Law Council
OF AUSTRALIA

Statutory Review of the *Online Safety Act 2021*

Ms Delia Rickard PSM, Reviewer

2 July 2024

Telephone **+61 2 6246 3788**
Email **mail@lawcouncil.au**
PO Box 5350, Braddon ACT 2612
Level 1, MODE3, 24 Lonsdale Street,
Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

Table of contents

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level; speaks on behalf of its Constituent Bodies on federal, national, and international issues; promotes and defends the rule of law; and promotes the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts, and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents its Constituent Bodies: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Law Society of the Australian Capital Territory
- New South Wales Bar Association
- Law Society of New South Wales
- Northern Territory Bar Association
- Law Society Northern Territory
- Bar Association of Queensland
- Queensland Law Society
- South Australian Bar Association
- Law Society of South Australia
- Tasmanian Bar
- Law Society of Tasmania
- The Victorian Bar Incorporated
- Law Institute of Victoria
- Western Australian Bar Association
- Law Society of Western Australia
- Law Firms Australia

Through this representation, the Law Council acts on behalf of more than 104,000 Australian lawyers.

The Law Council is governed by a Board of 23 Directors: one from each of the Constituent Bodies, and six elected Executive members. The Directors meet quarterly to set objectives, policy, and priorities for the Law Council. Between Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2024 are:

- Mr Greg McIntyre SC, President
- Ms Juliana Warner, President-elect
- Ms Tania Wolff, Treasurer
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member
- Mr Lachlan Molesworth, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.au.

Acknowledgements

The Law Council of Australia acknowledges the contributions of the following Constituent Bodies in the preparation of this submission:

- Law Institute of Victoria;
- Law Society of New South Wales;
- Law Society of South Australia; and
- The Victorian Bar.

The Law Council is also grateful for the assistance of the following of its committees:

- Business and Human Rights Committee;
- National Human Rights Committee; and
- the Business Law Section's Media and Communications Committee.

Introduction

1. The Law Council of Australia appreciates the opportunity to contribute to the Statutory **Review** of the *Online Safety Act 2021* (Cth). Commencing on 23 January 2022, the Act created a new regulatory framework to improve and promote the safety of Australians online, including the establishment of the eSafety **Commissioner**.

2. The Law Council notes that section 239A of the Act requires an independent Review of the Act to be commenced within three years of it coming into force, and that the Australian Government has asked that the Reviewer report by 31 October 2024.

3. The Law Council acknowledges the significant impacts of harmful online content and unacceptable online behaviour, and recognises the importance of the Act in strengthening protections to ensure users of online platforms are safeguarded from abusive, or harmful, content. Nonetheless, when considering any potential reforms, the Australian Government must adequately balance the need to protect individuals from online harm, while limiting any potential overregulation. Amendments to the Act should be proportionate, and should not curtail individuals' freedom of expression, nor serve as a placeholder for addressing broader societal issues, where harms are facilitated through social media or other online services.

4. The Law Council, therefore, is pleased that the Review is being conducted now to ensure that the Act is responsive to the evolving online environment. We welcome the Terms of Reference of the Review, considering the pace of recent technological change—including the emergence of generative artificial intelligence (**AI**)—and the fact that several like-minded jurisdictions overseas have recently implemented regulatory schemes to combat online harms.

5. The following comments are in response to the matters raised in the Issues Paper, dated April 2024, and seek, to the greatest possible extent, to present a unified view on behalf of the legal profession in Australia. However, in the time available to prepare this submission, the Law Council has not had sufficient opportunity to adopt a settled position in response to all 33 questions asked in the Issues Paper. As such, there are several matters where a range of views have been expressed and have been set out for the Reviewer's consideration.

General comments

Consistency of approach

6. Any proposed reforms to the Act must be consistent with other reviews and inquiries being undertaken by the Government. As outlined below, a range of significant initiatives and reviews that will impact the regulation of digital spaces are currently being undertaken, including with respect to privacy, data, and artificial intelligence. Other related reviews include the Department of Home Affairs' Multicultural Framework Review[1] and the current inquiry by the Joint Select Committee on Social Media and Australian Society.[2]

[1] Department of Home Affairs, *Multicultural Framework Review* (Web Page, March 2024) <https://www.homeaffairs.gov.au/about-us/our-portfolios/multicultural-framework-review/multicultural-framework-review>.
[2] Parliament of Australia, *Joint Select Committee on Social Media and Australian Society* (Web Page, May 2024) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Social_Media/SocialMedia>.

Privacy

7. As noted in the Issues Paper, significant reforms to the *Privacy Act 1988* (Cth) are currently being contemplated. In this context, the Law Council notes the Privacy Act Review Report, where, in September 2023, the Government agreed (or agreed in principle) to recommendations seeking to address the vulnerability of children to online harm.[3] Of note, many of the harms under the Act are likely to involve 'personal information' as defined in section 6 of the Privacy Act.

8. As stated in the Government Response to the Privacy Act Review Report:

> *The Privacy Act is one piece of legislation in a broader digital and data regulatory framework … In order to reduce complexity and compliance costs, the Privacy Act should provide a baseline set of protections that are interoperable with other frameworks that deal with the handling of personal information*.[4]

9. For the purposes of clarity and consistency of approach, it is critical that initiatives arising from the Privacy Act Review are considered in tandem with—and can reinforce—any reforms to the Act. For example, the development of a Children's Online Privacy Code (as agreed to by the Government in its response to the Privacy Act Review Report) necessarily intersects with changes to Australia's online safety regime, including the introduction of any duties placed on online services to design for safety, and monitor the content published on their platforms.[5]

10. We also draw the Reviewer's attention to the consideration currently being given to the development of a statutory tort for serious invasions of privacy. The Government agreed in principle to this proposal in its response to the Privacy Act Review Report, and noted:[6]

> *A statutory tort … would provide people with the ability to seek redress through the courts for serious invasions of privacy without being limited by the scope of the [Privacy] Act … While it is possible that an action in the statutory tort would have an overlap with existing legal remedies (such as state-based surveillance laws), these laws usually focus on punishment of the offender and not compensation to the victim*.[7]

11. Furthermore, in March 2024, the Attorney-General's Department publicly consulted on measures to address the practice of doxxing, including on whether a statutory tort for serious invasions of privacy would improve the available options for victims of doxxing.[8]

12. It is important that consideration of provisions under the Act—particularly relating to potential harms—is complementary to, and harmonised with, the measures under the Privacy Act, once reformed. The Law Council reiterates its calls for a roadmap for the harmonisation of Australia's privacy and data laws, to ensure the

---

[3] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF> 13-14.
[4] Ibid 16.
Ibid 16.
14, 30.
[6] Ibid 19, 36.
[7] Ibid 19.
[8] See Attorney-General's Department, *Public Consultation on Doxxing and Privacy Reforms* (Web Page, March 2024) <https://consultations.ag.gov.au/integrity/doxxing-and-privacy-reforms/> and Law Council of Australia, *Doxxing and privacy reforms* (Submission, 10 April 2024) <https://lawcouncil.au/resources/submissions/doxxing-and-privacy-reforms>.

development of a national privacy framework that is consistent, clear and accessible.[9]

Artificial Intelligence

13. Similarly, work that is currently being undertaken to address new challenges arising from generative AI for online safety should be addressed from a coordinated, cross-governmental perspective.

14. As noted in the Government's response to the 2023 Safe and Responsible AI consultation:

> *… existing laws likely do not adequately prevent AI-facilitated harms before they occur, and more work is needed to ensure there is an adequate response to harms after they occur*.[10]

These harms necessarily intersect with issues of online safety—including discussions about mandatory safety guardrails for generative AI in high-risk settings—and should be considered together. A further example of legislated responses not necessarily being undertaken in a coherent and coordinated manner is the recent introduction of the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024. It is critical that such reforms are considered in the context of the review of the Act.

