Inquiry into the Internet Search Engine Services Online Safety Code

Submission to the Senate Standing Committees on Environment and Communications

10 October 2025

www.humanrights.gov.au

ABN 47 996 232 602
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
National Info Service 1300 656 419

Australian Human Rights Commission

Contents

[Type here]

About the Australian Human Rights Commission

Our vision is an Australian society where human rights are respected, promoted and protected and where every person is equal in dignity and rights.

The Commission's key functions include:

- **Access to justice:** We help people to resolve complaints of discrimination and human rights breaches through our investigation and conciliation services.
- **Fairer laws, policies and practices:** We review existing and proposed laws, policies and practices and provide expert advice on how they can better protect people's human rights. We help organisations to protect human rights in their work. We publish reports on human rights problems and how to fix them.
- **Education and understanding:** We promote understanding, acceptance and public discussion of human rights. We deliver workplace and community human rights education and training.
- **Compliance:** We are the regulator for positive duty laws requiring employers and others to address sexual harassment, sex discrimination and other unlawful conduct.

Australian Human Rights Commission www.humanrights.gov.au

ABN 47 996 232 602

GPO Box 5218 Sydney NSW 2001

For general enquiries, call us on 1300 369 711.
For complaints, call us on 1300 656 419.
For TTY, call 1800 620 241.

Summary

1. Part 4A of the *Online Safety Act 2021* (Cth) (Social Media Ban) and Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) (SES Code) represent a new approach to online safety in Australia.
2. While age assurance is a central feature of this emerging framework, the Commission has serious reservations about whether it strikes the right balance in a human rights centred approach. Other safety by design approaches (such as content filtering, crisis response tools, education and Digital Duty of Care) could offer a more proportionate and rights-respecting pathway to protecting children online. These approaches have potential to shift responsibility from users to service providers and can be implemented with less risk of compromising privacy, autonomy or inclusion.
3. Our submission calls for stronger safeguards, clearer definitions and greater transparency. Online safety and safety by design measures must be human rights centred and enhance our rights – not diminish them.

Recommendations

4. The Commission makes the following recommendations.

Recommendations

1. eSafety works with industry to create safeguards within Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) to ensure that measures to restrict access to pornography do not inadvertently block access to inclusive, evidence-based sexual health and relationship information, particularly for LGBTQIA+ young people.
2. eSafety amends its Regulatory Guidance to expressly discourage age-restricted social media platforms from using government-issued identification and/or biometrics as a method of age assurance.
3. eSafety works with industry to clarify that government-issued identification and/or biometrics are not an acceptable method of age assurance under Compliance Measure 2 of Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material).
4. eSafety amends the Regulatory Guidance to expressly state in the guiding principles that the steps taken by providers be compliant with Australia's obligations under international human rights law.
5. The Australian Government prioritise the second tranche of privacy law reforms.
6. The Australian Government amends section 63C(5) of the Online Safety Act 2021 (Cth) to require that the Minister for Communications exercise their

discretion in accordance with clear criteria. These criteria should be designed to ensure decisions are evidence-based, transparent and consistent with the best interests of children.

7. eSafety amends the Social Media Minium Age Regulatory Guidance to mandate that an informed human in the loop be present and engaged in any challenge to an age assurance outcome.
8. eSafety works with industry to create an additional Compliance Measure in Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) which requires an accessible review pathway for users to challenge an age assurance outcome.
9. eSafety amends the Guidance to require age-restricted social media platforms to publish annual transparency reports.
10. eSafety works with industry to create an additional Compliance Measure in Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) which requires providers to publish annual transparency reports.
11. eSafety immediately establishes baseline parameters and the collection of data about the use of social media by under-16s.
12. The Australian Government and eSafety clarify that Class 1C and Class 2 materials excludes legitimate sexual health and educational content.
13. eSafety works with industry to introduce a Compliance Measure within Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) to conduct a human rights impact assessment when implementing the full suite of measures.
14. The Australian Government introduce legislation for the creation of a Digital Duty of Care.
15. eSafety conducts further consultation and human rights analysis of the impact and implementation of the Social Media Ban, with a larger and more diverse group of children and young people.

1 Human rights risks of social media and 18+ content

The Commission recognises the importance of protecting children and young people from harmful online content, including pornography and other harmful material. While there are positive aspects to both the SES Code and Social Media Ban, the Commission holds serious concerns about impact on access to information and privacy. A balanced approach is needed to ensure safety by design measures do not inadvertently block inclusive, evidence-based resources that support wellbeing and development.

5. The Commission acknowledges that online environments can facilitate serious harms, and that both:
   - Part 4A (Social Media Ban) of the *Online Safety Act 2021* (Cth) (OS Act); and
   - Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) (SES Code),

   aim to reduce children's exposure to harmful online content.

6. The Social Media Ban prevents under 16s from having a social media account on designated platforms. The SES Code seeks to reduce under 18s exposure to harmful, but not illegal internet content. This includes pornography and content which is sexually explicit, depicts high-impact violence or simulated gambling. It deploys a wider range of safety by design measures beyond age assurance (such as filtering of content, blurring of images etc). The Commission continues to hold serious reservations about the Social Media Ban due to the disproportionate impact it can have on the right to access information (particularly for vulnerable or marginalised groups) and concerns about age assurance.

