental defects in the bill is the extraordinary transfer of legislative power from the Parliament to the Executive. Rather than setting out clearly the scope, application and substance of the law, the bill leaves many of these critical matters to the discretion of the Minister and the Commissioner.

1.30 As leading constitutional law expert Professor Emerita Anne Twomey argued in her submission to the inquiry, this represents a deeply concerning shift of power from the Parliament to the Executive, leaving Parliament 'legislating blind as to the consequences of its law'.[6]

1.31 Professor Twomey raised particular concerns about the extraordinary powers conferred on the Minister to determine which online services are exempt from the law, which online services are deemed to be social media services and which design features have negative behavioural impacts. These are not matters of administrative detail but go to the very heart of the operation of the law.

1.32 In likening the Minister's proposed exemption powers to the 'dispensing power' of Stuart monarchs, abolished under the Bill of Rights of 1689, Professor Twomey also warned of the potential for lobbying and undue influence by corporations seeking exemptions from the law. She concluded:

> In my view, Parliament should take greater responsibility for determining the application of its laws, rather than surrendering this to the Executive.[7]

---

6 Anne Twomey Professor Emerita, *Submission 132*, p. 1.

7 Anne Twomey Professor Emerita, *Submission 132*, p. 2.

1.33 Coalition senators wholeheartedly agree. It is a fundamental responsibility of the Parliament, not the minister or an unelected regulator, to determine the scope, substance and application of laws which have such profound implications for the rights and freedoms of Australians.

1.34 It is unconscionable that the Government is asking the Parliament to pass legislation of such consequence without knowing the full extent of the obligations to be imposed, the online services to which they will apply or the implications for the free speech of Australians. The Parliament must not surrender its legislative responsibilities by handing the Executive such a dangerous blank cheque.

An untenable assault on free speech

Dangerously vague concepts of harm

1.35 The bill introduces new and uncertain categories of harm, including material or conduct that encourages or promotes hostile attitudes towards women or gender equality, glorifies crime or seriously harmful practices, or otherwise may cause serious harm to children.[8] These concepts are not confined to unlawful material or conduct.[9] The bill's definition of gender-based violence also encompasses non-physical violence, raising further questions about the limits of regulated expression.

1.36 In response to questioning from Coalition senators about whether women advocating for single-sex spaces, biological sex-based rights or changes to gender identity laws could be caught by the bill, Australian Human Rights Commissioner Dr Lorraine Finlay said:

> The risk that we've identified in our written submissions is that 'hostile attitudes' is not a settled legal concept. It's inherently subjective, and therefore it's a problematic legal standard because it doesn't provide a really clear dividing line between harmful expression and robust disagreement. It risks turning subjective judgements about tone and viewpoint into a basis for regulatory intervention.[10]

1.37 Even the eSafety Commissioner has called on Parliament to define these new categories:

> Where new terms are not defined, such as harms under sections 25D and 25E of the Bill, eSafety recommends definitions be determined which can be

---

8 Proposed section 25E.

9 The bill, Revised Explanatory Memorandum, p. 59.

10 Dr Lorraine Finlay, Human Rights Commissioner, Australian Human Rights Commission, *Proof Committee Hansard*, 9 November 2026, p. 75.

> debated and agreed to by Parliament to give the regulator the clearest approach to enforcement and to provide industry with sufficient clarity.[11]

1.38 Alarmingly, when questioned about the meaning of hostile attitudes towards women or gender equality, the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (department) was unable to provide a precise definition.

> There will be a process by which the eSafety Commissioner will provide guidance around that, but, ultimately, it may be something that ends up being tested through the courts.[12]

1.39 While the Government removed the exposure draft power for the Minister to prescribe further categories, proposed section 25E(1)(f) retains a broad, catch-all provision covering other material or conduct that may cause serious harm to children. As Dr Finlay pointed out, the use of the word 'may' establishes a threshold of mere possibility.[13]

1.40 By effectively leaving online service providers and the Commissioner to determine the boundaries of acceptable expression, the bill undermines a fundamental principle of the rule of law: that laws must be clear, certain and predictable.

1.41 Certainly the bill risks suppressing legitimate debate about women's sex-based rights, gender ideology, religious beliefs, government policy and other contested social and political issues. What one person considers harmful, another may regard as the legitimate expression of a conscientiously held belief.

1.42 The vice-president of the Rule of Law Institute of Australia, Chris Merritt, warned the committee:

> Broadly, I think it should not proceed in its current form for this reason: key provisions are either undefined or are described in vague terms. What that means is this bill would leave itself open to subjective or arbitrary application.[14]

1.43 Mr Merritt argued that the bill fundamentally reverses the manner in which laws restricting free speech are made in Australia:

> Generally, speech should be free—that's our heritage—except when parliament chooses to impose limits. We see that with all sorts of things in

---

[11] eSafety Commissioner, *Submission 129*, p. 8.

[12] Ms Clare Chapple, First Assistant Secretary, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, *Proof Committee Hansard*, 10 November 2026, p. 76.

[13] Dr Lorraine Finlay, Human Rights Commissioner, Australian Human Rights Commission, *Proof Committee Hansard*, 9 November 2026, p. 76.

[14] Mr Chris Merritt, Vice President, Rule of Law Institute of Australia, *Proof Committee Hansard*, 9 November 2026, p. 69.

> parliament. I've mentioned terror laws, but there are also laws of defamation and of contempt. Those are carve-outs from a broad, general right, whereas this approach is completely the reverse.[15]

1.44 Liberty Victoria, notwithstanding its broad support for a Digital Duty of Care, also raised concerns that overly broad definitions of harm could capture lawful expression and incentivise platforms to remove lawful speech to minimise regulatory risk.[16]

1.45 In its submission, the Institute of Public Affairs (IPA) warned:

> The digital duty of care bill would create a censorship machine built on arbitrary government decision-making, opaque controls, and surveillance of users.[17]

1.46 In evidence to the committee, the IPA's Director of the Law and Freedom Program, Dr Andrew Bushnell, reinforced the dangers of regulatory overreach and the threat to Australians' freedom of expression:

> Freedom of speech is not a privilege; it's a right that Australians have enjoyed since the foundation of our country … The default position is that Australians are free to speak and free to participate. This bill basically reverses that. It says everyone is captured by the digital duty of care, unless eSafety says otherwise.[18]

1.47 Dr Bushnell also made clear that these defects were so fundamental that the bill could not be salvaged by amendment:

> Our position has been that this is simply the wrong regulatory approach and, therefore, can't be salvaged by any amendments.[19]

1.48 While the bill contains exclusions for certain categories of material, including professional news and material in the public interest, these do not provide comprehensive protection for lawful expression.

1.49 Compounding the uncertainty created by ill-defined categories of harm, the bill fails to define what constitutes material in the public interest. This leaves independent journalists including podcasters, community groups and ordinary Australians particularly vulnerable to inconsistent or overly cautious moderation. The Australian Human Rights Commission (AHRC) called for

---

15 Mr Chris Merritt, Vice President, Rule of Law Institute of Australia, *Proof Committee Hansard*, 9 November 2026, p. 71.

16 Liberty Victoria, *Submission 143*, [pp. 1–2 and 4–5].

17 Institute of Public Affairs, *Submission 56*, p. 1.

18 Dr Andrew Bushnell, Director, Law and Freedom Program, Institute of Public Affairs, *Proof Committee Hansard*, 9 November 2026, p. 67.

19 Dr Andrew Bushnell, Director, Law and Freedom Program, Institute of Public Affairs, *Proof Committee Hansard*, 9 November 2026, p. 63.

greater certainty about the exclusion and stronger protection for political communication and public debate.