15. The Law Council recently provided a submission to the inquiry by the Senate Select Committee on Adopting Artificial Intelligence on the opportunities and impacts arising out of the uptake of AI technologies in Australia.[11] The Law Council looks forward to engaging with that Committee's recommendations in due course, along with the outcomes of this Review.

International operation

16. The Law Council notes that the majority of online service providers, to which the Act applies, operate internationally. As such, consideration and comparison of online safety legislation in international jurisdictions—for example, the existence of a duty of care on platforms, and the potential extraterritorial application of online safety legislation[12]—will be important to ensure consistency in approach to the management of online risks and enforcement mechanisms.

The impacts of overregulation

17. The Law Council understands the importance of protecting the community from the dissemination of abhorrent content online. While we support strengthening

---

[9] Law Council of Australia, *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (Submission, 8 November 2022) <https://lawcouncil.au/resources/submissions/privacy-legislation-amendment-enforcement-and-other-measures-bill-2022> 8.
[10] Australian Government, *Safe and responsible AI in Australia consultation: Australian Government's interim response* (January 2024) <https://consult.industry.gov.au/supporting-responsible-ai> 5.
[11] Law Council of Australia, *Inquiry into the opportunities and impacts of the uptake of artificial intelligence technologies in Australia* (Submission, 20 May 2024) <https://lawcouncil.au/resources/submissions/inquiry-into-the-opportunities-and-impacts-of-the-uptake-of-artificial-intelligence-technologies-in-australia>.
[12] In a globalised environment, effective enforcement of the Act requires consideration of practicable provisions for the Act's extraterritorial application to protect Australians from defined classes of online harms. The Privacy Act was amended in 2022 to allow for enforcement of penalties on an overseas entity conducting business-related activities in Australia (*Privacy Act 1977* (Cth) ss 5A, 5B). In its response to the Privacy Act Review Report, the Government agreed that further consultation should be undertaken on the extraterritorial provisions of the Privacy Act to determine if an additional requirement that personal information is connected to Australia is necessary to narrow the current scope.

protections in the ways described in this submission, we caution against overregulation, to the extent that it may lead to undue restriction on freedom of expression.

18. On 13 May 2024, the Federal Court of Australia handed down its judgment in *eSafety Commissioner v X Corp* [2024] FCA 499. This case involved a removal notice, issued by the Commissioner to X Corp under section 109 of the Act, for 65 links that contained video footage of a knife attack (alleged Class 1 material) in Sydney in April 2024. While X Corp—an American corporation—did not remove the material, the material was 'geo-blocked', meaning that users in Australia could not access it from an Australian IP address.

19. Justice Geoffrey Kennett held that it would be reasonable for X Corp to remove the content, but unreasonable for the Commissioner to compel removal through section 109 of the Act. His Honour found that:

> *If given the reach contended for by the Commissioner, the removal notice would govern (and subject to punitive consequences under Australian law) the activities of a foreign corporation in the United States (where X Corp's corporate decision-making occurs) and every country where its servers are located; and it would likewise govern the relationships between that corporation and its users everywhere in the world. The Commissioner … would be deciding what users of social media services throughout the world were allowed to see on those services. The content to which access may be denied by a removal notice is not limited to Australian content.*
>
> *…*
>
> *The potential consequences for orderly and amicable relations between nations, if a notice with the breadth contended for were enforced, are obvious. Most likely, the notice would be ignored or disparaged in other countries.*
>
> *…*
>
> *The result is that … the "reasonable steps" required by a removal notice issued under s 109 do not include the steps which the Commissioner seeks to compel X Corp to take in the present case*.[13]

20. This judgment is likely to have significant implications for actions for the removal of content, as it demonstrates that:

- courts can—and will—reject attempts by one country to 'regulate' the global internet by compelling the removal of content; and
- governments should be cautious, in considering the powers of the Commissioner, as to the potential impact of overregulation on fundamental rights, such as freedom of expression and the right to privacy.

21. Nonetheless, the Law Council acknowledges there is growing concern surrounding social media entities profiting from the dissemination of abhorrent content. The global nature of Big Tech companies presents a challenge for regulation, as laws vary significantly between countries, and enforcement efforts can prove difficult.

[13] *eSafety Commissioner v X Corp* [2024] FCA 499 [50]–[53].

22. The Law Council is concerned that, in the absence of a global regulatory framework, social media technology giants may continue to distribute, and profit from, harmful online content, and minimise accountability for the associated effects. To address these concerns, international cooperation to agree on common standards will likely be required, such as through the negotiation and development of an international convention on the regulation of online materials.

Online safety and digital inclusion for First Nations peoples

23. The matters outlined below present an important contextual backdrop to any reform considerations for the Act, by demonstrating the heightened risks that the online environment can pose to First Nations peoples—especially First Nations children and women—in Australia.

24. According to research conducted by the Commissioner, First Nations peoples generally:

- experience online hate speech at more than double the national average (33 per cent versus 14 per cent);
- are twice as likely to experience image-based abuse; and
- experience family violence (including technology-facilitated gender-based violence) at much higher rates than other Australians.[14]

25. First Nations children face particularly acute risks. For example, the Commissioner has noted that First Nations children are more likely to have been exposed to a variety of potentially harmful experiences online, including hate speech.[15] As at March 2023, First Nations children have been found to be:

- more likely than the wider Australian population to be the target of hate speech and cyberbullying.[16] Notably, 29 per cent have had offensive things said to them because of their race, ethnicity, gender, nationality, sexual orientation, religion, age or disability, compared to the national average of 11 per cent;[17] and
- more likely to be 'treated in a hurtful or nasty way' online (68 per cent, compared to 45 per cent).[18]

26. These statistics are particularly notable, in a context where First Nations children have been found to be more likely than the national average to:

- make new friends or contacts online (37 per cent versus 20 per cent);

[14] eSafety Commissioner, *Annual report 2022-23* (2023) <https://www.esafety.gov.au/sites/default/files/2023-10/ACMA-and-eSafety-Commissioner-annual-report-2022-23.pdf?v=1718323077201> 189.
[15] eSafety Commissioner, *Cool, beautiful, strange and scary: The online experiences of Aboriginal and Torres Strait Islander children and their parents and caregivers* (Report, March 2023) <https://www.esafety.gov.au/sites/default/files/2023-03/Cool_beautiful_strange_and_scary_report.pdf?v=1718323290470> 7. See also House of Representatives Select Committee on Social Media an Online Safety, *Social Media and Online Safety* (Report, March 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report> [2.111].
[16] eSafety Commissioner, *Cool, beautiful, strange and scary: The online experiences of Aboriginal and Torres Strait Islander children and their parents and caregivers* (Report, March 2023) <https://www.esafety.gov.au/sites/default/files/2023-03/Cool_beautiful_strange_and_scary_report.pdf?v=1718323290470> 8.
[17] Ibid 10.
[18] Ibid.

- post their own video and music content online (37 per cent verses 19 per cent); and
- story or blog content (35 per cent versus 16 per cent).[19]

Further, 30 per cent of First Nations children discuss social and political problems online weekly or more often—more than double the national average of 13 per cent.[20]

27. While research indicates that First Nations children are proactive and knowledgeable in responding to negative experiences online,[21] the Law Council considers it is necessary to pursue reforms that would make the internet safer for First Nations children, given the extent and severity of the harm being experienced by them.