Access to social media

7. Social media can be important for some children and young people who already face barriers to inclusion, safety and wellbeing - including those from culturally and linguistically diverse backgrounds, children with disability and LGBTQIA+ young people. For example, research shows that social media plays a vital role in supporting LGBTQIA+ young people by offering spaces where they can safely explore their identities, find relevant information and build connections with others who share similar experiences.[1]

8. Equally, social media can be harmful for children and young people due to the ease of access to age-inappropriate content. It can also negatively impact mental health through exposure to cyberbullying and addictive design features that encourage excessive use. Inadequate content moderation means children and

young people often encounter harmful material without adequate safeguards or support. These risks are further amplified by algorithmic systems that prioritise engagement, making it more likely that vulnerable users are exposed to sensational or damaging content.[2]

Access to pornography and other harmful content

9. The SES Code rightly makes it more difficult for children and young people to be exposed to pornographic content.[3] Exposure to online pornography can be connected to a range of harmful sexual beliefs and behaviours.[4] Reports indicate that nearly half of children between 9–16 experience regular exposure to sexual images.[5] Studies have found that 'pornography both contributes to and reinforces the kinds of social norms and attitudes that have been identified as drivers of violence against women',[6] and that viewing pornography is 'associated with unsafe sexual health practice'.[7]

10. A 2022 report also showed that 23% of 14–17-year-olds had encountered violent sexual material online, which fails to depict consent, safe sex or relational intimacy.[8] Consumption of this content may be associated with harmful sexual practices, sexual violence, stronger beliefs in gender stereotypes and sexually objectifying views of women.[9]

11. By reducing access and unintentional exposure to online pornography, the SES Code contributes positively to the fulfilment of several human rights. For example:
    - It assists Australia in meeting it obligations under the *Convention on the Rights of the Child* by ensuring children have access to age-appropriate information that promotes their well-being and development, including by protecting them from harmful content.[10]
    - It supports the rights of women and girls by addressing the role that pornography plays in reinforcing gender stereotypes and normalising sexual violence.[11]
    - It helps safeguard the right to health by limiting exposure to content linked with unsafe sexual practices and harmful attitudes towards sexual relations and intimacy.[12]

12. These protections are particularly important given the prevalence of violent and degrading sexual material online, and the disproportionate impact such content can have on young people. In this context, the SES Code represents a meaningful step toward creating safer digital environments that promote respectful relationships, gender equality and the wellbeing of children and young people.

13. While there is a compelling rationale for implementing measures that protect children and young people from pornographic and other harmful content, it is

important to ensure that such measures do not inadvertently limit access to safe and inclusive information - particularly for LGBTQIA+ young people. Many young people face barriers to comprehensive sex education that reflects diverse identities and experiences, and may turn to online spaces in search of understanding, connection and information. Protective frameworks should therefore be designed in ways that uphold the rights of all young people to access developmentally appropriate and non-exploitative resources.

14. The Commission has previously highlighted the need to balance access to information with online safety measures in its submission to the Statutory Review of the Online Safety Act. Any regulatory approach should strike this careful balance: protecting children from genuinely harmful and age-inappropriate content while ensuring that affirming and educational material is not indiscriminately removed.

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

2 Risks of age assurance

The Commission recognises that age assurance is a key feature of the SES Code and Social Media Ban and remains concerned that current approaches (e.g. government-issued ID, facial recognition and age inference) pose serious risks to privacy, inclusion and human rights. A more proportionate and rights-respecting approach should be prioritised to shift responsibility from users to service providers and platforms.

15. A key area of overlap between the SES Code and Social Media Ban is the emphasis on age assurance as a means to restrict access to unsuitable online content. Age assurance requires service providers and platforms to implement mechanisms that reliably determine a user's age.[13] This includes methods such as government-issued identification (ID) and biometric estimation,[14] which both have serious consequences for privacy, as data from all users will be collected and used in some way.

16. There are risks associated with the three main age assurance methods discussed in the Guidance (age verification, estimation and inference). These risks relate not only to human rights concerns, but also technical feasibility, practical limitations and implications for mass surveillance. While the Commission acknowledges that any safety by design initiative is well-intended, it must also be human rights centred. There is no perfect solution to keeping children safe online, and any solution will need to be proportionate to the risks posed. Alternative, less restrictive measures, such as a Digital Duty of Care (discussed below) are preferable.

Use of government-issued identification

17. Social media platforms may offer government issued identification (government ID) as one option for age assurance under the Guidance.[15] They cannot require it as the sole method, and must provide reasonable, privacy-preserving alternatives to ensure compliance is fair and inclusive.[16]

18. Under the SES Code, providers could also implement age assurance methods which require the use of government ID.[17] The use of government ID for age assurance poses a serious risk to privacy for all Australians.[18] Asking people to upload sensitive documents (e.g. passports or driver licences) without ensuring sufficient safeguards are in place is a serious intrusion on privacy. It creates heightened risks of data breaches, identity theft and misuse of sensitive personal information. Social media platforms have historically struggled to meet basic privacy and security standards,[19] and the comprehensive collection of identity data creates a high-value target for malicious actors. The Commission is

concerned that expanding corporate data collection may lead to harms that are incompatible with the human rights of all Australians – irrespective of their age.

19. The risks of collecting government ID are already impacting Australians with Discord having just reported that driver's licences and passports were among the forms of data accessed via a third-party customer service provider in a leak.[20]

Facial recognition technology

20. Mandating private technology companies to use facial recognition technology (FRT) to determine age is also not an acceptable alternative to government ID. Individuals should not be forced to choose between two highly intrusive methods (government ID or biometric scans) to access social media or use search engines. Framing these options as a choice creates the illusion of agency, when in reality both pathways compromise privacy and involve the collection of highly sensitive personal information.

21. The Commission has previously raised concerns about the use of FRT in Australia.[21] In its Human Rights and Technology Final Report, the Commission highlighted the technology's potential to infringe on the right to privacy, exacerbate discrimination and undermine public trust in digital systems.[22]

22. There is documented inaccuracy of FRT for certain demographic groups. The Age Assurance Technology Trial found that facial age estimation systems perform less reliably for individuals with darker skin tones and for those aged 16–20, raising serious concerns about equality and discrimination.[23]

23. People who don't have access to government ID might be pushed into using FRT, even though there is evidence of inaccuracy with FRT.[24] That means they could be wrongly blocked or treated unfairly. Age assurance mechanisms must be designed to uphold human rights by offering fair, respectful and privacy-preserving alternatives that do not force users to forsake their rights in order to participate in digital life.

24. The Commission continues to strongly support efforts to protect children from online harms, recognising the importance of ensuring that children can engage with digital environments in ways that support their rights and well-being. However, we have serious reservations about the methods proposed in this instance. Current age assurance technologies are not yet capable of implementing the Australian social media ban in a way that avoids significant human rights risks. Given the Government is committed to proceeding with the ban, it is essential that its implementation is closely monitored to ensure that rights are protected and that any unintended consequences are promptly addressed.