1.50 In a liberal democracy, Australians must be free to express opinions which others may find controversial, confronting or offensive. Freedom of speech is not confined to views which enjoy popular support or the approval of the government of the day.

1.51 Coalition senators consider it untenable that lawful expression could be suppressed as a consequence of subjective, open-ended and ill-defined concepts of harm, without Parliament ever having legislated to prohibit that expression.

Powerful incentives to remove lawful speech

1.52 The bill creates a perverse financial incentive for online service providers to censor lawful speech. While corporations face penalties of up to $109.2 million for breaching the Digital Duty of Care, there is no corresponding penalty under the bill for the unjustified removal or suppression of lawful material. Given the uncertainty as to what constitutes harmful material, the safest commercial decision will be to remove or restrict any content which might fall foul of the regulator.

1.53 As the Anglican Diocese of Sydney submitted:

> The statutory incentives therefore run in only one direction: towards the removal or restriction of more material.[20]

1.54 Australian Human Rights Commissioner Dr Lorraine Finlay warned that the subjective nature of some of the harms prescribed in the bill meant that decisions about the boundaries of expression would be:

> … made by private companies who will be incentivised not to test those boundaries because of the significant penalties that are attached …[21]

1.55 These concerns were reinforced by the evidence of Dr Jennifer Duxbury, interim managing director of the Digital Industry Group Inc.:

> The fines are very large. It applies across the entire economy. In combination, we would suggest that that incentivises a lot of companies to take down content that they may be doubtful about or consider to be borderline to avoid the very substantial consequences of breaching this legislation.[22]

---

[20] Anglican Church, Diocese of Sydney, *Submission 63*, p. 4.

[21] Dr Lorraine Finlay, Human Rights Commissioner, Australian Human Rights Commission, *Proof Committee Hansard*, 9 November 2026, p. 75.

[22] Dr Jennifer Duxbury, Interim Managing Director, Digital Industry Group Inc., *Proof Committee Hansard*, 9 November 2026, p. 37.

1.56 Similarly, TikTok raised concerns about the potential for 'overzealous moderation' given the ambiguity and uncertainty in the bill.[23]

1.57 Bishop Anthony Percy of the Australian Catholic Bishops Conference warned that the bill 'places the power of censorship in the hands of tech companies'. He told the committee:

> The fines that can be placed upon people for this make people very, very risk averse to any type of legitimate debate.[24]

1.58 The Australian Jewish Association raised concerns that automated content moderation could result in the removal of material published by Australians seeking to expose or condemn antisemitism, terrorism and extremism. The association called for financial penalties to be imposed on platforms for the 'repeated and systemic wrongful removal of lawful content'.[25]

1.59 The NSW Council for Civil Liberties similarly warned that platforms could seek to shield themselves from multimillion-dollar penalties by establishing 'digital exclusion walls' and deploying 'blunt, error-prone automated moderation algorithms'.[26]

1.60 The Free Speech Union of Australia (FSU) provided compelling evidence of the bill's potential to suppress lawful political communication. Using artificial intelligence to test the proposed laws, the FSU found that parliamentary speeches by Senators Mehreen Faruqi and Jacqui Lambie, footage of political protests, political satire and even a documentary on Indigenous cultural practices were all at risk of censorship.

1.61 The FSU also warned of the potential misuse of sweeping government powers, including the Commissioner's capacity to influence censorship decisions and obtain warrantless access to computer systems, potentially including those of political parties. Far from reining in big tech, the FSU argued the bill would entrench its dominance by driving smaller online services out of the market. Given the serious and pervasive defects in the bill, the FSU recommended its rejection in its entirety.[27]

1.62 While the Commissioner sought to dismiss concerns about over-censorship, her evidence about the conduct of digital platforms under the current regulatory

---

23 Ms Jessika Lofstedt, Head, Public Policy, TikTok, *Proof Committee Hansard*, 9 November 2026, p. 46.

24 Bishop Anthony Percy, Member, Bishops Commission for Life, Family and Public Engagement, Australian Catholic Bishops Conference, *Proof Committee Hansard*, 10 November 2026, p. 16.

25 Mr Robert Gregory, President, Australian Jewish Association, *Proof Committee Hansard*, 10 November 2026, pp. 12–13.

26 NSW Council for Civil Liberties (NSWCCL), *Submission 55*, p. 3.

27 Free Speech Union of Australia, *Submission 54*, pp. 1–5, 7–11 and 15.

framework fails to address the very different commercial and regulatory incentives created by the bill.[28]

1.63 The suppression of lawful speech does not simply involve the removal of online material. It may involve the demotion of content, restrictions on its reach, age-based access restrictions or the suspension of user accounts.

1.64 Arguably, the Government is outsourcing censorship to online service providers, backed by the threat of enormous financial penalties. The chilling effect on lawful speech, political debate and religious expression cannot be underestimated.

A stifling of religious freedom

1.65 There is no express exclusion for religious worship or teaching. The inquiry received evidence from the Australian Catholic Bishops Conference, theAnglican Diocese of Sydney, the Coptic Orthodox Diocese and the Australian Jewish Association about the risk to lawful religious expression. The Anglican Diocese of Sydney warned that:

> … a Sunday sermon on a topic such as marriage could be removed from a local parish website without the knowledge of the parish, and without right to contest that removal.[29]

1.66 The Australian Jewish Association also warned that the broad definitions could capture material published to expose or condemn antisemitism, terrorism and extremism. Coalition senators consider that lawful religious expression and robust public debate on controversial issues must be protected in legislation, not left to the discretion of the regulator or the risk appetite of a technology company.

Repeal of codes and standards weakens Australia's online safety laws

1.67 Coalition senators are deeply concerned that, under the guise of making Australians safer online, the Government is dismantling fundamental protections in the Online Safety Act, enacted by the former Coalition government.

1.68 The Act already provides a comprehensive regulatory framework to combat unlawful and harmful online material, underpinned by removal powers, mandatory industry obligations and substantial penalties. This framework comprises 17 legally enforceable codes and standards: six Unlawful Material Codes, two Unlawful Material Standards and nine Age-Restricted Material Codes.

---

[28] Ms Julie Inman Grant, Commissioner, Office of the eSafety Commissioner, *Proof Committee Hansard*, 10 November 2026, p. 69. See also, Mr Richard Fleming, General Counsel, Office of the eSafety Commissioner, *Proof Committee Hansard*, 10 November 2026, p. 69.

[29] Anglican Church, Diocese of Sydney, *Submission 63*, p. 3.

1.69 These instruments impose specific, proactive obligations on online service providers to prevent, detect, report and remove unlawful material or restrict access to age-inappropriate content. They address some of the most serious online harms, including child sexual abuse and exploitation, terrorist material, extreme violence, pornography and material promoting or instructing illicit drug use, suicide, self-harm and eating disorders.

1.70 The Government's repeated assertions that Australia's existing online safety laws are merely reactive and allow big tech to mark its own homework are a gross misrepresentation of the law. Not only are the codes and standards mandatory, but the Commissioner has exercised her statutory powers to reject inadequate industry codes and impose two industry standards in their place.

1.71 Shockingly, after a 12-month transition period, the bill abolishes all 17 codes and standards in favour of a broadly defined Digital Duty of Care, with no guarantee that the existing protections will be replicated.

1.72 In a damning assessment of this fundamental deficiency in the bill, the Commissioner stated in her submission:

> As currently drafted, the Bill does not provide any mechanism to set specific obligations. While eSafety will provide regulatory guidance that outlines what it sees as best practice, this guidance is not enforceable.[30]

1.73 Most alarmingly, the Commissioner warned that online service providers could scale back their existing measures to detect and prevent child sexual exploitation and that it would be more difficult for eSafety to take enforcement action in response.