28. The fact that First Nations children are particularly exposed to risks online is also recognised in research, with respect to 'digital parenting' of parents and caregivers of First Nations children. They are especially aware of their child's encounters with online hate speech (84 per cent versus 64 per cent), and are more likely than the Australian average to instruct their child on ways to use the internet safety, to comply technical measures (such as blocking software), and to regularly monitor their child's online activities.[22]

29. The Law Council also notes recent research that finds that First Nations women in rural, regional and remote areas experience technology-facilitated abusive behaviours, most commonly from a current or former male partner, within the context of intimate partner violence.[23] The most commonly reported behaviours include threats, harassment, monitoring, and stalking,[24] and the most commonly reported vehicles for these behaviours are fake social media accounts and monitoring apps or platforms, among others.[25]

30. The authors of that research argued that, to minimise the impacts of technology-facilitated abusive behaviours:

> *… there needs to be culturally appropriate accessible services, good relationships between the community and services and police, and there needs to be clear and consistent legislation. Social media and technology companies must have some accountability and play a role in preventing online abuse.*[26]

31. The Law Council also notes that research conducted on First Nations women living in urban areas found that abuse by third parties via social media was a prevalent form of technology-facilitated abuse amongst such women.[27]

---

[19] Ibid 9.
[20] Ibid.
[21] Ibid 11.
[22] Ibid 12.
[23] See eSafety Commissioner, *'Can I just share my story?' Experiences of technology-facilitated abuse among Aboriginal and Torres Strait Islander women from regional and remote areas* (Report, August 2021) <https://www.esafety.gov.au/research/technology-facilitated-abuse-among-aboriginal-and-torres-strait-islander-women> 8.
[24] Ibid.
[25] Ibid.
[26] Ibid 9.
[27] See eSafety Commissioner, *Online safety for Aboriginal and Torres Strait Islander women living in urban areas* (Report, October 2019) <https://www.esafety.gov.au/research/online-safety-for-aboriginal-and-torres-strait-islander-women-living-urban-areas> 20-22.

32. The Law Council considers that the Commissioner should ideally be liaising with the First Nations Digital Inclusion Advisory Group[28] about the online safety risks and issues canvassed in the research, outlined above. This collaborative approach would assist to fulfil the priority commitment to shared decision-making under the National Agreement on Closing the Gap.[29]

33. More broadly, the Law Council welcomes the Government's commitment to narrow the digital gap for First Nations peoples. We acknowledge work currently underway to co-design free community Wi-Fi for remote First Nations communities, and to support the safe use of this infrastructure, including through content filtering.[30] This initiative exemplifies how online safety can be promoted for First Nations peoples through partnership with community.

34. The First Nations Digital Inclusion Advisory Group is currently consulting on the development of a roadmap to support digital inclusion for First Nations people in Australia.[31] We look forward to providing a submission to this consultation, and we will engage closely with any proposals or outcomes arising from this process.

Education and resourcing

35. The Law Council supports an approach that broadens the scope of online safety education to the community, including enhanced education about what tools and services are available to protect Australians, including children.

36. It is critical that the Government, and the Commissioner, support the provision of practical advice to parents, carers, educators, and the community at large about online safety and device management and ensure that digital literacy education is delivered to children and parents.

37. A consistent community approach to messaging about online safety is vital, as well as ensuring that educators are at the forefront of technological advancements, including generative AI. These measures will assist the community to better understand the risks, opportunities, and challenges associated with children engaging with online services and platforms.

38. Finally, if the regulatory purview, tools, and powers available to the Commissioner are increased, there must be a commensurate increase in resourcing for the Office of the eSafety Commissioner to undertake this additional work, and to implement other measures to drive systemic change.

[28] Commonwealth of Australia, *First Nations Digital Inclusion Advisory Group* (Web Page, 2023) <https://www.digitalinclusion.gov.au/>
[29] Commonwealth of Australia, *National Agreement on Closing the Gap* (July 2020) <https://www.closingthegap.gov.au/national-agreement>.
[30] See the Hon Michelle Rowland MP and the Hon Linda Burney MP, *Narrowing the digital Gap through community Wi-Fi* (Media Release, 21 June 2024) <https://minister.infrastructure.gov.au/rowland/media-release/narrowing-digital-gap-through-community-wi-fi>.
[31] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Have your say: A roadmap for First Nations digital inclusion* (Web Page, 2024) <https://www.infrastructure.gov.au/have-your-say/roadmap-first-nations-digital-inclusion>.

Discussion questions

Part 2: Australia's regulatory approach to online services, systems, and processes

Question 1: Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?

39. The objects of the Act, contained in section 3, are to improve and promote online safety for Australians.

40. While the Law Council generally considers the objects of the Act to be sufficient, consideration should be given to including an explicit reference to the aims of identifying, mitigating, and managing risks of harm. The Law Council refers to the 2022 Report of the House of Representatives Select Committee on Social Media and Online Safety, where that Committee argued:

> *The time has come to fundamentally shift the burden of responsibility regarding ensuring online safety. For too long, the onus of maintaining online safety has been on the most vulnerable users, including children and their parents. This is unacceptable and unsustainable in an environment where users like children are exposed to the most risk online and suffer extreme forms of harm as a result.*[32]

41. Expanding the objects of the Act to include harm prevention and mitigation would need to be accompanied by legislative and regulatory changes. This would mean that a systemic focus on mitigating harm is introduced, over and above the current 'content-focused' approaches, whereby certain material is subject to mandatory and enforceable removal notices.

Question 5: Should the Act have strengthened and enforceable Basic Online Safety Expectations?

42. The Act was introduced to 'hold industry more accountable for the safety of their products and services',[33] including by articulating 'a core set of basic online safety expectations to improve and promote online safety for Australians'.[34]

43. However, the Law Council has received feedback suggesting that too much responsibility is currently placed on users—including children—to ensure their own safety online. Accordingly, more must be done to shift responsibility for ensuring online safety on to the platforms that provide online services, to:

- increase transparency;
- assist to determine whether platforms are meeting the Basic Online Safety Expectations;

[32] House of Representatives Select Committee on Social Media an Online Safety, *Social Media and Online Safety* (Report, March 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report> [5.78].
[33] Explanatory Memorandum, Online Safety Bill 2021 (Cth), 25.
[34] Ibid 1.

- strengthen industry efforts to improve online safety; and
- assist in measuring the effectiveness of the current legislative framework that governs industry codes.

44. To give effect to the above objectives, the Reviewer could consider the following measures:

    (a) imposition of stronger penalties on online service providers that fail to comply with a notice or determination of the Commissioner in respect of the Basic Online Safety Expectations;

    (b) introduction of a mandatory standard for online service providers to detail their strategies for managing user-safety issues, including measures to address violent content, scams, pornography, and degrading deepfakes;[35] and

    (c) expanding the powers of the eSafety Commissioner to initiate investigations about complaints, or suspected breaches of codes or standards under the Online Content Scheme.

Part 3: Protecting those who have experienced or encountered online harms

Question 8: Are the thresholds that are set for each complaints scheme appropriate?

45. As outlined in the Issues Paper, the Commissioner has powers to investigate complaints made under the four complaints and content-based schemes under the Act:[36]

    - the child cyberbullying scheme;
    - the adult cyber-abuse scheme;
    - the non-consensual sharing of intimate images scheme; and
    - the Online Content Scheme.

46. The Issues Paper identifies that there were a high number of adult cyber-abuse complaints during the 2022–23 financial year that did not meet the threshold for adult cyber-abuse.[37] Those complaints were made with respect to the technologies that existed at the time, and it follows that the emergence of new technologies since that period may lead to an even greater number of adult cyber-abuse complaints that fail to meet the required threshold.

47. The Law Council considers that the threshold for complaints must be set at a level that will enable an appropriate degree of intervention by the Commissioner, including in response to additional complaints that are anticipated, based on new and emerging technologies that may contribute to the proliferation of cyber-abuse.

[35] The Law Council notes that the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 (Cth) was introduced on 5 June 2024.
[36] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 19.
[37] Ibid 21.

Question 10: Does more need to be done to make sure vulnerable Australians at the highest risk of abuse have access to corrective action through the Act?

48. Despite the existence of the adult cyber-abuse scheme, the Act itself does not provide for corrective action in respect of online material that amounts to hateful content targeting a particular individual or group, on account of a specific shared characteristic (e.g., religion, ethnic background, culture, disability, age, or gender identity) or those with intersectional characteristics (e.g., gender and race).