Recommendation 2: eSafety amends its Regulatory Guidance to expressly discourage age-restricted social media platforms from using government-issued identification and/or biometrics as a method of age assurance.

Recommendation 3: eSafety works with industry to clarify that government-issued identification and/or biometrics are not an acceptable method of age assurance under Compliance Measure 2 of Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material).

25. Public trust in social media platforms is low, and the use of either option risks further undermining confidence in both platforms and the Social Media Ban. Research shows that Australians (particularly young people) are uncomfortable with platforms collecting sensitive personal information, especially when the purpose is unclear or the safeguards are opaque.[25]

26. The Human Technology Institute (led by former Human Rights Commissioner, Ed Santow) has proposed a Model Law for Facial Recognition Technology (Model Law), which takes a risk-based approach grounded in international human rights law.[26] The Model Law sets out a legal framework to ensure that all FRTs are developed and deployed in ways that uphold human rights, promote transparency, and enable effective oversight and accountability.[27] While the Model Law offers a rights-based approach to managing these risks, such protections are not yet in place.

Age inference

27. Age inference enables platforms to draw probabilistic conclusions about a user's likely age based on behavioural patterns, contextual data and metadata already held by the service.[28] This approach avoids requiring users to submit additional personal information and can reduce barriers to access, particularly for users who may not possess government ID.

28. As noted in the Guidance, platforms may use existing signals such as account age, engagement patterns and device settings to infer whether a user is likely under 16.[29] However, the age-related signal examples provided on page 32 of the Guidance reveal the extent to which age inference relies on pervasive surveillance and profiling which includes accessing:
    - photos
    - tags
    - connections
    - engagement activity
    - linguistic analysis and/or
    - school-hour login patterns.

29. Accessing this type of information is intrusive and can enable social media platforms to create a detailed picture of a person's life. Relying on these data points can lead to discriminatory results. For example, relying on linguistic analysis of written information may disproportionately impact people with a cognitive disability. Additionally, age inference risks normalising the routine analysis of users' personal content and interactions, often without knowledge or meaningful consent.

Misleading messaging

30. The Guidance and surrounding messaging risks presenting technically accurate statements in a way that may oversimplify or obscure important nuances – for example, that platforms will not verify the age of all users to ensure compliance.[30] While technically accurate, this framing obscures the reality that every social media account holder will be subject to age inference.

31. Platforms are expected to deploy inference tactics to flag suspected under-16 accounts, which are then escalated to formal age assurance processes.[31] The Commission understands this to mean that all users, regardless of age, will have their photos, posts, connections and activity analysed to determine whether they should be flagged. In effect, age inference becomes a universal surveillance mechanism, with significant implications for privacy, autonomy and trust.

Human rights-centred approach

32. These risks underscore the need for human rights – including, but not limited to, rights to privacy, equality and non-discrimination, freedom of expression, access to information, and the rights of the child – to be more than an overarching consideration in the Guidance. While the Guidance states that human rights 'underpin' the guiding principles, this framing is insufficient.[32] Without a human rights centred-approach to online safety, platforms may prioritise technical efficiency over rights-respecting design.

Recommendation 5: eSafety amends the Regulatory Guidance to expressly state in the guiding principles that the steps taken by providers be compliant with Australia's obligations under international human rights law.

33. The Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) (Head Term) provides that industry must be able to demonstrate that its implementation of Compliance Measure are reasonable.[33] This expressly requires providers to take into account:

> the importance of protecting and promoting human rights online, including the right to freedom of expression, the right not to be subjected to arbitrary or unlawful interference with privacy, the right to protection from

exploitation, violence and abuse, and the rights and best interests of children, including associated statutory obligations;

Note: In this context, the rights of children include the rights recognised in the United Nations Convention on the Rights of the Child.[34]

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

Right to privacy

35. The right to privacy is a cornerstone which underpins freedoms of association, thought and expression, as well as freedom from discrimination.[35] In an age where digital participation has become embedded in everyday life, users are being given an illusion of choice – agree to have data collected or risk being left behind in an increasingly digital society. The Commission does not accept that digital participation should come at the expense of privacy.

36. Both the SES Code and Social Media Ban rely heavily on the *Privacy Act 1988* (Cth) (Privacy Act) to ensure the privacy of data collected as part of age assurance methods.[36]

37. Using the Privacy Act as the principle means of protecting the right to privacy is insufficient. The former Attorney-General stated that the Privacy Act 'has not kept pace with the changes in the digital world'.[37] Although the Commission welcomes the enactment of much-needed reforms under the *Privacy and Other Legislation Amendment Bill 2024* (Cth), these amendments represented only a fraction of the reforms committed to by government.[38]

38. To ensure that age assurance technologies do not compromise the right to privacy, the second tranche of Privacy Act reforms must deliver a modern, robust framework capable of addressing the unique risks posed by age assurance. The current reliance on outdated provisions leaves individuals vulnerable to opaque data practices, surveillance and potential misuse. Without these reforms, regulatory efforts to protect children online risk being undermined by inadequate privacy safeguards, eroding public trust and exposing users to new forms of harm.

Recommendation 4: The Australian Government prioritise the second tranche of privacy law reforms.

Children's Online Privacy Code

39. The Commission made a submission to the Office of the Australian Information Commissioner on the Children's Online Privacy Code. This submission emphasises the need to protect children's privacy in the context of social media

platforms and the impending ban. Specifically, it notes that social media platforms should be captured by the Children's Online Privacy Code despite under 16s no longer being technically able to hold accounts.

3 Accountability, oversight and transparency

The Commission emphasises the need for stronger accountability and oversight in the implementation of the Social Media Ban and SES Code - particularly regarding ministerial discretion, review mechanisms and transparency obligations. Without clear criteria, accessible challenge pathways or public reporting, decisions about age assurance and content access risk being opaque, inconsistent and potentially harmful to users' rights.

Minister's rule making power

40. Under the OS Act, the Minister for Communications (Minister) has the sole discretion to determine what social media platforms must comply with the Guidance via disallowance instruments.[39]

41. Disallowable instruments play an important role in regulating the digital ecosystem. However, the Minister's discretion should be guided by stronger, clearly defined criteria to ensure decisions are consistent, transparent and grounded in evidence.