1.74 The Commissioner also identified deficiencies in the bill's age assurance provisions, which are considerably narrower in scope than the existing mandatory requirements to protect children from harmful material.

1.75 Rather than strengthening existing online safety protections and holding non-compliant providers to account, the Government is abandoning clear and enforceable safety obligations in favour of an uncertain, complex and potentially protracted enforcement regime.

1.76 The importance of retaining mandatory codes and standards was also underscored by grieving parents Mia Bannister, Wayne Holdsworth and Emma Mason, all of whom supported the need for enforceable obligations on online service providers.[31] Coalition senators pay tribute to their extraordinary courage and tireless advocacy in the face of unimaginable loss. In honouring the memory

---

30 eSafety Commissioner, *Submission 129*, p. 5.

31 Ms Mia Bannister, Private capacity, *Proof Committee Hansard*, 9 November 2026, p. 6; Mr Wayne Holdsworth, Founder, SmackTalk, *Proof Committee Hansard*, 9 November 2026, p. 6; Ms Emma Mason, Private capacity, *Proof Committee Hansard*, 9 November 2026, p. 6.

of Ollie, Mac and Tilly, we share their unwavering commitment to protecting Australian children from online harm.

1.77 It is therefore particularly concerning that legislation purportedly designed to make the online world safer risks weakening the very protections on which Australian children and their families should be able to rely.

Covert accounts and surveillance

1.78 Proposed sections 205G to 205L permit the Commissioner and approved researchers to operate online under false or fictitious identities. While approved researchers may use these accounts for online safety research, the Commissioner's power extends to the performance of any function or exercise of any power under the Online Safety Act. The bill also provides civil immunity for acts done in good faith.

1.79 The Commissioner has indicated that covert accounts are intended to test online services. However, the bill does not confine her powers to that purpose or contain the same authorisation, reporting and audit safeguards that apply to assumed identities under Part IAC of the *Crimes Act 1914*.

1.80 The AHRC warned that the provisions could support activities that:

> … influence online discussions, alter the information environment experienced by users, or promote particular messages or content.[32]

1.81 The bill also makes the Commissioner an enforcement body under the *Privacy Act 1988* and expands the range of Commonwealth entities to which information may be disclosed under section 212 of the Online Safety Act. The Institute of Public Affairs raised concerns about the potential collection and sharing of sensitive information, including political opinions and biometric data.

1.82 The capacity of a civilian regulator to operate covertly online, alongside expanded information-gathering and sharing powers, raises serious questions about the protection of Australians' privacy and freedom of expression.

1.83 Professor Michael Shellenberger, CBR Chair of Politics, Censorship and Free Speech at the University of Austin, described the bill as 'by far the most radical censorship legislation I've ever seen' and characterised the sock puppet provisions as 'quite shocking'.

1.84 Professor Shellenberger highlighted the hypocrisy of a government which previously sought to crack down on anonymous online accounts now seeking the power to operate such accounts itself. Most alarmingly, he warned that these powers could be used to 'spy on citizens, create a chilling effect among social

---

[32] Australian Human Rights Commission, *Submission 58*, p. 15.

media platforms and, essentially, have the power to run informational warfare with hidden, secretive propaganda'.[33]

A poorly defined duty risks a complex web of legal disputes

1.85 Under proposed section 26 of the bill, online service providers must take appropriate action to ensure a safe online environment, including taking effective measures to mitigate identified risks. The bill removes the exposure draft's express qualification that this duty be discharged so far as is reasonably practicable. Further, under proposed subsection 26A(3), the cost of any action or measures must not be taken into account.

1.86 The imposition of such a poorly defined legal duty, backed by substantial civil penalties, creates enormous regulatory uncertainty. While the bill sets out a number of matters to be considered in determining what constitutes appropriate action, it fails to establish clear, objective and enforceable minimum standards against which compliance can be assessed.

1.87 The difficulties in enforcing the social media minimum age laws should serve as a salutary warning to the government. Under section 63D of the Online Safety Act, social media platforms are required to take 'reasonable steps' to prevent children under 16 from holding accounts. Despite compelling evidence that large numbers of children continue to hold social media accounts, establishing a breach of the law has proven to be a complex and protracted exercise.

1.88 At Senate Estimates on 27 May 2026, the Commissioner confirmed she had retained an external legal team to assist with investigations and potential enforcement action, acknowledging that 'systemic non-compliance needs to be proven in court with solid evidence and complex legal proceedings'.

1.89 If establishing non-compliance with a relatively narrow statutory obligation is so challenging, the difficulties in enforcing a sweeping Digital Duty of Care across vast sections of the Australian economy, encompassing a broad and ill-defined range of online harms, are likely to be exponentially greater.

1.90 In abolishing the existing mandatory industry codes and standards and relying on non-binding regulatory guidance, the government is compounding this uncertainty. Online service providers will have no equivalent set of enforceable minimum standards on which they can rely, while the regulator will face a substantially more complex evidentiary burden in establishing breaches of the duty.

1.91 In the view of Coalition senators, the government is walking blindly into a complex web of legal disputes, protracted investigations, costly litigation and

---

[33] Mr Michael Shellenberger, Publisher, Public, *Proof Committee Hansard*, 9 November 2026, pp. 60 and 62.

regulatory uncertainty, at the expense of delivering effective online safety protections for Australians.

A serious risk to privacy and private communications

1.92 The Government removed an express requirement to consider privacy impacts from the exposure draft. The Office of the Australian Information Commissioner (OAIC) and the AHRC both raised concerns about this omission. Assurances in the Explanatory Memorandum do not substitute for an express statutory safeguard.

1.93 The distinction between duties owed to adults and children may also drive much wider use of age assurance, potentially resulting in the collection of personal information from adults as well as children. The OAIC warned that these systems may handle sensitive information, including biometric templates, and noted that:

> … the Bill does not include privacy safeguards for the destruction of personal information collected for age assurance purposes.[34]

1.94 Google warned that the bill could extend age assurance and proactive content scanning to messaging, email and private file storage. The NSW Council for Civil Liberties raised concerns about automated interception or analysis of private communications. The potential for data breaches compounds these concerns.

1.95 Coalition senators support proportionate age assurance where it is necessary to protect children from specified harms. However, the protection of Australians' personal information, including private communications, must be a central consideration in the design of any new online safety regime.

Trojan horse for misinformation and disinformation laws

1.96 The Government's previous misinformation and disinformation legislation was abandoned in 2024. Coalition senators are concerned that the breadth of the new duty and the powers conferred by the bill could be used to pursue similar objectives without the Parliament expressly legislating for them.

1.97 As referenced above, Prime Minister Anthony Albanese linked the reforms to broader concerns about misinformation, disinformation and political polarisation:

> The truth is this is having an impact on our entire society and how it functions with misinformation, disinformation, with the increased polarisation that we're seeing as well in the political system, where people are moving away from the centre and more and more to the extremes, be they of the left or the right. And that is why we think that this is a very positive move that's being put forward.

---

34 Office of the Australian Information Commissioner (OAIC), *Submission 48,* p. 3.

1.98 The AHRC expressed concern about political calls for the legislation to be used to limit the reach of particular political messages:

> The purpose of the DDC must be to reduce foreseeable harm arising from the design and operation of online services, not to influence which political views people encounter.[35]

Labor's rushed legislative process

1.99 Consultation on the exposure draft closed on 22 September 2026 after only two weeks. This was half the minimum one-month consultation period referred to in the Department of the Prime Minister and Cabinet's Legislation Handbook. The consultation process was further constrained by a five-page limit on submissions.