49. Under section 7 of the Act, material is 'cyber-abuse material targeted at an Australian adult' if, amongst other things:

- an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult;[38] and

- an ordinary reasonable person, in the position of the Australian adult, would regard the material as being, in all the circumstances, menacing, harassing or offensive.[39]

50. While the Law Council agrees that more needs to be done to make sure that Australians have access to corrective action through the Act, it does not have a settled position on how this could be most effectively achieved. Potential options, as suggested by the Law Institute of Victoria (**LIV**), include:

- amending the Act so that:

  - section 7 has regard to whether such content is likely to incite hatred or violence against such individuals or groups, on account of their specific shared characteristic; and

  - section 8 has regard to distinguishing factors that are relevant to a diverse society, when determining whether material is offensive;

- adopting the approach in the United Kingdom (**UK**), where the *Online Safety Act 2023* (**UK Act**) requires service providers to ensure that adult users have the ability to increase their control over online content viewable by them if it is abusive and targets any of the following characteristics: race, religion, sex, sexual orientation, disability, or gender reassignment.[40] This provides control to service users, allowing them to limit the availability of such content when using online services; and

[38] *Online Safety Act 2021* (Cth) s 7(1)(b).
[39] Ibid s 7(1)(c).
[40] *Online Safety Act 2023* (UK) ss 15, 16(4).

- incorporating a reference within the Act to Australia's federal anti-discrimination law. For example, the Act could specify that online material that meets the first criterion of section 18C of the *Racial Discrimination Act 1975* (Cth) ('reasonably likely, in all the circumstances, to offend, insult, humiliate or intimidate another person or group of people)[41] also constitutes offensive and hateful online material.

    - This change would place additional obligations on service providers, and relevant governmental bodies, to regulate access to such content, and reflects the approach taken in Ireland's *Online Safety and Media Regulation Act 2022* (**Irish Act**). The Irish Act specifies that, where the release of content would constitute an offence under certain statutes (listed in Schedule 3), this content constitutes 'harmful online content'.[42]

51. The Law Council emphasises, however, that any such measures must be carefully considered in light of the need to protect the right to freedom of expression, as enshrined in Article 19 of the International Covenant on Civil and Political Rights (**ICCPR**). However, under Article 19(3), freedom of expression may be limited as provided for by law and when necessary to protect the rights or reputations of others, national security, public order, or public health or morals.

Question 12: What role should the Act play in helping to restrict children's access to age-inappropriate content (including through the application of age assurance)?

52. The Law Council supports a framework that aims to address, and reduce, children's access to harmful content.

53. Currently, age-assurance protections within the Act are achieved through the Online Content Scheme, the Restricted Access System, and the Basic Online Safety Expectations.[43] Further, the Commissioner, where appropriate, is to have regard to the Convention on the Rights of the Child in performing functions conferred by, or under, the Act, and in relation to children residing in Australia.[44]

54. Despite these existing measures, the issue of children encountering different types of age-inappropriate content, having regard to their capabilities, development, rights and interests, remains a significant concern in Australia.[45] For instance, exposure to such content—especially pornography—can be seen to shape attitudes and behaviours contributing to gender-based violence,[46] while a child having access to racially offensive material can be especially harmful if they are from a racially marginalised background.

[41] *Racial Discrimination Act 1975* (Cth) s 18C(1)(a).
[42] *Online Safety and Media Regulation Act 2022* (Ireland) s 139A.
[43] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 13.
[44] *Online Safety Act 2021* (Cth) s 24.
[45] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 23.
[46] eSafety Commissioner, *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography* (Report, March 2023) <https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf?v=1718318408994>.

Australia's Age-Assurance Pilot

55. In May 2024, the Government announced that it will provide resourcing to conduct a pilot of age-assurance technology to protect children from harmful content, such as pornography and other age-restricted online services.[47] The pilot will identify available age-assurance products to protect children from online harm, and test their efficacy, including in relation to privacy and security.[48]

56. While this initiative represents a proactive step towards enhancing online safety for minors through the use of age-verification mechanisms, the Law Council urges the Government to consider the practicality of such a measure, and to consider additional options in this regard. Any next steps should be informed by the Commissioner's *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*, published in March 2023.[49]

57. The Law Council is concerned that children faced with age-assurance restrictions could circumvent these controls by, for instance, entering a false date of birth, creating new accounts online, or changing virtual private network (**VPN**) or Wi-Fi settings to avoid such controls.[50] As such, for the age-assurance pilot to achieve its intended effect:

    - it must be implemented carefully, with the potential for circumvention in mind;
    - it must operate to prevent access to content, wherever that content is hosted; and
    - the Government must carefully balance the need for online safety with a need for privacy and security.

58. Fundamentally, a coordinated effort is required between the Government and service providers to tackle online harm against children. While age-assurance technologies may provide additional safeguards for children who seek to access age-inappropriate content, service providers must continue to remain accountable for the safety of their Australian users.

[47] The Hon Anthony Albanese MP, Senator the Hon Katy Gallagher, The Hon Amanda Rishworth MP, The Hon Mark Dreyfus KC MP and the Hon Michelle Rowland MP, *Tackling online harms* (Media Release, 1 May 2024) <https://www.pm.gov.au/media/tackling-online-harms>.
[48] Ibid.
[49] eSafety Commissioner, *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography* (Report, March 2023) <https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf?v=1718318408994>.
[50] See, e.g., Revealing Reality, *Families' attitudes towards age assurance* (Report, October 2022) <https://revealingreality.co.uk/wp-content/uploads/2022/10/DRCF-Ofcom-ICO-Families-attitudes-towards-age-assurance-.pdf>.

Part 4: Penalties and investigation and information gathering powers

Question 17: Does the Act need stronger investigation, information gathering and enforcement powers?

59. Compliance with the Act is critical. Yet, investigations and enforcement are problematic, given the technology involved and the geographical location of those who engage in harmful conduct online.

60. Broad powers of investigation are necessary, including powers to gather relevant information. At present, as the Issues Paper notes:

> *Investigation powers include powers to summon a person to attend before the Commissioner to answer questions, to provide information or documents to the Commissioner, and to examine a person under oath or affirmation*.[51]

These are important and valuable tools that are available.

61. The imposition of higher maximum penalties may be useful to demonstrate that Australia takes a 'tough' approach to social media companies that infringe laws. This issue is discussed in response to Question 18 below. Regardless, the Law Council understands that, in practice, increased penalties are unlikely to result in significantly greater compliance. A more effective approach is likely to be one that assists in the recoupment of penalties imposed.

62. As outlined in the Issues Paper, the current maximum (civil) penalty for a company that is found to be in contravention of the Act is $782,500.[52] However, where the infringement is an ongoing one, this is a maximum penalty that potentially applies for each day that the contravention is occurring, which may lead to higher penalties.[53] The majority of offences under the Act would involve this daily infringement. For example, a failure to provide reporting notices or determinations about Basic Online Safety Expectations,[54] or failures to comply with removal notices,[55] a blocking notice,[56] a remedial notice,[57] a link deletion notice,[58] an app removal notice,[59] or a notice to comply with an industry standard[60] are likely to result in daily infringements.

63. The Law Council understands that there are infringements that, in certain circumstances, do not attract a daily maximum fine. These include a failure to comply with an industry standard,[61] and posting intimate images of a person without their consent,[62] even though in such a case, the failure to comply with a removal notice would attract a daily maximum fine.[63]

---

[51] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 36.
[52] Ibid 33.
[53] Ibid.
[54] *Online Safety Act 2021* (Cth) ss 49, 50, 53, 56.
[55] Ibid ss 66, 79, 91, 111, 116.
[56] Ibid s 103.
[57] Ibid s 121.
[58] Ibid s 125.
[59] Ibid s 129.
[60] Ibid s 143.
[61] Ibid s 146.
[62] Ibid s 75.
[63] Ibid s 79.