42. The current approach gives the Minister broad power to decide which platforms must comply with the Social Media Ban. This creates uncertainty and inconsistency (as seen in the delayed inclusion of YouTube and uncertainty about which other platforms may be captured)[40] and means that important decisions about children's online safety can be made based on subjective or shifting criteria.

43. While flexibility is important in regulating fast-changing digital environments, the absence of clear decision-making standards or safeguards around the exercise of discretion increases the risk of arbitrary or politically motivated decisions. To ensure that platform regulation is evidence-based, transparent and aligned with the best interests of children, the legislation should embed stronger criteria to guide the Minister's discretion and promote accountability.

Recommendation 6: The Australian Government amends section 63C(5) of the *Online Safety Act 2021* (Cth) to require that the Minister for Communications exercise their discretion in accordance with clear criteria. These criteria should be designed to ensure decisions are evidence-based, transparent and consistent with the best interests of children.

Challengeable outcomes

44. The Commission acknowledges that the Guidance repeatedly states that age assurance outcomes must be contestable and subject to review.[41] However, we

are concerned that the Guidance does not go far enough in safeguarding the integrity of these review processes. The regulatory guidance rightly states that platforms should ensure a 'human in the loop' is involved in all review processes.[42] The Commission strongly supports this and believes it must go further.

45. A 'human in the loop' simply means that a person is involved somewhere in the decision-making process. However, this involvement can be superficial - for example, a person rubber-stamping an automated decision without understanding how it was made. The Commission recommends that this be strengthened to require an 'informed human in the loop'. This means a person who has access to the relevant information, understands how the age assurance system works (including any AI components) and is empowered to override or correct automated decisions. Without this, there is a risk that review processes will be performative rather than meaningful, and that users will be denied fair and accountable decisions about their access to digital spaces.

46. Ensuring informed and effective review processes is essential to upholding the right to access justice,[43] particularly where automated systems may impact individuals' rights or restrict access to digital spaces.

Recommendation 7: eSafety amends the Regulatory Guidance to mandate that an informed human in the loop be present and engaged in any challenge to an age assurance outcome.

SES Code

47. The SES Code does not prescribe a mechanism for users to challenge the outcome of an incorrect age assurance process. This omission is concerning given the increasing reliance on automated age assurance technologies, such as FRT and age inference, which carry known risks of error, demographic bias and limited transparency (as discussed above).

48. Unlike the Social Media Ban, which mandates accessible review pathways and human oversight, the SES Code lacks any equivalent safeguard. While general complaint and feedback mechanisms exist (Compliance Measures 13, 14, 17, and 18), they are not tailored to age assurance outcomes and do not guarantee a structured, transparent or fair process for users to contest age-based determinations. This creates a regulatory gap that risks unjust exclusion of users from accessing lawful content or services due to flawed age assurance methods.

49. The absence of a clear review pathway risks compounding digital exclusion for marginalised groups, including those whose age may be miscategorised due to demographic bias in AI models or FRT.

Recommendation 8: eSafety works with industry to create an additional Compliance Measure in Schedule 3 - Internet Search Engine Services Online

Safety Code (Class 1C and Class 2 Material) which requires an accessible review pathway for users to challenge an age assurance outcome.

Transparency

50. The Guidance requires platforms to provide detailed information to eSafety about their compliance with the Social Media Ban, including data on account removals, age assurance outcomes and review mechanisms.[44] However, the Guidance is silent on whether this information will be made publicly available. The Commission is concerned that this lack of transparency undermines public accountability and limits the ability of civil society, researchers and affected communities to scrutinise how both platforms are implementing the Social Media Ban and eSafety is regulating it.

51. Transparency is a cornerstone of human rights protection and promotion in digital environments. Decisions by platforms to remove accounts on the basis of age assurance can have serious consequences for human rights. Public reporting on the number of accounts removed, the number of successful challenges and the types of age assurance methods used would help ensure that these decisions are transparent and publicly accountable.

52. Platforms should be required to publish annual transparency reports detailing their compliance with the Social Media Ban. These reports should include anonymised, aggregated data on:
    - account removals
    - age assurance outcomes
    - review processes and
    - the number of successful challenges.

53. Annual transparency reports should also include information about the types of data used for age inference and the safeguards in place to protect users' rights. Making this information publicly available would promote accountability, build public trust and support evidence-based policy development.

Recommendation 9: eSafety amends the Guidance to require age-restricted social media platforms to publish annual transparency reports.

SES Code

54. The SES Code requires providers to report on their compliance with safety obligations to eSafety.[45] However, these reports are only submitted upon request and are not required to be made publicly available. There is no express obligation for providers to publicly publish data on their actions and outcomes in relation to the Compliance Measures.

55. This lack of public transparency limits the ability of civil society, researchers and affected communities to scrutinise how providers are implementing age

assurance and content filtering obligations. Without access to meaningful data, it is difficult for stakeholders to assess whether these measures are being applied fairly, proportionately and in a manner consistent with human rights.

Recommendation 10: eSafety works with industry to create an additional Compliance Measure in Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) which requires providers to publish annual transparency reports.

Review of Social Media Ban

56. Section 239B OS Act requires an independent review of the Social Media Ban within two years of s 63D OS Act taking effect. The Explanatory Memorandum reinforces this requirement, stating that the review will assess the effectiveness of the measures and consider whether changes to scope, minimum age (or if additional powers) are necessary.[46]

57. It is essential that the collection of baseline data about social media use and restrictions begins now. This will ensure that the statutory review of the Social Media Ban is informed by robust, comparative data from different points in time. Without this foundation, it will be difficult to meaningfully assess the impact of the Social Media Ban or recalibrate policies to ensure they remain proportionate and rights-respecting.

Recommendation 11: eSafety immediately establishes baseline parameters and the collection of data about the use of social media by under-16s.

4 Inadvertent censorship

The Commission welcomes safety-by-design measures to reduce exposure to harmful content but remains concerned that some measures under the SES Code may unintentionally restrict access to legitimate health and educational resources. To uphold the rights to health, information and non-discrimination, safeguards must be introduced to ensure protective measures do not inadvertently censor inclusive, evidence-based material.