1.100 Significant changes were made between the exposure draft and the introduction of the bill, including the removal of express consideration of privacy and the qualification that the duty be satisfied so far as is reasonably practicable. On 28 October 2026, a further 15 amendments were made in the House of Representatives, including a late change concerning Class 2 material. Debate was guillotined.

1.101 The breadth of the bill makes the lack of consultation particularly concerning. Professor Anne Twomey warned:

> I suspect that many of those who will be seriously affected by this bill, if passed, have no idea and therefore have not made submissions to the Committee.[36]

1.102 Much of the detail of the new scheme, including regulatory guidance and legislative instruments, remains to be developed. The Commissioner's term expires in January 2027. Parliament is being asked to approve a regulatory framework whose practical operation will depend substantially on decisions made by her successor.

1.103 The fact that the Commissioner herself has identified significant defects and called for further changes after the bill passed the House is a serious indictment of the Government's legislative process.

Insufficient resources to enforce existing and new obligations

1.104 The Commissioner advised that the duty would require more intensive supervision, monitoring and enforcement than the existing codes and standards. However, the Explanatory Memorandum identifies only a minor impact on Commonwealth expenditure. The Government has not announced additional funding for eSafety to implement the bill.

---

35 Australian Human Rights Commission, *Submission 58*, p. 25.

36 Anne Twomey Professor Emerita, *Submission 132*, p. 6.

1.105 In 2025–26, the eSafety Commission received 40,030 complaints, an increase of 38 per cent on the previous year, while resourcing levels remained comparatively static. The Commissioner's annual report noted that increasing complaints and limited resources had curtailed proactive investigations.

1.106 The consequences of inadequate enforcement are especially serious in relation to online radicalisation. The Australian Federal Police Commissioner told Senate Estimates that 55 youth counter-terrorism cases between 2020 and 2025 involved boys aged 12 to 17 who had been radicalised wholly or partly online. eSafety's proceedings against Telegram also allege significant delays in the removal of terrorist and abhorrent violent material.

1.107 The Commissioner made the following important point:

> Regulation without enforcement is merely a suggestion. If Parliament intends for Australians to be protected from online harms it must effectively resource the regulator with both staffing and a litigation budget to deliver on enforcement of the digital duty of care obligations.

1.108 Coalition senators reiterate that effective enforcement of existing online safety laws should be a priority. Expanding the regulator's responsibilities while abolishing specific safeguards risks undermining, rather than improving, the protection of Australians online.

Far-reaching powers to control user empowerment tools

1.109 There is a legitimate debate about whether Australians should be able to switch algorithmic profiling on or off. However, no government should dictate what Australians see online by replacing one compulsory system with another.

1.110 Coalition senators support giving Australians more control over the content they see online, including greater algorithmic transparency and access to non-profiled feeds. However, these objectives do not justify the breadth of the Minister's powers under the bill.

1.111 Proposed section 27A allows the Minister, by legislative instrument, to require a specified online service to provide a specified user empowerment tool and to prescribe requirements relating to such tools. These tools are not confined to social media services or recommender algorithms.

1.112 The bill prohibits the Minister from taking into account the material accessible to or delivered to a user. However, regulation of recommendation systems and default feed settings can still affect the visibility, distribution and reach of content. Professor Twomey identified the particular implications for electoral advertising:

> The way these political advertisements are targeted during election campaigns has the potential to alter outcomes. This raises the important

> question of how ministerial control over empowerment tools may potentially operate in relation to political advertising.[37]

1.113 Proposed sections 25C and 25G also create uncertainty for providers by linking a safe online environment for children to design features deemed to have negative behavioural impacts, including recommender and logged-in features. The Minister may prescribe further design features. The impact of these provisions on legitimate recommendation services has not been adequately assessed.

1.114 Recommendation systems play a critical role in helping Australian small businesses reach new customers, from personalised social media feeds to services such as Google Maps which recommend local restaurants, retailers and other businesses. Yet the bill makes no adequate distinction between recommender systems which amplify harmful content and those which provide significant economic and consumer benefits.

1.115 The Council of Small Business Organisations Australia (COSBOA) raised concerns about the failure to adequately assess the impact of recommender algorithm controls on small businesses. As COSBOA CEO Skye Cappuccio warned:

> … being recommended to someone who doesn't already follow you can be the difference between reaching a new customer and never appearing on their radar.[38]

1.116 Coalition senators are deeply concerned that the bill's indiscriminate treatment of recommender systems risks damaging small business revenue and competitiveness, without any demonstrable online safety benefit.

Another red tape hit job on small business

1.117 The bill extends well beyond large social media platforms. Nine categories of online services are covered, including hosting, search engines, messaging and email services, and AI services. There is no general size threshold for the duty. The inquiry heard that even a small business website with limited functionality may be captured by the risk assessment requirements.

1.118 COSBOA submitted that:

> …a local tradesperson whose website simply describes services and accepts bookings may be required to prepare and maintain a formal written risk

---

37 Anne Twomey Professor Emerita, *Submission 132*, p. 3.

38 Council of Small Business Organisations Australia (COSBOA), 'New online safety laws could create new hurdles for small business', *Media Release*, https://cosboa.org.au/post/new-online-safety-laws-could-create-new-hurdles-for-small-business/ (accessed 20 November 2026).

> assessment, despite having limited functionality and minimal exposure to online harms.[39]

1.119 The risk assessment obligation, including annual assessments and six-year record retention, will impose disproportionate costs on genuinely low-risk businesses, charities, schools and community organisations. The Australian Computer Society also raised the question of the competence required of those conducting risk assessments.

1.120 The National Catholic Education Commission and Independent SchoolsAustralia raised the possibility that non-government schools could be covered by the duty while government schools are not. Churches may also face regulatory uncertainty in relation to material published on their own websites.

1.121 The impact analysis estimates an increase in average regulatory costs for Australian businesses of $1.408 million per year over ten years. Coalition senators question whether this estimate adequately reflects the breadth of the bill and the cost of ongoing compliance, particularly for small organisations without specialist legal or technical staff.

1.122 Professor Twomey warned of the unintended consequences for competition if smaller providers cannot afford to comply:

> The effect may be to increase the dominance of large global platforms.[40]

1.123 Coalition senators note the committee's recommendation that the bill's scope be narrowed to exempt low-risk websites and online services. That such a basic defect was not addressed before the bill passed the House of Representatives further demonstrates the inadequacy of the Government's consultation and policy development.

A civil right of action requires rigorous legal analysis

1.124 Coalition senators note the committee's recommendation that the bill be amended to establish a civil right of action for individuals who suffer harm or loss as a consequence of a breach of the Digital Duty of Care.

1.125 While Coalition senators strongly support victims of online harm having access to effective remedies and appropriate avenues for redress, the introduction of a new statutory cause of action is a significant legal reform which warrants detailed examination and proper consultation.

1.126 The existing Online Safety Act provides for a regulatory enforcement framework administered by the Commissioner. Depending on the

---

39 Council of Small Business Organisations Australia (COSBOA), *Submission 65,* p. 3.

40 Anne Twomey Professor Emerita, *Submission 132,* p. 2.

circumstances, individuals may also have access to remedies under existing laws, including negligence, defamation, privacy and discrimination law.

1.127 The establishment of a new civil right of action raises complex legal questions concerning the scope of liability, the threshold for actionable harm, causation, damages, the potential for class actions and the interaction with existing laws.

1.128 Given the vague and subjective nature of the harms prescribed in the bill, exposing online service providers to civil litigation, in addition to substantial regulatory penalties, could further incentivise the censorship of lawful speech. There is also a risk that such a mechanism could be weaponised by individuals or organisations seeking to suppress legitimate public debate.

1.129 The legal, financial and broader public policy consequences of this proposal have not been adequately examined by the committee. A reform of this magnitude should be subject to rigorous legal analysis, a comprehensive regulatory impact assessment and meaningful stakeholder consultation.