64. Where the maximum fine is a daily one, the ultimate maximum penalty can quickly escalate into millions of dollars. It is unlikely, in that circumstance, that any failure or refusal to comply with a direction or notice is because the online service has taken the calculated view that the fine is simply a cost of doing business. Instead, if there is a failure to comply, it is much more likely that this is a result of a belief that it is difficult—if not impossible—to enforce such a penalty. Any reforms to the Act, with respect to enforcement, should have close regard to this reality.

Question 18: Are Australia's penalties adequate and if not, what forms should they take?

Civil penalties and infringement notices

65. The Law Council is aware of—and shares—concerns as to the adequacy of the maximum civil penalties available, particularly in light of:

- the size, resources, and power of some online platforms; and
- the maximum penalties that can be imposed by international online regulators and other Australian regulators for contraventions under the Privacy Act and Australian Consumer Law.[64]

66. As canvassed in the response to Question 17 above, the introduction of greater penalties could be a useful measure to demonstrate to social media companies that Australia has a tough stance on behaviour that violates the Act. Nonetheless, in practice, a more effective approach is likely to be one that assists in the recoupment of penalties awarded.

67. Notwithstanding this, as a first step, it would be an improvement if the Act mirrored the maximum level of civil penalties imposed by the Privacy Act, Australian Consumer Law, and the UK Act. Under the UK Act, the maximum amount of the penalty for which an entity is liable is whichever is the greater of £18 million (approximately $35 million AUD), or 10 per cent of the entity's qualifying worldwide revenue. Further, the concept of penalties that are determined by way of calculation of global turnover is not unfamiliar to Australian legislation.[65]

68. The Law Council also considers that there is merit in ensuring that civil penalties under the Act can be imposed in a nuanced and proportionate way to respond to the harm posed, although the regulator should retain a considerable amount of discretion to make the appropriate assessment. To achieve this, a non-exhaustive list of criteria could be developed for the regulator to take into account when assessing what level of sanction is appropriate, such as the seriousness of the breach, and whether, in addition to being objectively harmful, the material is illegal in itself (i.e., child exploitation material, or material that promotes terrorist ideology).

69. This proposed approach would assist to address concerns that the introduction of substantial penalties—both civil and criminal—could create an incentive for platforms to 'err on the side of over-moderating the online environment'.[66] This

[64] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 21.
[65] See, e.g., amendments introduced in 2022 to the *Competition and Consumer Act 2010* (Cth) where the maximum penalty for companies was raised to $50 million; three times the value of the benefit obtained; or 30 per cent of the company's adjusted turnover during the breach turnover period for the offence.
[66] Centre for Strategic and International Studies, *A New Chapter in Content Moderation: Unpacking the UK Online Safety Bill* (Web Page, 18 October 2023) <https://www.csis.org/analysis/new-chapter-content-moderation-unpacking-uk-online-safety-bill>.

potential impact on the freedom of expression may be exacerbated by the fact that automated systems that are used to detect harm may not have the required level of sophistication to distinguish illegal or otherwise harmful material from that which may be described as, for instance, political satire or dissent.

Suspension of services

70. Part 9, Division 9 of the Act currently vests power in the Commissioner to apply to the Federal Court for an order that a person cease providing a social media service,[67] a relevant electronic service,[68] a designated internet service,[69] or an internet carriage service,[70] if the Court if satisfied that:

    - there were two or more occasions during the previous 12 months where the person contravened a civil penalty provision regarding Class 1 or Class 2 material; and

    - as a result of those contraventions, the continued operation of that service represents a significant community safety risk.

71. In contrast, Article 51 of the European Union's (**EU**) *Digital Services Act 2022* provides that the relevant regulatory bodies in EU Member States can request the temporary suspension of a service, or online interface for an intermediary service, if such service is in breach.[71] However, as outlined in the Issues Paper, temporary suspension is seen as a last resort, applying only if the infringement persists, causes serious harm to users, and entails criminal offences involving threat to persons' life or safety.[72]

72. While the Law Council supports the removal of abhorrent and violent material from online platforms, it is imperative that penalties are proportionate. As a penalty, therefore, the suspension of services should be used in limited circumstances only, given the implications of suspension on the fundamental right to freedom of expression.

73. More broadly, any penalty must be clearly necessary and proportionate to the aim sought to be achieved.

[67] *Online Safety Act 2021* (Cth) s 156.
[68] Ibid s 157.
[69] Ibid s 158.
[70] Ibid s 159.
[71] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC*, Article 51.
[72] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 34.

Questions 19 and 20:

- **What more could be done to enforce action against service providers who do not comply, especially those based overseas?**
- **Should the Commissioner have powers to impose sanctions such as business disruption sanctions?**

74. While section 23 of the Act formally extends its application to 'acts, omissions, matters and things outside Australia',[73] the Law Council is aware that the regulation of, and enforcement against, international service providers poses a challenge in some circumstances.

75. Where the social media provider has assets in the jurisdiction, then the Law Council considers that enforcement should not be difficult. Civil penalties are enforceable under section 83 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) (**Regulatory Powers Act**) as debts due to the Commonwealth. The process in the Federal Court requires the filing of a 'Request for Enforcement' and, when granted, the applicant (in this instance, the Commonwealth) would then utilise the enforcement procedures of the Supreme Court of the jurisdiction where the order was made. Ultimately, the standard array of enforcement mechanisms (e.g., garnishee orders / order for attachment of debts, a warrant of seizure and sale, or a warrant of possession) would be available. If the company is located overseas, then a statutory demand will not be effective.

76. If the social media company does not have assets in the jurisdiction, but receives advertising revenue from Australian companies, then it would be possible to garnish those revenues. Ordinarily, it should not be difficult to determine which Australian companies are advertising, because their advertisements will be visible to those seeking to enforce the penalty.

77. International developments may also provide examples of potential solutions in circumstances where the social media company does not have assets in the jurisdiction, but receives advertising revenue from Australian companies. For example, the UK has established new powers that could be used to stop UK companies working with a platform, to prevent it from generating money.[74] In considering what additional measures might be available to enforce action against overseas service providers, the Law Council encourages the Reviewer's consideration of mechanisms, such as those adopted in the UK, to disrupt the ability of online service providers to generate revenue in Australia. Such mechanisms may be appropriate in circumstances where there is severe non-compliance with regulatory standards by overseas platforms.

78. However, it may be that the particular company within a corporate group that owes money to the social media company is not apparent, and that the social media company to which the advertising revenue is owed is not the same entity against which the civil penalty order is made. It is not always possible to undertake an examination of a third party (as distinct from the judgment debtor) for the purposes of enforcement.[75]

79. The Law Council, therefore, suggests that the focus should be directed towards simplifying the process of enforcement and determining which entities are indebted

[73] *Online Safety Act 2021* (Cth) s 23(2).
[74] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 33.
[75] See, e.g., *Supreme Court Rules* (Vic) r 67.02.

to the social media company. For instance, a provision could be inserted in the Regulatory Powers Act, requiring companies to answer questions of the Commonwealth relating to debts owed by judgment creditors. It may also be necessary to permit penalties to be recouped from related companies, where it is only the related company that is doing business in Australia.

80. The Law Council understands that if a company does not have assets or income in Australia, then enforcement is almost impossible. Few overseas jurisdictions permit enforcements of fines from overseas jurisdictions. Australia does not permit the enforcement—in Australia—of fines or penalties from overseas jurisdictions.[76]

81. The only steps that can be taken against entities that have no assets in Australia, and derive no income from Australian sources, is to prohibit them publishing their material in Australia (which, given the use of VPNs, would likely need to be directed to internet service providers). However, if such an entity derives no income from Australia, it may be doubted whether such a penalty is likely to encourage them to comply. Further, such a step may punish the Australian users of the service more than it would punish the service itself. The Law Council considers that, while this is a frustration, it is simply a limitation of country-specific legal systems when dealing with international communications systems.