58. The SES Code obliges service providers to:
    - reduce unintentional exposure to self-harm material[47]
    - provide crisis prevention information in response to search queries regarding an eating disorder[48] and
    - provide crisis prevention information in response to search queries regarding suicide and self-injury.[49]

59. These are examples of measures that place an obligation on providers to take a human right centred approach to safety by design. This can be considered as human rights centred because it enhances rights protection by reducing children's exposure to harmful content in compliance with the *Convention on the Rights of the Child.*[50]

60. Yet the SES Code's measures present both opportunities and challenges for the fulfilment of human rights. There are legitimate concerns about the accessibility of certain types of content which impedes the right to seek, receive and impart information.[51] It is important to recognise that although children have this right to access information, some material should not be easily accessible (as discussed above).

61. The challenge lies in ensuring that efforts to restrict harmful content do not inadvertently suppress legitimate, educational or affirming resources.

Over censorship

62. The Commission is concerned that the current definitions and application of Class 1C and 2 materials under the SES Code may inadvertently restrict access to legitimate, non-pornographic health and educational resources.[52] This raises significant human rights concerns, particularly in relation to the rights to health and access to information.[53]

63. eSafety summarises Class 1C and Class 2 material as that:

> which includes online pornography and other high-impact material as defined by reference to the National Classification Scheme. This includes themes such as suicide and simulated gambling.[54]

Inadvertent censorship

64. Both definitions lack safeguards to ensure they do not capture legitimate educational or health-related content.

65. This is concerning because in practice, content moderation systems (particularly those relying on automated detection and classification) have a documented history of over censorship. A key example is the common misclassification of LGBTQIA+ content as sexually explicit or inappropriate. Research has shown that platforms such as YouTube and Tumblr have disproportionately flagged or suppressed LGBTQIA+ content on the basis of 'restricted mode' or 'community standards', even when the content is educational.[55] This has serious consequences for LGBTQIA+ young people who already face significant barriers to accessing inclusive health education.

66. Equally, automated content moderation systems used by search engines and social media platforms have misclassified content related to women's health as sexually explicit, resulting in the removal or suppression of educational and health-related material. This includes posts promoting breastfeeding support, breast cancer awareness and maternal health education, which are often flagged due to the presence of anatomical terms such as 'breast' or images depicting breastfeeding (even when clearly non-sexual and medically relevant).[56]

67. Research has shown that young mothers rely heavily on online communities for breastfeeding support.[57] When such content is removed or suppressed, it undermines the right to access health information.[58] These practices also risk reinforcing harmful cultural norms that sexualise women's bodies regardless of context.

68. To uphold Australia's human rights obligations, it is essential that content moderation systems distinguish between explicit material and legitimate health education.

Recommendation 12: The Australian Government and eSafety clarify that Class 1C and Class 2 materials excludes legitimate sexual health and educational content.

69. To address the risks associated with restricting access to information under the SES Code and to uphold Australia's human rights obligations, providers should be required to conduct human rights impact assessments (HRIAs) when they first introduce compliance measures.

70. A HRIA is a systematic process used to identify, evaluate and address the potential effects of a policy, law or systems on people's human rights.[59] It ensures that new measures (such as content filtering) do not inadvertently harm or discriminate against individuals or groups, and that any risks are properly managed and mitigated.[60]

Inadvertent censorship

71. While the Head Term already requires providers to consider human rights, mandating HRIAs as a Compliance Measure in the SES Code would strengthen this obligation and provide greater protection against unintended harms when access to certain types of information is restricted.

Recommendation 13: eSafety works with industry to introduce a Compliance Measure within Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) to conduct a human rights impact assessment when implementing the full suite of measures.

5 Global experience

While the UK framework shares similar objectives with Australia's SES Code and Social Media Ban, early evidence reveals risks of over-censorship, inconsistent enforcement and reduced access to legitimate information.

72. The Australian government has described its new online safety measures as 'world-leading'.[61] Due to the novel nature of the Social Media Ban and the SES Code, there are few comparable international examples, and limited evidence on how these measures may impact the experiences of children and young people.

73. However, lessons may be drawn from the United Kingdon's 2023 *Online Safety Act 2023* (UK OS Act), which represents a comprehensive safety by design framework.[62] The UK legislation aims to make various online platforms, such as social media, search engines and pornography sites 'legally responsible for keeping people, especially children, safe online'.[63] Platforms captured by the UK OS Act have a legally binding responsibility to implement measures to mitigate online risks to children, including through robust age checks.[64]

74. While the UK OS Act is grounded in safety by design principles, its implementation has uncovered human rights issues related to age verification and information classification. These are discussed in the following sections.

75. With the legislation only becoming fully enforceable two months ago, evidence of its impact is not readily available - particularly evidence based on the experiences of children and young people. Notably, Ofcom carried out consultations with children and young people prior to the implementation of this legislation, with many outlining their fears and concerns.[65]

Access to information

76. The legislation's principles-based approach, provides scope for inconsistent interpretation from technology companies around what information will be classified as harmful to children.[66]

77. The UK OS Act defines content that is 'harmful to children' but legal, including pornographic content, material that promotes suicide, self-harm and eating disorders, abusive and hateful behaviour and violent content.[67]

78. Ofcom, as the regulator, provides guidance to companies about how to define these subjective categories,[68] but examples are already emerging of content being wrongfully classified as 'adult' in nature. For example, Wikipedia may be subject to the strictest level of age controls under the UK OS Act if designated a Category 1 service – a possibility that formed the basis of its recent unsuccessful legal challenge.[69] According to Wikimedia (who run Wikipedia), complying with

the rules would mean cutting access by around 75%, which would severely limit public access to information.[70] Importantly, Wikimedia warned that forcing users to verify their identity could put contributors' privacy and safety at risk.[71] This case shows how unclear and uneven enforcement of the UK OS Act undermines human rights, including the right to access information and the right to privacy.

79. In Ofcom's consultations with children and young people, many participants expressed concern about the legislation limiting their access to information online.[72] One participant said:

> how are they going to decide what's harmful? I remember revising for my biology exam and pictures were blocked, but that content is different from fighting and violence.[73]

80. This example highlights the risks posed by restrictions to children's access to information, including for education and awareness of events in one's own community.