1.130 Such a significant change to Australian law cannot be the product of policy on the run. Accordingly, while supportive of the objective of ensuring that victims of online harm have access to appropriate redress, Coalition senators are not in a position to support this recommendation.

Conclusion

1.131 The Coalition supports strong online safety laws and further measures to protect children. The bill, however, weakens the enforceable protections already in place, creates serious risks to freedom of expression and privacy, confers extensive powers on the minister and the Commissioner, and exposes small businesses and community organisations to disproportionate compliance costs.

1.132 One of the central arguments deployed by the Government in defence of this bill is that it will empower users. However, to the contrary, the legislation does not guarantee users control over their feed. Furthermore, the expansive and invasive nature of the regulation, privacy concerns and penalties instead risk entrenching the control and regulation of free speech by large technology companies seeking to over-correct to manage the risk of penalties.

1.133 Dany Elachi, co-founder of the Heads Up Alliance, which campaigned for the social media minimum age, told the committee that the Alliance:

> … very much wants a digital duty of care for the protection of children but is opposed to this nebulous piece of legislation with the fingerprints of illiberalism all over it.[41]

[41] Mr Dany Elachi, Founder, Heads Up Alliance, *Proof Committee Hansard*, 9 November 2026, p. 14.

1.134 Coalition senators consider that stronger online safety laws must be based on clearly defined harms, enforceable obligations and appropriate safeguards to ensure the protection of free speech. The bill seriously fails that test.

Recommendation 1

1.135 That the Online Safety Amendment (Digital Duty of Care) Bill 2026 not be passed.

Senator the Hon Sarah Henderson
Member
Liberal Senator for Victoria

Senator Dean Smith
Member
Liberal Senator for Western Australia

Australian Greens' Additional Comments

1.1 Every Australian deserves to be safe online and free to choose what they want to see in their social media feeds.

1.2 The Government's legislation needs fixing to ensure every Australian has the right to be safe online and to change big tech's business model of harm.

1.3 All tech platforms should have a legally enforceable duty of care to their users - a requirement to keep their customers safe from harm and dangerous products.

1.4 For too long big tech and social media giants have been able to avoid these basic obligations to their users online. Big tech has made billions of dollars in profits off technology that is deliberately designed to be addictive and to keep people scrolling, even when the content being consumed is harmful and dangerous.

1.5 These are some of the wealthiest companies in the world, who earn hundreds of billions of dollars. Social media companies must be held responsible for design features that cause harm to their users and exploit the most vulnerable, like young people, for profit and reach.

1.6 The Australian Greens have long campaigned for a Digital Duty of Care - but these laws must have the teeth and enforcement that will actually change industry behaviour. It's not enough to say kids shouldn't be on these platforms - these platforms need to be safe for all users, kids and adults alike.

1.7 Just like any other product sold in shops in cities and towns across the country, tech platforms must be legally required to ensure their products are safe to use. We wouldn't accept a faulty toy that might hurt our kids or eat contaminated food - so why should we accept an online world that uses addictive technology that radicalises our children with isolating and toxic echo chambers, and profits off the clickbait of outrage and hatred?

1.8 Big tech must be treated just like any other industry. They must actively assess the risks their platforms pose, and be proactive in stopping harm from occurring - not profiting off it. The time for making money off design features that intentionally addict and harm Australia's most vulnerable, with impunity, must end.

1.9 The consequences for big tech must be big enough to hurt their business model. It's not enough to just give these companies a slap on the wrist. They need to be held to account to make their products safe, and when the product causes serious harm, it should mean a serious hit to their bottom line.

Private right of action - Australians should have the right to sue for damages.

1.10 **The Greens are proposing a private right of action, so when people are seriously harmed online, they have an avenue to seek compensation.** The threat of being liable for harms caused through civil action will be an important lever in ensuring the tech platforms take the digital duty of care seriously.

1.11 Success in civil litigation in the US has resulted in billions of dollars in compensation payouts, and forced product design changes that actually protect users. Australians deserve the same rights as Americans to take action against big tech.

1.12 These platforms will not change out of the goodness of their own hearts. They must understand that safe products are a mandatory requirement if they want to do business on Australian soil and profit off Australians. To do this, we need a private right to action, with compensation.

Fines a percentage of Global Revenue - hitting big tech where it hurts, their profits

1.13 **The Greens are proposing tying fines for breaches of the duty to a portion of global revenue.** In the context of multi billion dollar companies, like Meta, Google, and TikTok, fines as currently set out in the legislation barely scratch the surface. In the last financial year alone, Meta reported global revenue of USD$201 billion. Fines for breaches of the government's proposed Digital Duty of Care represent a tiny fraction of their total revenue.

1.14 There is a real risk that fines, as set in the legislation, will not disincentivise breaches of the duty, but instead become the regular cost of doing business on Australian shores.

1.15 Penalties can't just be another number on a balance sheet. Australia must be a part of the global push to introduce meaningful penalties tied to global revenue, and stand alongside other leading nations like the EU, Canada and NZ.

External complaints resolution process

1.16 **The bill must be amended to include an external dispute resolution system.** The committee heard from a number of witnesses who were unable to resolve complaints about their social media accounts through internal dispute systems of individual social media platforms. These poorly moderated systems often leave users with nowhere to go to challenge a decision.

1.17 A commonsense fix for this is to provide Australians with an independent ombudsman that would provide a binding external dispute resolution system. This would give consumers a centralised place to resolve issues with online platforms, just like what's available for so many other industries. The Telecommunication Industry Ombudsman has already proposed to take on

this role, representing a key opportunity to centralise similar tech complaints, like NBN, telcos and data breaches.

Addictive design - ending the doomscroll

1.18 The Government's proposal to let Australians opt-in to recommended content is an important first step in giving users more control, and choice, over their social media use. But giving people more control when and how they use these products requires platforms to be transparent and implement genuine Safety by Design features and policies.

1.19 Social media algorithms are designed to be deliberately addictive, and prioritise divisive, outrage filled content, all with the aim to keep us hooked and get more eyeballs, so they can bombard us with more ads, and extract more money. Doomscrolling is not just a side effect of social media, it is the very business model that drives billions of dollars of profits, to the detriment of Australians' control over their time.

Addictive design must be addressed as a key part of risk assessments and harm mitigation.

Gambling - keeping young people safe

1.20 Gambling is a serious risk to children, and must be actively age assured at the digital door.

1.21 There is no question that gambling is harmful to children. Wagering services are taking advantage of this gaping hole in the system, and grooming young people, especially young boys, into becoming gambling addicts.

1.22 Current regulations blocking children from online wagering services is clearly not working, and betting apps only check ID once upon sign up. After this, there are no requirements to check those placing bets are actually over 18. The current age verification systems aren't working, and with this Bill we can address this issue.

1.23 If the Government is serious about protecting children online, **the bill should be amended to age gate online wagering services at the digital door, and wagering must be considered as harmful when services are conducting risk assessments.**

Transparency for academic research

1.24 The Australian Greens recommend that the Bill is strengthened to include further provisions that enhance researchers' access to critical data and information. Academic research on algorithms, and how platforms operate, is essential to hold big tech to account. The committee heard a number of suggestions around how to ensure this research is protected and further bolstered, including allowing for individuals to donate their own data for

research into online safety, and ensuring further transparency around how platforms are required to share their advertising material in ad libraries.

1.25 **The Bill should be amended to strengthen transparency provisions that provide academic researchers with the information they need to hold big tech to account.**

Recommendations - the Bill must be amended.

Recommendation 1:

1.26 That the Bill be amended to introduce a private right of action, with compensation, so that those who are seriously harmed online have the right to sue online platforms.