Part 5: International approaches to address online harms

Question 22: Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?

82. While 'online services' is a term used frequently throughout the Issues Paper, it is not defined in the Act. The Law Council expects that the intention of the Issues Paper is to include under this umbrella term those 'online services' that are subject to the Basic Online Safety Expectations pursuant to section 45 of the Act,[77] and/or those 'online services' that are subject to the Online Content Scheme, administered by the Commission under Part 9 of the Act.[78]

83. The Basic Online Safety Expectations require the online platform to take reasonable steps to ensure that end-users can use the service in a safe manner.[79] However, as noted in the Issues Paper, this does not create a legally enforceable duty.[80]

84. The Law Council observes that the emergence of new technologies, particularly AI, creates greater capability for technology companies to anticipate, detect and eliminate online harms, including before they occur. This additional capability arguably makes it more reasonable for governments to impose statutory duties on online services to prevent harm, whether as part of a general statutory duty of care, or duties directed specifically to safety by design (as contemplated by Question 29).

[76] See the definition of 'enforceable money judgment' in the *Foreign Judgments Act 1991* (Cth).
[77] I.e., social media services, relevant electronic services, and designated internet services, as defined in the Act.
[78] I.e., social media services, relevant electronic services, designated internet services, internet search engine services, App distribution services, hosting services, internet carriage services, etc.
[79] *Online Safety Act* 2021 s 46(1)(a). Changes to the Basic Online Safety Expectations commenced on 31 May 2024 through the *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* (Cth).
[80] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 40.

85. In addition, the use of new technology in the design of online systems should mean that:

- the steps required to prevent harm are now less onerous than they have been previously; and
- there is less likelihood that design steps implemented for online safety will unintentionally restrict communications that are not potentially harmful and/or unreasonably interfere with freedom of expression.

86. In the time available, the Law Council has had insufficient opportunity to adopt a settled position as to whether a new statutory duty of care should be introduced for online platforms. Nonetheless, the feedback received on this matter is set out below for the Reviewer's consideration.

87. The Law Society of New South Wales (**LS NSW**), Law Society of South Australia (**LS SA**) and the Victorian Bar support the adoption of a statutory duty of care, and consider that such an approach has significant merit. As the House of Representatives Select Committee on Social Media and Online Safety noted in its Report, this model 'flips the onus of responsibility to provide and ensure user safety back onto social media platforms'.[81] These three bodies consider that any such duty should not be limited merely to social media platforms—it should be flexible enough to ensure the duty is owed by online services, as entities controlling the regulated environment.

Limitations of the current approach

88. The LS NSW considers that the current legislative approach is too heavily weighted towards a reactive 'notice and take down approach' that is unsuited to the digital environment. Nonetheless, the introduction of a duty of care should supplement—not replace—the existing complaints mechanism under the Act.

89. The LS NSW agrees with a paper released in April 2024 by Reset Australia that describes the focus on discrete pieces of content as a regulatory 'whack-a-mole' approach that fails to address systemic risk.[82] The paper outlines the five key elements of a 'comprehensive and enforceable regulatory framework', namely:[83]

(a) introduction of an overarching duty of care on the platform;

(b) requirements for platforms to assess all their systems and elements for serious risks they may pose;

(c) requirements for risk mitigation measures;

(d) an effective framework for public transparency; and

(e) strong enforcement powers.

[81] House of Representatives Select Committee on Social Media an Online Safety, *Social Media and Online Safety* (Report, March 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report> [5.82].
[82] Reset Australia, *A duty of care in Australia's Online Safety Act* (Policy Briefing, April 2024) <https://au.reset.tech/uploads/Duty-of-Care-Report-Reset.Tech.pdf> 5.
[83] Ibid 6.

Preferred model

90. The Victorian Bar considers, consistent with the principles of self-determination, that this statutory duty should adopt a direct-action model—those affected should have standing to pursue breaches of the duty of care directly. They should not be asked to rely on a regulator (i.e., the Commissioner, an ombudsman, or some other entity) to pursue possible breaches of the statutory duty.

91. The LS NSW considers that the introduction of an overarching duty is preferable to the introduction of multiple duties, as has occurred under the UK Act. The UK Act imposes multiple duties of care on providers of regulated user-to-user and search services, depending on the type of content involved—for example, illegal content, and content that is likely to be accessed by children.

92. While there are advantages in the nuance of the UK regime, in that it enables specific duties to match particular harms, the LS NSW agrees with the arguments of Reset Australia that this approach introduces significant regulatory complexity.[84]

93. Further, the LS NSW considers that a truly systemic approach starts from the system level, with proactive risk identification at the time of building the system (i.e., safety by design), rather than an assessment of risk that is focused on the content after the system has been set up.[85]

International standards on business and human rights

94. The Victorian Bar commends the development of an enforceable duty of care on businesses operating online platforms as being consistent with international standards on business and human rights. As the Issues Paper notes:

> *A statutory duty of care includes an overarching obligation to exercise care in relation to user harm (including through risk assessments and implementing migration measures) … [and] to continually assess the effectiveness of those measures*.[86]

95. The duty of care being considered is, in effect, a form of mandatory due diligence, whereby a business is required to assess the adverse impacts it may cause, contribute to, or be directly linked to, and to remedy those adverse impacts. In the Victorian Bar's view, this proposal is aligned with the United Nations **Guiding Principles** on Business and Human Rights, which were unanimously endorsed by the United Nations Human Rights Council, and which Australia has agreed to implement.[87] Such an approach would also be consistent with Australia's adherence to the Organisation for Economic Co-operation and Development (**OECD**) **Guidelines** for Multinational Enterprises on Responsible Business Conduct.[88]

96. The Guiding Principles recognise the duty of States to protect human rights from harm by business operations, including by legislative means. Both the Guiding Principles and the OECD Guidelines reflect the importance of businesses undertaking human rights due diligence—that is, assessing and preventing (or mitigating) risks that the business may pose to human rights, including the rights to

---

[84] Ibid 8.
[85] See *Online Safety Act 2021* (Cth) s 79.
[86] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 38.
[87] United Nations, *Guiding Principles on Business and Human Rights* (2011) <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf>.
[88] OECD, *Guidelines for Multinational Enterprises on Responsible Business Conduct* (2023) <https://doi.org/10.1787/81f92357-en>.

equality, freedom from discrimination, and freedom from expression. In addition, businesses should provide for (or participate in) a remedy, where their conduct causes or contributes to human rights harms.

97. The Victorian Bar, therefore, supports the adoption of a statutory duty of care that would require businesses to undertake human rights due diligence by:

- assessing the risk of online harms;
- preventing and minimising the realisation of the risks assessed; and
- participating in the provision of remedies for harms to human rights that arise.

Question 23: Is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?

98. The Law Council suggests that additional transparency obligations should be imposed on industry, especially regarding decision-making processes, and policies relating to the monitoring or removal of certain content. Transparency would be especially desirable in terms of how providers can track individuals and their browsing habits, as well as when this data might be provided to third parties.

99. Many companies now rely on AI to conduct content moderation on their platforms, often resulting in a large amount of content being removed without human oversight. It is understandable that online service providers would rely on automated content moderation, given the sheer volume of content made available daily, and the increasing obligations imposed on companies to monitor such content.