81. Ofcom recognised the heightened impact that online safety legislation can have on LGBTIQA+ young people through consultations,[74] stating:

> good practice proposals around fact-checking and labelling for gendered disinformation could result in false positives related to gender identity and sexual orientation content, as malicious actors might exploit reporting features to trigger these processes.[75]

82. Ofcom's suggestion to mitigate this risk is that services 'implement robust verification processes and providing a clear appeal mechanism, as suggested in the draft Guidance'.[76]

83. Despite recognising this impact, the unintentional limiting of access to LGBTIQA+ resources has become an issue. Pride in Labour has launched a monitoring initiative and is encouraging users to report instances where platforms have restricted access to LGBTIQA+ content.[77]

Age verification

84. Under the UK OS Act, age verification is required for all people seeking to access adult content. These regulations impact a broad range of services, not just those which deal exclusively with mature content. For example, entertainment platforms like Spotify and Xbox have required British users to verify their age.[78] Much like the Australian SES Code and Social Media Ban, platforms in the UK are not required to use a specific method of age verification to comply, as long as they use one that is deemed 'effective'.[79] Effective age assurance include facial age estimation and photo-identification matching, which this submission has already outlined concerns with.

Global experience

85. After the UK OS Act came into effect, the UK saw an increase in virtual private network (VPN) use.[80] This trend indicates significant concern about how privacy is being impacted by age verification requirements. The Internet Matters Tracker Survey, which involved 1,000 children and 2,000 parents, found that the most significant concerns around age assurance were privacy, data use and access to documentation.[81]

86. eSafety should continue to monitor the impacts of the UK OS Act, with a particular focus on the experiences of children and young people. In the absence of robust child-focused evidence from global examples, decisions must be made based on the best interest of children.

6 Digital duty of care

The Commission supports in principle the introduction of a legislated Digital Duty of Care to unify and strengthen Australia's online safety framework. This approach would shift responsibility from individual users to service providers, requiring platforms to take reasonable steps to prevent foreseeable harms through safety-by-design, risk assessments and transparency reporting. If carefully designed with robust human rights safeguards, a Digital Duty of Care offers a proportionate and coherent way to address systemic online risks and better protect all users.

87. A key objective of the Phase 2 Codes is to protect and prevent children and young people from being exposed to content which is inappropriate and developmentally harmful for them.[82] Equally the Social Media Ban aims to safeguard the '… health and wellbeing of the youngest users of social media platforms …'.[83] These initiatives reflect a growing recognition to make digital spaces safer for children and young people. While the Commission acknowledges the intent behind these efforts, we remain concerned about the fragmented and piecemeal nature of protections.

88. What is needed is a whole-of-environment response to online safety, one that addresses the systemic nature of online harms. The Commission notes the potential benefits of introducing a Digital Duty of Care, as recommended by the Statutory Review of the Online Safety Act and supported by the former Minister for Communications.[84]

89. A Digital Duty of Care would place a positive obligation on online service providers to take reasonable steps to prevent foreseeable harms on their platforms.[85] It shifts the burden of safety away from individual users, and onto the entities best positioned to identify and mitigate risks: the service providers themselves.

90. The Statutory Review of the Online Safety Act proposed that this duty be underpinned by safety-by-design principles, regular risk assessments, mitigation strategies and transparency reporting.[86] Importantly, the Digital Duty of Care is not a technical solution in itself but a policy framework that requires technical implementation. It demands that services embed safety into their architecture, algorithms and user interfaces, and that they continuously monitor and improve their systems to reduce harm.[87]

91. The Commission provides in principle support for the introduction of a Digital Duty of Care, noting that this support is contingent on the details of the proposed framework and its implementation. Any Digital Duty of Care must be carefully designed to include robust safeguards that uphold fundamental human rights, including freedom of expression, privacy, access to information

and non-discrimination. If appropriately implemented, such a duty would offer a coherent and rights-respecting basis for regulating online harms, ensure accountability for service providers and better protect all users in an increasingly complex and immersive digital environment.

Recommendation 14: The Australian Government introduce legislation for the creation of a Digital Duty of Care.

7 Other matters

The Commission raises concerns about inconsistent user experiences under the Social Media Ban, noting that platform discretion may result in fragmented protections and unequal outcomes for children. It also highlights the limited scope of eSafety's consultation process and the reliance on government materials to assess human rights compatibility, which undermines transparency and accountability. To ensure evidence-based and inclusive policy development and implementation, further consultation and human rights analysis are needed.

Inconsistent user experience

92. The Commission is concerned that the significant discretion afforded to social media platforms in how they choose to comply with the Guidance risks creating a fragmented and inconsistent landscape of protections for children. In the absence of prescriptive standards or minimum technical requirements, platforms are left to determine what constitutes 'reasonable steps' based on their own interpretation of the Guidance. This may result in vastly different approaches to age assurance across platforms, with some deploying robust, privacy-preserving systems and others relying on minimal or opaque measures.

93. This fragmentation is problematic given the diversity of platforms in the Australian digital ecosystem. Smaller platforms, niche services or those with limited resources may adopt low-cost or low-certainty age assurance methods that fail to detect underage users. Meanwhile, larger platforms may implement more sophisticated systems, but with greater risks of overreach, surveillance or exclusion. Without a baseline standard, children's safety becomes contingent on the commercial priorities and technical capacity of individual platforms. The Commission believes that a rights-respecting regulatory framework must ensure consistency in outcomes, not just flexibility in implementation.

Statement of Commitment to Children's Rights

94. On 16 September eSafety released a Statement of Commitment to Children's Rights. The Commission acknowledges that eSafety has undertaken consultations with children, young people and child rights experts on the Social Media Ban – these efforts are always welcomed.

95. However, the consultation process was limited in scope. Only 53 children and young people were included in this particular consultation process on the Social Media Ban, which will affect all Australians, including those over 16 who will be subjected to age inference measures.[88] This sample size is insufficient to meaningfully assess the impact on rights.[89]

Recommendation 15: eSafety conduct further consultation and human rights analysis of the impact and implementation of the Social Media Ban, with a larger and more diverse group of children and young people.