Recommendation 2:

1.27 That the Bill be amended to set the rate of fines for breaches of the duty to 10 per cent of a company's global revenue.

Recommendation 3:

1.28 That the Bill be amended to establish an external dispute resolution system for social media platforms.

Recommendation 4:

1.29 That the Bill be amended to explicitly include addictive design in risk assessments.

Recommendation 5:

1.30 That the Bill be amended to list wagering as a harm to children, and online wagering services are age assured at the digital entry point.

Recommendation 6:

1.31 That the Bill be amended to strengthen transparency and data access provisions for academic researchers to investigate online safety.

Senator Sarah Hanson-Young
Deputy Chair
Greens Senator for South Australia

Appendix 1
Submissions and additional information

1 Digital Readiness Lab
2 Social Media Research Institute
3 Carers and Advocates Australia Pty Ltd
4 HarmGuard.org
- Attachment 1

5 3primitives.io
6 Dr Honni van Rijswijk
- 6.1 Supplementary to submission 6

7 Ms Mia Bannister
8 Professor Jason Jacobs
9 Associate Professor Andrew Moshirnia and Dr Amanda Selvarajah
10 Prevention United
11 Dr Aashish Srivastava
12 Libertarian Party (WA)
13 Digital Defence
14 Euroa Connect Inc
15 Doctor Ads Ltd
16 Democracy Counts
17 Protocol Policy Lab Ltd
18 The Computer and Communications Industry Association
19 Soroptimist International Australia Inc
20 Dr Rhonda Small
21 Australian Communications Consumer Action Network (ACCAN)
22 NableU Community Systems Inc.
23 Brighter Websites
24 Dr Vivi Tan
25 Privacy 108
26 Good Things Australia
27 Google
28 TikTok Australia
29 Teach Us Consent
30 National Council of Women Australia
31 Alannah & Madeline Foundation
32 Australians for Science and Freedom
33 Ms Emma Mason
34 The Business Council of Australia (BCA)
35 National Catholic Education Commission
36 FamilyVoice Australia

37 The Information Rights Project
38 With You We Can
39 Relationships Australia
40 Snap Australia
41 Telecommunications Industry Ombudsman
42 National Drug Research Institute, Curtin University
43 Australian Computer Society (ACS)
- 43.1 Supplementary to submission 43

44 SWOP NSW
45 Dr Alexander Hatzikalimnios
46 Coptic Orthodox Diocese of Sydney & Affiliated Regions
47 Australian Services Union
48 Office of the Australian Information Commissioner (OAIC)
49 Alcohol and Drug Foundation
50 International Justice Mission Australia
51 Our Watch
52 The Centre for Excellence in Child & Family Welfare
53 Consumer Policy Research Centre, CHOICE and Consumer Action
54 Free Speech Union of Australia
- 54.1 Supplementary to submission 54

55 NSW Council for Civil Liberties (NSWCCL)
56 Institute of Public Affairs
57 Human Rights Law Centre
58 Australian Human Rights Commission
59 Equality Australia
60 Alliance for Gambling Reform
- 60.1 Supplementary to submission 60

61 Australian Jewish Association
62 Australian Catholic Bishops Conference
63 Anglican Church, Diocese of Sydney
64 Digital Rights Watch
65 Council of Small Business Organisations Australia (COSBOA)
66 Australian Telecommunications Alliance
67 Free TV Australia
68 The Australia Institute
69 Tech Policy Design Institute
70 QUT Digital Media Research Centre
71 ARC Centre of Excellence for Automated Decision-Making and Society
72 Ms Elizabeth Hall
73 Meta
74 Associate Professor Mark Humphery-Jenner and Prosperity Institute
75 Ms Noelle Martin
76 Older Women's Network NSW

77 QNews
78 Consumer Choice Center
79 Duolingo
80 Information Technology and Innovation Foundation (ITIF)
81 Zonta Australia
82 Women's Services Network
83 National Aboriginal and Torres Strait Islander Women's Alliance (NATSIWA)
84 Associate Professor Joel Scanlan, Professor Jeremy Prichard, Dr Rachel Baird and Dr Nina Hudson
85 Gender Justice Australia
86 Penington Institute
87 Australian Alcohol and Other Drugs Council
88 ARACY - Australian Research Alliance for Children and Youth
89 Bravehearts
90 Digital Industry Group Inc (DIGI)
91 Bluelight Communities Ltd
92 Match Group
93 Interactive Games & Entertainment Association (IGEA)
94 AMPS
95 Women's Legal Service NSW
96 Suicide Prevention Australia
97 Y Australia
98 Australians vs. The Agenda
99 Australian Christian Lobby
100 yourtown
101 Trans Justice Project
102 The LEGO Group
103 Dr Rob Nicholls
104 Business Software Alliance
- 104.1 Supplementary to submission 104

105 Center for Cybersecurity Policy and Law
106 Association for Competitive Technology (ACT)
107 Bumble Inc.
108 liber-net
109 Freedom for Faith
110 Primary Purpose Advisory
111 Minderoo Foundation
112 Health Equity Matters
113 National Foundation for Australian Women (NFAW)
114 National Association of People with HIV Australia
115 The Matilda Centre for Research in Mental Health and Substance Use
116 Independent Schools Australia
117 National Centre for Clinical Research on Emerging Drugs

118 Associate Professor Darcy W. E. Allen and Professor Chris Berg
119 Alcohol Tobacco and Other Drug Association ACT
120 UNICEF Australia
121 Scarlet Alliance, National Sex Workers Association
122 Your Community Health
123 Centre for Media Transition
124 Canberra Declaration
125 Repro Uncensored
126 YouTour Pty Ltd
127 Internet Association of Australia
128 Arnold Bloch Leibler, ECAJ, ZFA, NSW JBOD, NCJWA, JCCV, Dor Foundation & AIJAC
129 eSafety Commissioner
130 Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts
131 Streaming for Australia
132 Anne Twomey, Professor Emerita
133 SBS
134 Working with Women Alliance
135 Amplify51 Limited
136 Dr Isabelle Volpe, Professor Kate Seear, Laura Purcell, Dr Adrian Farrugia, Professor Joanne Bryant, Dr Gabriel Caluzzi
137 Australian Lawyers Alliance
138 Slater and Gordon Lawyers
139 Jesuit Social Services
140 Human Rights Law Alliance
141 Headspace National
- Attachment 1

142 Global Institute for Women's Leadership at the ANU
143 Liberty Victoria
144 Centre for Multicultural Youth
145 Dr Mark Fowler
146 Wesley Mission
147 Youth Support and Advocacy Service
148 The Australian Lobby Group
149 GetUp
150 Office of Australia's Special Envoy to Combat Antisemitism
- Attachment 1

151 Australian Broadcasting Corporation
152 South Australian Network of Drug and Alcohol Services (SANDAS)
153 QuIVAA and QuIHN
154 QuIVAA
155 Australian Retail Council

156 Australian Injecting and Illicit Drug Users League (AIVL)
157 Australian Muslim Advocacy Network
158 People Standing United Australia (PSUA)
159 Harm Reduction Australia
160 Consumer Electronics Suppliers Association
161 Maurice Blackburn
162 FinTech Australia
163 Children and Media Australia
164 The Twelve (HIV, STI and BBV joint sector submission)
165 Benjamin Chidiac
166 Hello Sunday Morning
167 Reset.Tech Australia
168 Collective Shout
169 Name Withheld
- 169.1 Supplementary to submission 169

170 Orygen
171 Darren Edwards
172 Youth Law Australia
173 Middle Tech Australia
174 Netflix
175 X Corp
176 Tech Council of Australia
177 Australian Publishers Association
178 Guy Leggett
179 Dr John Bellavance
180 Firefly Medium
181 Law Council of Australia
182 Mr Zen Dodd
- 182.1 Supplementary to submission 182