100. However, as the Law Council has previously noted, machine learning is subject to bias and assumptions,[89] and these can be subsequently reflected in automated decisions to remove online content. Recent media reports have highlighted the occurrence of large social media platforms censoring legitimate activists on social media, likely due to inadequately developed automated content moderation, and a lack of human oversight in the moderation process.[90]

101. When developing automated content moderation tools, internal policies to define harmful material, and internal decision-making processes related to content moderation, companies should be required to provide transparency, ensuring that an explanation for the restriction of material can always be provided. The Law Council notes that the *Digital Services Act 2022* (EU) includes such a requirement, which places a legal obligation on online platforms to provide clear and specific statements of reasons for their content moderation decisions.[91]

---

[89] See Law Council of Australia, *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper* (Submission, 3 June 2022) <https://lawcouncil.au/resources/submissions/positioning-australia-as-a-leader-in-digital-economy-regulation---automated-decision-making-and-ai-regulation-> and Law Council of Australia, *Inquiry into the opportunities and impacts of the uptake of artificial intelligence technologies in Australia* (Submission, 20 May 2024). <https://lawcouncil.au/resources/submissions/inquiry-into-the-opportunities-and-impacts-of-the-uptake-of-artificial-intelligence-technologies-in-australia> 30.

[90] Merlyna Lim and Ghadah Alrasheed, *Beyond a technical bug: Biased algorithms and moderation are censoring activists on social media* (online, 16 May 2021) <https://theconversation.com/beyond-a-technical-bug-biased-algorithms-and-moderation-are-censoring-activists-on-social-media-160669>.

[91] European Commission, *The impact of the Digital Services Act on digital platforms* (Web Page, April 2024) <https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms>.

102. The Law Council submits that it may be appropriate, in certain cases, for decisions as to the removal, or censorship, of content should be made (or at least, reviewed) by a human. Human oversight may be particularly useful when such content does not directly relate to violent or extreme material, and may well be within the bounds of lawful expression.

Question 25: To what extent do industry's current dispute resolution processes support Australians to have a safe online experience? Is an alternative dispute resolution mechanism such as an Ombuds scheme required? If so, how should the roles of the Ombuds and Commissioner interact?

103. As identified in the Issues Paper, the fifth interim report of the Australian Competition and Consumer Commission (**ACCC**) Digital Platform Services Inquiry 2020–25 recommended in 2022 that Australia establish internal dispute resolution obligations and an independent external dispute resolution scheme in the form of an ombudsman scheme.[92]

104. In its submission to inform the ACCC's Digital Platform Services Inquiry Preliminary Report, the Law Council:

- recommended against the establishment of a platforms-specific ombudsman;
- suggested that existing regulatory bodies should be given the appropriate powers and resources to deal with complaints, rather than creating a new ombudsman; and
- submitted that, if the ACCC proceeds to recommend a digital platforms ombudsman, potential areas of overlap between regulatory authorities should be reviewed to avoid duplication, minimise confusion, enable streamlining of resources and provide clarity of the complaint avenues, processes and expected outcomes for consumers.[93]

105. In its submission to inform the ACCC's fifth interim report, the Law Council supported steps to improve the quality and timeliness of the dispute resolution processes, subject to fundamental legal principles of fairness and proper procedure being followed.[94]

106. While the Law Council has not had an opportunity to revisit its position on these matters, the Victorian Bar supports the ACCC's recommendation to require online providers to have internal dispute resolution mechanisms, and to establish an external ombudsman scheme.

[92] ACCC, *Digital platform services inquiry: Interim report No. 5* (September 2022) <https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20September%202022%20interim%20report.pdf> [4.3]-[4.3.1].
[93] Law Council of Australia, *Digital Platforms Inquiry: Preliminary Report* (Submission, 15 February 2019) <https://lawcouncil.au/publicassets/d952f581-944e-e911-93fc-005056be13b5/3581%20-%20ACCC%20Digital%20Platforms%20Inquiry%20Preliminary%20Report%20Submission.pdf> 18-19.
[94] Law Council of Australia, *Digital Platform Services Inquiry: Discussion Paper for Interim report No. 5* (Submission, 2 May 2022) <https://lawcouncil.au/resources/submissions/discussion-paper-for-interim-report-no--5--updating-competition-and-consumer-law-for-digital-platform-services> 16.

107. According to the Victorian Bar, such an approach would be consistent with international law on business and human rights, noting that:

- the Guiding Principles recognise that:
  - the State is responsible for providing external judicial and non-judicial complaints mechanisms as part of its duty to protect against business-related human rights abuse. Within this context, the development of an ombudsman scheme would be a welcome development; and
  - while State-based judicial and non-judicial grievance mechanisms should form the foundation of a wider system of remedy, operational-level grievance mechanisms can provide early-stage recourse and resolution.
- the Guiding Principles and OECD Guidelines urge companies to have in place effective grievance mechanisms that ought to meet certain identified criteria of effectiveness. Specifically, these mechanisms should be legitimate, accessible, predictable, equitable, transparent, rights-compatible, dialogue-based and a source of learning.

108. The Victorian Bar supports a regulator—be it the Commissioner, or some alternative entity, such as an ombudsman—also having the power to pursue breaches of the statutory duty of care, on behalf of persons affected by purported breaches of the duty. This framework would ensure that persons adversely affected by online harm have the option to either bring the claim themselves, or to bring the harm to the attention of a regulator, for that regulator to then act accordingly.

Question 26: Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?

109. The Issues Paper highlights the importance of applying a human rights lens to the Review and to any subsequent reform to Australia's online safety regime. These observations include that the groups of Australians who are most likely to experience online harm—or the effects of dangerous online behaviour—include children, women, individuals from culturally or linguistically diverse backgrounds, First Nations peoples, people with particular religious beliefs, people who identify as LGBTQIA+, and older Australians.[95]

110. Accordingly, often the groups of Australians who are most vulnerable to online harm are people with attributes that are given a particular focus in treaties, or other instruments, that provide the foundational legal framework for international human rights, and that find some reflection in domestic anti-discrimination laws.[96]

111. More essentially, the disproportionate harms experienced by First Nations peoples, and other minority groups of the Australian population, undermine attainment of the concepts of human dignity, the right to equality and other fundamental freedoms. Australia aspires to these rights, as a proponent of the United Nations Declaration of

[95] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 10.
[96] Including *Convention on the Elimination of All Forms of Discrimination against Women* (18 December 1979) 1249 U.N.T.S. 13; 19 I.LM. 33 (1980); *Convention on the Rights of Persons with Disabilities* (3 May 2008) A/RES/61/106, Annex I; *Convention on the Rights of the Child* (20 November 1989) 1577 U.N.T.S. 3; 28 I.L.M. 1456 (1989); *International Convention on the Elimination of All Forms of Racial Discrimination* (21 December 1965) S. Exec. Doc. C, 95-2 (1978) S. Treaty Doc. 95-18; 660 U.N.T.S. 195, 212; *United Nations Declaration on the Rights of Indigenous Peoples* (13 September 2007) G.A. Res. 61/295, U.N. Doc. A/RES/61/295 46 I.L.M. 1013 (2007).

Human Rights (**UDHR**) and as a State Party to the ICCPR, the International Covenant on Economic, Social and Cultural Rights (**ICESCR**),[97] and several other principal United Nations human rights treaties.[98]

112. Article 12 of the UDHR and Article 17 of the ICCPR provide that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. In this context, the current limitations of the framework for online safety require assessment and reform. For example:

- the current framework is such that the Commissioner may not be able to intervene in situations where a person may be affected by abusive posts targeted at a group of people, such as dehumanising commentary on a particular race or belief;[99] and

- the structure of the current regulatory framework rests significantly on voluntary industry codes and standards of conduct. These are likely to be sufficient to address vexed issues such as online hate speech, which the Issues Paper identifies as requiring particular attention.[100]

Freedom of expression

113. Applying a human rights lens to the Review requires recognition of the right to freedom of expression, protected by Article 19 of the UDHR and ICCPR. Freedom of expression is associated with other human rights, such as the right to freedom of thought, conscience and religion, and the right to freedom of association—it is the cornerstone of a free and democratic society.

114. Consideration could be given to introducing a new provision in the Act which requires the Commissioner to have regard to the right to freedom of expression in the performance of their functions. Protection of this right is paramount in ensuring that tensions are resolved between the right of people to impart and receive information, and the right of people to be protected from the harms of hateful and inciteful conduct.