96. There are also serious shortcomings in the analysis itself. It is disappointing that eSafety relied on the Government's Explanatory Memorandum as evidence of compatibility with human rights.[90] The Statement of Compatibility produced during the legislative process was criticised by submissions to the Senate Standing Committee on Environment and Communications as underdeveloped and lacking engagement with Australia's full human rights obligations.[91]

97. Both the Senate Standing Committee on Environment and Communications and the Parliamentary Joint Committee on Human Rights (PJCHR) expressed concern about the truncated legislative process, which limited the opportunity for meaningful scrutiny.[92] The PJCHR noted that it was unable to seek further information from proponents due to the rushed timeframe, and the Senate Committee acknowledged that almost all submitters and witnesses raised serious concerns about the lack of time afforded to consider the ban.[93]

Endnotes

[1] Craig Shelley, et al., 'Can Social Media Participation Enhance LGBTQ+ Youth Well-Being? Development of the Social Media Benefits Scale' (2021) 7(1) *Social Media + Society* 1, 8; Boston Children's Digital Wellness Lab, *The Online Experiences of LGBTQ+ Youth* (Webpage) <https://digitalwellnesslab.org/research-briefs/the-online-experiences-of-lgbtq-youth/>.

[2] See generally Smitha Mills, et al., 'Engagement, user satisfaction, and the amplification of divisive content on social media' (2025) 4(3) *PNAS Nexus* 1.

[3] SES Code Compliance Measures 1-7.

[4] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 7.

[5] Antonia Quadara, Alissar El-Murr & Joe Latham, *The Effects of Pornography on Children and Young People* (Australian Institute of Family Studies, Report, December 2017) 10.

[6] Our Watch, *Pornography, Young People and Preventing Violence against Women* (Background Paper, 2020) 14.

[7] Our Watch, *Pornography, Young People and Preventing Violence against Women* (Background Paper, 2020) 14.

[8] eSafety Commissioner, *Mind the Gap: Parental Awareness of Children's Exposure to Risks Online* (Report, February 2022) 47.

[9] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 7.

[10] *Convention on the Rights of the Child* art 17(e).

[11] While no single article in the *Convention on the Elimination of all Forms of Discrimination against Women* ('CEDAW') explicitly names gender-based violence as a form of discrimination to be eliminated - art 1 defines 'discrimination' to include gender-based violence due to clarifications included in *General recommendation No. 35 (2017) on gender-based violence against women* 8 [21]. Article 2 of CEDAW then goes on to require states to eliminate such discrimination; eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 7; ICESCR art 12.

[12] *International Covenant on Cultural, Economic and Social Rights* ('ICESCR') art 12.

[13] See generally SES Code Compliance Measures; eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025).

[14] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 12-14.

[15] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 14.

[16] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 14.

[17] SES Code Compliance Measure 2.

[18] *International Covenant on Civil and Political Rights* art 17.

[19] See e.g. Federal Trade Commission, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* (Staff Report, September 2024).

10.

8.

[20] Josh Taylor, 'Proof-of-age ID leaked in Discord data breach', *The Guardian* (Online, 07 October 20205) <https://www.theguardian.com/games/2025/oct/07/discord-data-breach-proof-of-age-id-leaked>.
[21] Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021) 111-120.
[22] Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021) 111-120.
[23] Age Check Certification Scheme, *Age Assurance Technology Trial Part D Age Estimation* (Trial Report, August 2025) 70-73; eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 13.
[24] Age Check Certification Scheme, *Age Assurance Technology Trial Part D Age Estimation* (Trial Report, August 2025) 70-73; eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 13.
[25] Social Research Centre, Age Assurance Consumer Research (Analytical Report, December 2024) 39-45.
[26] See generally Human Technology Institute, *Towards a Model Law* (Report, September 2022).
[27] See generally Human Technology Institute, *Towards a Model Law* (Report, September 2022).
[28] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 12-14.
[29] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 32-33.
[30] eSafety, 'New regulatory guidance released to support social media industry ahead of minimum age law' (Media Release, 16 September 2025); eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 14
[31] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 30-34.
[32] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 21.
[33] Head Term s 5.1.
[34] Head Term s 5.1(b)(iii).
[35] Office of the Australian Information Commissioner ('OAIC'), '*What is Privacy?*' <https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy>.
[36] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 24-25; See generally Head Term.
[37] The Hon Mark Dreyfus KC MP, *Landmark Privacy Act Review report released* (Media Release, 16 February 2023). <https://ministers.ag.gov.au/media-centre/landmark-privacy-act-review-report-released-16-02-2023>.
[38] See generally, Attorney-General's Department, *Government Response Privacy Act Review Report* (Report, 2023).
[39] *Online Safet Act 2021* (Cth) s 63C(5); eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 6-7.

10.

8.

[40] Ange Lavoipierre, 'Legal fights are brewing over which online social platforms will have to ban under-16s', *ABC News* (Online, 24 September 2025) <https://www.abc.net.au/news/2025-09-24/digital-dilemna-social-media-age-ban-platforms/105807302>.

[41] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 41-42.

[42] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 42.

[43] *International Covenant on Civil and Political Rights* ('ICCPR') art 2(3).

[44] eSafety, *Social Media Minimum Age Regulatory Guidance* (Regulatory Guidance, September 2025) 49.

[45] *Schedule 3 - Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)* ('SES Code'), Compliance Measure 25.

[46] Explanatory Memorandum, *Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]* 28.

[47] SES Code Compliance Measure 10.

[48] SES Code Compliance Measure 12.

[49] SES Code Compliance Measure 11.

[50] *Convention on the Rights of the Child* art 17(e).

[51] ICCPR art 19.

[52] SES Code Pt 7.

[53] ICESCR art 12; ICCPR art 21.

[54] eSafety, *Industry codes and standards* (Webpage) <https://www.esafety.gov.au/industry/codes#:~:text=The%20material%20to%20be%20considered,as%20suicide%20and%20simulated%20gambling>.