Additional Information

1 Opening Statement, Right Reverend Dr Michael Stead, Bishop of South Sydney, Anglican Church Diocese of Sydney, received 11 November 2026
2 Opening Statement, International Justice Mission Australia, received 13 November 2026
3 Petition, International Justice Mission Australia, received 13 November 2026
4 Research Note, Institute of Public Affairs, received 10 November 2026
5 Supplement to hearing evidence, Digital Readiness Lab, received 16 November 2026

Answer to Question on Notice

1 Tech Policy Design Institute, Answers to questions taken on notice, public hearing 10 November 2026 (received 10 November 2026)

2 Reset.Tech Australia, Answers to questions taken on notice, public hearing 10 November 2026 (received 11 November 2026)

3 Internet Association of Australia Ltd, Answers to questions taken on notice, public hearing 9 November 2026 (received 12 November 2022)

4 Teach Us Consent, Answers to questions taken on notice, public hearing 9 November 2026 (received 12 November 2026)

5 ARC Centre of Excellence on Automated Decision-Making and Society, Answers to questions taken on notice, public hearing 10 November 2026 (received 13 November 2026)

6 TikTok Australia, Answers to questions taken on notice, public hearing 9 November 2026; Answers to written questions on notice from Senator David Pocock, sent 12 November 2026 (received 13 November 2026)

7 International Justice Mission Australia, Answers to questions taken on notice, public hearing 9 November 2026 (received 13 November 2026)

8 Snap Aus Pty Ltd, Answers to questions taken on notice, public hearing 9 November 2026 (received 13 November 2026)

9 Arnold Bloch Leibler, Answers to questions taken on notice, public hearing 10 November 2026 (received 13 November 2026)

10 Equality Australia, Answers to questions taken on notice, public hearing 10 November 2026 (received 13 November 2026)

11 Council of Small Business Organisations Australia (COSBOA), Answers to questions taken on notice, public hearing 9 November 2026 (received 14 November 2026)

12 Australia Institute, Answers to questions taken on notice, public hearing 10 November 2026 (received 15 November 2026)

13 Our Watch, Answers to questions taken on notice, public hearing 9 November2026 (received 16 November 2026)

14 Streaming for Australia, Answers to questions taken on notice, public hearing 10 November 2026 (received 16 November 2026)

15 Australian Communications Consumer Action Network (ACCAN), Answers to questions taken on notice, public hearing 9 November 2026 (received 16 November 2026)

16 eSafety Commissioner, Answers to questions taken on notice, public hearing 10 November 2026 (received 16 November 2026)

17 Snap Aus Pty Ltd, Answers to written questions on notice from Senator David Pocock, sent 12 November 2026 (received 16 November 2026)

18 Google, Answers to questions taken on notice, public hearing 9 November 2026; Answers to written questions on notice from Senator David Pocock, sent 12 November 2026 (received 17 November 2026)

19 Free TV Australia, Answers to questions taken on notice, public hearing 10 November 2026; Answers to written questions on notice from Senator David Pocock, sent 12 November 2026 (received 17 November 2026)

20 Streaming for Australia, Answers to written questions on notice from Senator David Pocock, sent 12 November 2026 (received 17 November 2026)

21 Australian Human Rights Commission, Answers to questions taken on notice, public hearing 9 November 2026 (received 17 November 2026)

22 SBS, Answers to written questions on notice from Senator David Pocock, sent 12 November 2026 (received 17 November 2026)

23 Meta, Answers to questions taken on notice, public hearing 9 November 2026; Answers to written questions on notice from Senator David Pocock, sent 12 November 2026 (received 16 November 2026)

24 Free Speech Union of Australia, Answers to written questions on notice from Senator Henderson, sent 10 November 2026 (received 12 November 2026)

Form Letters

1 Representative sample of campaign and petition material, approximately 3700 items of correspondence received.

Tabled Documents

1 Mr Jamie Crosby, Chief Executive Officer, Centre for Excellence in Child and Family Welfare, Opening Statement (tabled 9 November 2026)

2 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, Opening Statement (tabled 9 November 2026)

3 Mr Casey Tonkin, Policy Advisor, Australian Computer Society, Opening Statement (tabled 9 November 2026)

4 Ms Carol Bennett, Chief Executive Officer, Australian Communications Consumer Action Network, Opening Statement (tabled 9 November 2026)

5 Ms Chandni Gupta, Chief Executive Officer and Digital Policy Director, Consumer Policy Research Centre, Opening Statement (tabled 9 November 2026)

6 Dr Jennifer Duxbury, Interim Managing Director, Digital Industry Group Inc, Opening Statement (tabled 9 November 2026)

7 Ms Narelle Clark, Chief Executive Officer, Internet Association of Australia, Opening Statement (tabled 9 November 2026)

8 Ms Zara Cooper, Chief Executive Officer, Digital Defence, Opening Statement (tabled 9 November 2026)

9 Ms Jessika Lofstedt, Head of Public Policy, TikTok Australia, Opening Statement (tabled 9 November 2026)

10 Mrs Skye Cappuccio, Chief Executive Officer, Council of Small Business Organisations Australia, Opening Statement (tabled 9 November 2026)

11 Mr Ben Au, Head of Public Policy, ANZ, Snap Inc, Opening Statement (9 November 2026)

12 Mr Chris Merritt, Vice President, Rule of Law Institute, Opening Statement (tabled 9 November 2026)

13 Dr Lorraine Finlay, Human Rights Commissioner, Australian Human Rights Commission, Opening Statement (tabled 9 November 2026)

14 Ms Anna Brown OAM, Chief Executive Officer, Equality Australia, Opening Statement (tabled 10 November 2026)

15 Ms Sunita Bose, Chief Executive Officer, Alliance for Gambling Reform, Opening Statement (tabled 10 November 2026)

16 Mr Paul Muller, Convenor, Streaming for Australia, Opening Statement (tabled 10 November 2026)

17 Mr Luke Coleman, Chief Executive Officer, Australian Telecommunications Alliance, Opening Statement (tabled 10 November 2026)

18 Ms Cynthia Gebert, Ombudsman, Telecommunications Industry Ombudsman, Opening Statement, (tabled 10 November 2026)

19 Ms Elizabeth Hall, Opening Statement (tabled 10 November 2026)

20 Associate Professor Honni van Rijswijk, Opening Statement (tabled 10 November 2026)

21 Mr Robert Gregory, President, Australian Jewish Association, Opening Statement (tabled 10 November 2026)

22 Mr Peter Wertheim AM, Co-Chief Executive Officer, Executive Council of Australian Jewry, Opening Statement (tabled 10 November 2026)

23 Professor Christine Parker, Chief Investigator, ARC Centre of Excellence for Automated Decision-Making and Society, Opening Statement (tabled 10 November 2026)

24 Ms Rinat Strahlhofer, Founder, Digital Readiness Lab, Opening Statement (tabled 10 November 2026)

25 Professor Daniel Angus, Director, QUT Digital Media Research Centre, Opening Statement (tabled 10 November 2026)

26 Ms Bridget Fair, Chief Executive Officer, Free TV Australia, Opening Statement (tabled 10 November 2026)

27 Dr Rys Farthing, Chief Research Officer, Reset.Tech Australia, Opening Statement (tabled 10 November 2026)

28 Professor Nicholas Carah, Deputy Director, Australian Internet Observatory, Opening Statement (tabled 10 November 2026)

29 Professor Daniel Angus, Private Capacity, Opening Statement (tabled 10 November 2026)

30 Ms Julie Inman-Grant PSM, eSafety Commissioner, Office of the eSafety Commissioner, Opening Statement (tabled 10 November 2026)