115. As noted, the right to freedom of expression is not an absolute right under international human rights law. The exercise of the right carries special duties and responsibilities with it, and Article 19(3) of the ICCPR imposes a duty on Member States to apply a three-part test when considering restrictions. This test requires that:

(a) the restriction is provided by law;

(b) the restriction has been imposed to protect a specific legitimate aim—namely, to respect the rights or reputations of others, to protect national security or public order, or to protect public health and morals; and

---

[97] *Universal Declaration of Human Rights* (8 December 1948) G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948); *International Covenant on Civil and Political Rights* (16 December 1966) 999 U.N.T.S. 171; [1980] ATS 23; *International Covenant on Economic, Social and Cultural Rights* (16 December 1966) 993 U.N.T.S. 3; [1976] ATS 5).
[98] *Convention on the Rights of the Child* (20 November 1989) 1577 U.N.T.S. 3; *Convention on the Elimination of All Forms of Discrimination Against Women* (18 December 1979) 1249 U.N.T.S. 13; *International Convention on the Elimination of All Forms of Racial Discrimination* (21 December 1965) 660 U.N.T.S. 193; *Convention on the Rights of Persons with Disabilities* (13 December 2006) A/RES/61/106, Annex I.
[99] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) 21.
[100] Ibid 46-47.

(c) the restriction is proportionate to the legitimate aim, and is the least intrusive measure available to achieve the desired result.[101]

Therefore, any limitation in the Act on the right to freedom of expression—as with the limitation on any fundamental right—would require clear legislative intent.

116. In addition, the Law Council is of the view that online service providers should be required to act in a non-arbitrary and non-discriminatory manner—and consider the individual rights of service users—when determining policies and procedures for the monitoring of online content. This could assist to reduce the likelihood of legitimate expressions being censored, while ensuring that tensions arising with respect to the right to privacy, and the right to be protected from harmful discrimination, are resolved.

117. While there is no Commonwealth legislation enshrining a general right to freedom of expression, several States and Territories have recognised this right, as part of broader human rights acts. Human rights legislation in the Australian Capital Territory, Queensland, and Victoria provides that everyone has the right to freedom of expression. This right includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of borders, whether orally, in writing or in print, by way of art, or in another medium chosen by that person.[102]

Federal human rights legislative framework

118. In order to ensure that the Act upholds fundamental human rights and supporting principles, the legislation would also benefit from reference to a federal human rights legislative framework, as occurs in other jurisdictions. As noted in the Issues Paper, guidance is available from approaches taken in the UK, Canada, Ireland, and the European Union.[103] However, each of these jurisdictions also has national human rights legislation and/or regional human rights instruments, to which relevant online safety legislation can refer.

119. The Law Council is in favour of a Federal Human Rights Charter,[104] and recently reiterated this position in response to the Inquiry into Australia's Human Rights Framework, undertaken by the Parliamentary Joint Committee on Human Rights (**PJCHR**). In May 2024, the Law Council strongly welcomed the PJCHR's recommendation to establish a federal Human Rights Act,[105] and considers that, such framework, if developed, could be a useful reference point and means of ensuring that the Act upholds fundamental human rights principles.

120. In the absence of a federal Human Rights Act, the Law Council notes that there is significant guidance contained in the relevant international human rights law provisions, and the United Nations Rabat **Plan of Action**, on how to resolve the perceived tension between the right to freedom of expression and other rights.[106]

---

[101] Human Rights Committee, General Comment No. 34: *Article 19: Freedoms of opinion and expression*, U.N. Doc. CCPR/C/GC/34 (12 September 2021).
[102] *Human Rights Act 2004* (ACT) s 16(2); *Human Rights Act 2019* (Qld) s 21(2); *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 15(2).
[103] Australian Government, *Statutory Review of the Online Safety Act 2021* (Issues Paper, April 2024) Appendix 2.
[104] Law Council of Australia, *Federal Human Rights Charter* (Policy Position, November 2020) <https://lawcouncil.au/resources/policies-and-guidelines/federal-human-rights-charter>.
[105] Law Council of Australia, *A federal Human Rights Act is just right* (Media Release, 30 May 2024) <https://lawcouncil.au/media/media-releases/a-federal-human-rights-act-is-just-right>.
[106] United Nations, *The Rabat Plan of Action* (5 October 2012) <https://www.ohchr.org/en/documents/outcome-documents/rabat-plan-action>.

121. The Plan of Action provides key guidance to States on the difference between freedom of expression and 'incitement' to discrimination, hostility and violence, which is prohibited under criminal law. The Plan of Action suggests a high threshold for defining restrictions on freedom of expression, incitement to hatred, and for the application of Article 20 of the ICCPR, which includes 'any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law'.

Part 6: Regulating the online environment, technology and environmental changes

Question 27: Should the Commissioner have powers to act against content targeting groups as well as individuals? What type of content would be regulated and how would this interact with the adult cyber-abuse and cyberbullying schemes?

122. As a general proposition, the Law Council considers that the Commissioner should have the power to act against content targeting groups, as well as individuals.

123. Further, in the context of the risks faced by First Nations peoples in particular, any scheme:

- should be developed in very close consultation with the Commissioner, the First Nations Digital Inclusion Advisory Group, and the peak bodies representing the interests of First Nations peoples in Australia;
- should have, as at least one of its objectives, preventing or minimising online harm, to the extent it is faced by First Nations peoples;
- should be easy to access through a variety of means preferred by First Nations peoples;
- should empower the Commissioner to act quickly and efficiently to prevent the risk of harm; and
- should allow the decision maker to be able to consider, as a relevant factor in reaching their decision, the objective of the scheme, as to prevent or minimise First Nations peoples suffering online harm.

Question 28: What considerations are important in balancing innovation, privacy, security, and safety?

124. The Law Council recognises the need for online service providers to retain the ability to innovate. However, the harms currently being experienced online—particularly by children and adults within marginalised groups—mean that innovation must be balanced with privacy, security, and safety.

125. Many digital platforms have achieved an extraordinary level of integration into the daily lives of Australians. Consequently, online platforms hold large amounts of personal information about their users, and much of this information may have been obtained without proper consent. It is very difficult, if not impossible, for individual users of online platforms to withdraw consent, change user settings, or prevent harmful content being fed to them through algorithms over which the individual has little to no control.

126. The Law Council anticipates that the implementation of reforms to the Privacy Act will somewhat assist, noting that the Government has agreed, in-principle, that:

- consent must be voluntary, informed, current, specific, and unambiguous;[107] and
- the Privacy Act should expressly recognise the ability for individuals to withdraw consent in an easily accessibly manner.[108]

127. Therefore, as noted earlier in this submission, it is essential that there is a clear and consistent approach to this Review of the Act and the reforms to the Privacy Act.

Question 29: Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?

128. A technology-neutral approach is one where the legislation focuses on outcomes, rather than the specific technologies used to reach those outcomes. The Law Council regards this approach as central for any legislative regime that is to remain relevant. The objective should be to avoid technology- or platform-specific laws that become redundant, or only partially effective.[109] This is critical, given the rapid pace of technological advancement, and the evolution of harms that may be posed to children and other marginalised cohorts as a result of these technologies.

129. The Law Council's position in favour of a technology-neutral approach would not be affected by the introduction of a statutory duty of care or Safety by Design obligations.

[107] Australian Government, *Government Response: Privacy Act Review Report* (September 2023) <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF> 15, 17, 26.
[108] Ibid 17, 26.
[109] Law Council of Australia, *Inquiry into the opportunities and impacts of the uptake of artificial intelligence technologies in Australia* (Submission, 20 May 2024) <https://lawcouncil.au/resources/submissions/inquiry-into-the-opportunities-and-impacts-of-the-uptake-of-artificial-intelligence-technologies-in-australia> 8-9.