[55] See generally Clare Southerton, et al., 'Restricted modes: Social media, content classification and LGBTQ sexual citizenship' (2020) 23(5) *New Media & Society* 920.

[56] See generally CensHERship, *Censorship Revealed* (Report, June 2025).

[57] Christina Severinsen, Eva Neely & Rochelle Hutson, 'Resisting stigma: the role of online communities in young mothers' successful breastfeeding' (2024) 19(17) *International Breastfeeding Journal* 1, 1-2.

[58] ICESCR art 12.

[59] Australian Human Rights Commission & National Australia Bank, *Human Rights Impact Assessment Tool: AI-informed Decision-making Systems in Banking* (September 2023) 7-8.

[60] See e.g. Australian Human Rights Commission, *Technology and Human Rights* (Final Report, 2021) 55-59 in the context of artificial intelligence.

[61] Anthony Albanese & Michelle Rowland, 'Albanese Government delivers world-leading legislation to protect children online' (Media Release, 21 November 2024).

[62] https://www.legislation.gov.uk/ukpga/2023/50

[63] Ofcom, *Protecting children from harms online: A summary of our decisions* (Summary Report, 24 April 2025) 2.

[64] See generally Ofcom, *Protecting children from harms online: A summary of our decisions* (Summary Report, 24 April 2025).

10.

8.

[65] Ofcom and Revealing Reality, *Consulting children on Protection of Children Online Safety Protocols* (2025) 3 & 5.
[66] George Billinge, 'Everything the right - and the left – are getting wrong about the Online Safety Act', *The Guardian* (Online, 02 August 2025) <https://www.theguardian.com/commentisfree/2025/aug/01/everything-right-left-politics-getting-wrong-online-safety-act>.
[67] See generally Ofcom, *Protecting Children from Harms Online: Guidance on Content Harmful to Children* (24 April 2025).
[68] See generally Ofcom, *Protecting Children from Harms Online: Guidance on Content Harmful to Children* (24 April 2025).
[69] Reuters, 'Wikipedia operator loses court challenge to UK Online Safety Act regulations', *Reuters* (Online, 11 August 2025) <https://www.reuters.com/sustainability/society-equity/wikipedia-operator-loses-court-challenge-uk-online-safety-act-regulations-2025-08-11/>.
[70] Chris Vallance, 'Wikipedia loses challenge against Online Safety Act verification rules', *BBC News* (Online, 12 August 2025) <https://www.bbc.com/news/articles/cjr11qqvvwlo>.
[71] Wikimedia Foundation, *Wikimedia Foundation Challenges UK Online Safety Act Regulations* (Webpage) <https://wikimediafoundation.org/news/2025/09/12/wikimedia-foundation-challenges-uk-online-safety-act-regulations/>.
[72] Ofcom and Revealing Reality, *Consulting children on Protection of Children Online Safety Protocols* (2025) 3 & 18.
[73] Ofcom and Revealing Reality, *Consulting children on Protection of Children Online Safety Protocols* (2025) 3 & 20.
[74] Ofcom, *A safer life online for women and girls: Practical guidance for tech companies* (Practical Guidance, 25 February 2025) 3, 50 & A2.29.
[75] Ofcom, *A safer life online for women and girls: Practical guidance for tech companies* (Practical Guidance, 25 February 2025) 3, 52 & A2.29.
[76] Ofcom, *A safer life online for women and girls: Practical guidance for tech companies* (Practical Guidance, 25 February 2025) 3, 52 & A2.29.
[77] Pride in Labour, *Is the Online Safety Act Blocking LGBTQ+ Resources?* (Weebpage) <https://www.prideinlabour.org.uk/post/is-the-online-safety-act-blocking-lgbtq-resources>.
[78] https://www.theguardian.com/commentisfree/2025/aug/09/uk-online-safety-act-internet-censorship-world-following-suit
[79] OF com guidance - the link wont paste with correct formatting
[80] Liv McMahon, 'VPNs top download charts as age verification law kicks in', *BBC News* (Online, 29 July 2025) <https://www.bbc.com/news/articles/cn72ydj70g5o>.
[81] Katherine Lai, Katherine, Age assurance and online safety: What parents and children have to say (Internetmatters.org, Report, 11 April 2025).
[82] Head Term s 1.1.
[83] Explanatory Memorandum, *Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]* 1-2.

10.

8.

[84] Delia Rickard, *Statutory Review of the Online Safety Act* (October 2024) 24, rec 4; Michelle Rowland, 'New Duty of Care obligations on platforms will keep Australians safer online' (Media Release, 14 November 2024).
[85] Delia Rickard, *Statutory Review of the Online Safety Act* (October 2024) 50.
[86] See generally Delia Rickard, *Statutory Review of the Online Safety Act* (October 2024) chp 5.
[87] See generally Delia Rickard, *Statutory Review of the Online Safety Act* (October 2024) chp 5.
[88] Australian Youth Affairs Coalition & eSafety, *Consultations with children and young people on the social media minimum age* (Summary Report, August 2025) 4-5; eSafety, *eSafety's Implementation of the Social Media Age Restrictions: Statement of Commitment to Children's Rights* (September 2025) 2.
[89] Australian Youth Affairs Coalition & eSafety, *Consultations with children and young people on the social media minimum age* (Summary Report, August 2025) 4-5; eSafety, *eSafety's Implementation of the Social Media Age Restrictions: Statement of Commitment to Children's Rights* (September 2025) 2.
[90] eSafety, *eSafety's Implementation of the Social Media Age Restrictions: Statement of Commitment to Children's Rights* (September 2025) 1; see Explanatory Memorandum, *Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]* 9-16,
[91] See e.g. Flinders University, Submission No 69 to the Senate Standing Committees on Environment and Communications, *Online Safety Amendment (Social Media Minimum Age) Bill 2024* (22 November 2024) 1
[92] Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 11 of 2024, 27 November 2024) 67 [1.176]; Senate Standing Committee on Environment and Communications, *Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]* (Final Report, 26 November 2024) 26 [2.86].
[93] Senate Standing Committee on Environment and Communications, *Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]* (Final Report, 26 November 2024) 26 [2.86]; Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny Report* (Report 11 of 2024, 27 November 2024) 67 [1.176].