31 Dr Andrew Bushnell, Director, Law and Freedom Program, Opening Statement (tabled 9 November 2026)

32 Dr Romy Listo, Manager, Prevention Strategy and Policy, Opening Statement (tabled 9 November 2026)

33 Dr Rob Nicholls, Senior Research Associate, University of Technology Sydney, Opening Statement (tabled 10 November 2026)

34 Bishop Tony Percy, Auxiliary Bishop of Sydney, and Member of the Bishops Commission for Life, Family and Public Engagement, Australian Catholic Bishops Conference, Opening Statement (tabled 10 November 2026)

35 Mr Tom Sulston, Head of Policy, Digital Rights Watch, Opening Statement (tabled 9 November 2026)

Appendix 2
Public hearings and witnesses

Monday 9 November 2026
Committee Room 2S1
Parliament House
Canberra

Ms Emma Mason, Private capacity

Ms Mia Bannister, Private capacity

SmackTalk Ltd

- Mr Wayne Holdsworth, Founder (via videoconference)

Teach Us Consent

- Ms Chanel Contos, Chief Executive Officer and Founder (via videoconference)

The Centre for Excellence in Child & Family Welfare

- Mr Jamie Crosby, Chief Executive Officer

The Alannah & Madeline Foundation

- Ms Sarah Davies, Chief Executive Officer (via videoconference)
- Ms Ariana Kurzeme, Director, Policy and Prevention (via videoconference)

International Justice Mission Australia

- Mr David Braga, Chief Executive Officer
- Ms Carolyn Halliday, Chief Advocacy Officer

Heads Up Alliance

- Mr Dany Elachi, Founder

Our Watch

- Dr Romy Listo, Manager, Prevention Strategy and Policy (via videoconference)

Digital Rights Watch

- Mr Tom Sulston, Head of Policy (via videoconference)

Australian Computer Society

- Mr Casey Tonkin, Policy Advisor

Australian Communications Consumer Action Network

- Ms Carol Bennett, Chief Executive Officer (via videoconference)
- Dr Gareth Downing, Deputy Chief Executive Officer (via videoconference)

Consumer Policy Research Centre

- Ms Chandni Gupta, Chief Executive Officer and Digital Policy Director (via videoconference)

Digital Industry Group Inc

- Dr Jennifer Duxbury, Interim Managing Director

Internet Association of Australia

- Ms Narelle Clark, Chief Executive Officer (via videoconference)

Digital Defence

- Ms Zara Cooper, Chief Executive Officer (via videoconference)

Meta

- Mrs Mia Garlick, Regional Director (via videoconference)

Google

- Ms Rachel Lord, Senior Manager, YouTube Government Affairs and Public Policy (via videoconference)

TikTok Australia

- Ms Jessika Lofstedt, Head of Public Policy (via videoconference)

Snap Inc

- Mr Ben Au, Head of Public Policy, ANZ (via videoconference)

Free Speech Union of Australia

- Dr Reuben Kirkham, Director

Council of Small Business Organisations Australia

- Mrs Skye Cappuccio, Chief Executive Officer

Institute of Public Affairs

- Dr Andrew Bushnell, Director, Law and Freedom Program
- Ms Margaret Chambers, Research Fellow
- Mr Daniel Wild, Deputy Executive Director

Mr Michael Shellenberger, Private capacity

Human Rights Law Centre

- Mr Arif Hussein, Senior Lawyer (via videoconference)

Rule of Law Institute

- Mr Chris Merritt, Vice President (via videoconference)

Australian Human Rights Commission

- Dr Lorraine Finlay, Human Rights Commissioner (via videoconference)
- Dr Anna Cody, Sex Discrimination Commissioner (via videoconference)
- Mr Hugh de Kretser, President (via videoconference)

Tuesday 10 November 2026

Committee Room 2S1
Parliament House
Canberra

Equality Australia

- Ms Anna Brown OAM, Chief Executive Officer (via videoconference)
- Alex Lia, Senior Legal Policy Advisor (via videoconference)

Working with Women Alliance

- Dr Gemma Killen, Executive Director
- Ms Darcie Newland, Senior Policy Officer
- Ms Lara Freidin, Member and Director of Wildfire Advisory (via videoconference)

Alliance for Gambling Reform

- Ms Sunita Bose, Chief Executive Officer (via videoconference)
- Mr Mark Kempster, Lived Experience Advocate (via videoconference)

Australian Jewish Association

- Mr Robert Gregory, President (via videoconference)

Anglican Church Diocese of Sydney

- Right Reverend Dr Michael Stead, Bishop of South Sydney (via videoconference)

Australian Catholic Bishops Conference

- Bishop Tony Percy, Auxiliary Bishop of Sydney, and Member of the Bishops Commission for Life, Family and Public Engagement (via videoconference)

Executive Council of Australian Jewry

- Mr Peter Wertheim AM, Co-Chief Executive Officer

Arnold Bloch Leibler

- Mr Leon Zwier, Partner

Streaming for Australia

- Mr Paul Muller, Convenor (via videoconference)

Free TV Australia

- Ms Bridget Fair, Chief Executive Officer (via videoconference)
- Mr Michael Coonan, Director of Policy (via videoconference)

SBS

- Ms Clare O'Neil, Director, Corporate Affairs (via videoconference)
- Ms Sophie Kowald, A/g Head of Government, Policy and Regulatory Affairs (via videoconference)

Australian Telecommunications Alliance

- Mr Luke Coleman, Chief Executive Officer (via videoconference)
- Mrs Christiane Gillespie-Jones, Deputy Chief Executive Officer (via videoconference)

Digital Readiness Lab

- Ms Rinat Strahlhofer, Founder
- Dr Sarah Howe, Independent Developmental Research Psychologist

Reset.Tech Australia

- Dr Rys Farthing, Chief Research Officer (via videoconference)

The Australia Institute

- Mr Josh Bornstein, Director, Corporate Regulation

Telecommunications Industry Ombudsman

- Ms Cynthia Gebert, Ombudsman

Dr Rob Nicholls, Private capacity

Ms Elizabeth Hall, Private capacity

Tech Policy Design Institute

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

QUT Digital Media Research Centre

- Professor Daniel Angus, Director

ARC Centre of Excellence for Automated Decision-Making and Society

- Professor Christine Parker, Chief Investigator
- Professor Kimberlee Weatherall, Chief Investigator

Professor Nicholas Carah, Private capacity

Professor Daniel Angus, Private capacity

Associate Professor Honni van Rijswijk, Private capacity

Associate Professor Mark Humphery-Jenner, Private capacity

Office of the Australian Information Commissioner

- Ms Carly Kind, Privacy Commissioner (via videoconference)

Office of the eSafety Commissioner

- Ms Julie Inman-Grant PSM, eSafety Commissioner (via videoconference)
- Ms Ashley Katz, A/g Executive Manager, Strategy, Engagement and Research Branch (via videoconference)
- Ms Josephine Kirby, A/g Manager, Strategic Policy and Tech Futures Section (via videoconference)
- Mr Richard Fleming, General Counsel (via videoconference)
- Ms Heidi Snell, General Manager, Regulatory Operations Group (via videoconference)
- Ms Kathryn King, General Manager, Corporate and Strategy Group (via videoconference)

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

- Ms Clare Chapple, First Assistant Secretary, Digital Policy, Online Safety and Classification Division
- Mr Andrew Hyles, Assistant Secretary, Digital Platforms Policy Branch
- Mr Nolan Noeng, Acting Assistant Secretary, Online Safety Branch
- Ms Rebecca Day, Director, Online Safety Reform Section, Digital Platforms Policy Branch