Australian Human Rights Commission

Statutory Review of the Online Safety Act 2021

Australian Human Rights Commission

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

28 June 2024

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
National Information Service 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
National Information Service 1300 656 419
TTY 1800 620 241

1 Introduction

1. The Australian Human Rights Commission (Commission) welcomes the opportunity to make this submission to the Statutory Review (Review) of the *Online Safety Act 2021* (Cth) (OS Act).

2. The role of the Commission is to work towards a world in which human rights are respected, protected and fulfilled. The Commission is Australia's National Human Rights Institution.

3. The Commission recognises the intersections between online safety and a number of human rights. Drawing on the Commission's expertise and experience, this submission highlights just some of these intersections. This includes, in particular the specific expertise of the National Children's Commissioner, Race Discrimination Commissioner and Sex Discrimination Commissioner.

4. The Commission recognises the importance of the Office of the eSafety Commissioner's (eSafety) role under the OS Act as Australia's independent regulator for online safety. As the human rights of many people are impacted in online spaces, the role of eSafety is more important than ever. The Commission welcomes further opportunities to engage with the Review.

2 Children posting criminal activity online

5. There has been increasing community concern around criminal or violent activity being posted on social media in an effort to increase notoriety. In some cases, this social media activity includes posts from children under 18.

6. In the exercise of any powers to respond to these matters it is critical for all actors, including eSafety and law enforcement bodies, to consider the unique needs, vulnerabilities, and rights of children, including those in conflict with the law. It is important to recognise the underlying marginalisation and disadvantage that is often present in these cases.

7. Under art 40 of the Convention on the Rights of the Child (CRC), these children should not be treated the same as adults, and their age should be taken into account. In the first instance, every effort should be made to use alternatives to a criminal justice response where a child has

committed an offence, including where the posting of material on social media constitutes a criminal offence.

8. Policy responses in this area should also reflect other well-established principles under the CRC that underpin approaches to child justice. These include the use of detention only as a last resort, the establishment of a minimum age of criminal responsibility (recommended to be 14 years of age),[1] and an approach that avoids judicial proceedings whenever appropriate and that promotes a child's reintegration.

9. It is also of concern that social media posts of this criminal activity, whether posted by adults or the children themselves, can be used to publicly demonise children across social media and in mainstream media.[2] Images of children who have allegedly committed offences or are suspected of committing offences are increasingly being shared by adults across social media platforms, as well as by media outlets.[3] In some cases, the identities of these children are discernible.

10. The screenshotting and sharing of these images, and the identification of children in contact with the law can perpetuate harm and reduce a child's prospects of community reintegration.[4] It also contravenes their right to privacy at all stages of proceedings under art 40 of the CRC. The commentary to the Beijing Rules emphasises that children are particularly susceptible to stigmatization and points to criminological research providing evidence of the detrimental effects resulting from the permanent identification of children as 'delinquent' or 'criminal'.[5] The dissemination of this material can also result in abuse, harassment and cyberbullying of depicted children.[6] This may be particularly true for First Nations children, and children from culturally and racially marginalised communities who experience additional racist bullying and harassment online.[7]

11. Greater obligations on social media platforms to mitigate the risks to children associated with the posting and dissemination of material depicting criminal activity should be considered. Strong and nationally consistent guidelines for media outlets on the dissemination of online material featuring children are also required.

12. Any extension of eSafety's powers to address the posting of crimes must be balanced with eSafety's responsibilities to keep all children safe online, including children accused of criminal behaviour.

Recommendation 1: The Office of the eSafety Commissioner consider the full spectrum of child rights, including children's right to privacy and protection, in considering its role and powers to address the posting of material promoting criminal activity.

3 Access to pornography

13. Mainstream pornography will often target a male heterosexual audience and often depict sexual violence and degrading scenarios involving women. The Roadmap for Age Verification (Roadmap) notes that there is research indicating a correlation between mainstream online pornography and harmful sexual beliefs and behaviours.[8]

3.1 Evolving capacity of the child

14. Proposals to include mandatory age verification mechanisms are designed to ensure that children access age-appropriate material and prevent them from being exposed to harmful online content.

15. When determining what is 'age appropriate', the evolving capacities of the child must be taken into account. As noted by the former Special Rapporteur on the Right to Privacy, Professor Joe Cannataci, 'children vary enormously in their physical, intellectual, social and emotional capacity', and online risks change based on their stage of development, individual circumstances and environmental factors – and are not best determined by reference chronological age alone.[9] While there is harmful online content that will simply not be appropriate for any children to access, in relation to other content a blanket or blunt approach to age restrictions and consent may not be necessary or desirable. For example, teenagers will have a greater need for privacy and a stronger ability to understand consent processes than younger children.

3.2 Age-appropriateness

16. The former Special Rapporteur on the Right to Privacy, Professor Joe Cannataci cautioned that the 'notion of age-appropriateness sits uneasily with the principle of evolving capacity' and recommended that state

parties 'adopt age-appropriate standards as a regulatory instrument only with the greatest of caution when no better means exist'.[10] He made the following points in this regard:

- Material may be age appropriate and still harmful to children and their rights. The mechanism may protect and empower a child when individualised, but may not meet the needs of a cohort of children given the considerable variation in intellectual and emotional development among children of the same age.
- As a generic threshold, age appropriateness poses inequities for children of differing capacity and is a crude measure of their evolving capacities, potentially constraining the development of their personalities and the autonomous exercise of their rights, and is possibly discriminatory.
- When age is the criterion for accessing services, verifiable identity documents are required, raising concerns around security, prescriptive approaches and the lack of age assurance standards, tools and industry certification schemes. Others indicate that age verification processes can be delivered in a way that is compatible with privacy.[11]

3.3 Child access

17. Early and frequent exposure to online pornography has been connected to a range of harms affecting children. Nearly half of children between the ages of 9–16 experience regular exposure to sexual images.[12] 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',[13] and that viewing pornography is 'associated with unsafe sexual health practice'.[14]

18. Access to pornography is increasingly commonplace, with 75% of 16–18-year-olds having seen online pornography – of which nearly one-third were under 13 when they first viewed it.[15] Such widespread access is concerning, as exposure to some types of pornography (e.g. those which depict violent, sexist or racist scenarios) may negatively shape young people's sexual understanding, expectation and experiences.

19. For example, a 2022 report evidenced that 23% of 14–17-year-olds had encountered violent sexual material online, which fails to depict consent,

safe sex or relational intimacy.[16] Consumption of this content may be associated with harmful sexual practices, sexual violence, stronger beliefs in gender stereotypes and sexually objectifying views of women.[17]

20. Young men encounter pornography at a younger age and more frequently than their female counterparts.[18] For example 21% of young men encounter pornography daily, compared to 4% of young women.[19] These more frequent encounters are associated with an increase in unwanted sexual behaviours (e.g. sending sexual pictures, rude remarks, touching etc).[20]

21. It is within this context that eSafety is pursuing a pilot program to test Age Verification to limit child access to pornography. The Commission supports the pilot program. As noted by National Children's Commissioner, Anne Hollonds, 'I'd like to see a greater sense of urgency for reform that will safeguard our most vulnerable children'.[21]

Recommendation 2: The Office of the eSafety Commissioner's Age Verification Pilot be supported and appropriately resourced.

22. However, age-verification techniques may themselves pose risks for children's privacy and data protection, along with the privacy of all users of online platforms who will also be required to verify their ages before use. Age verification measures link a person's identity to their online activity. This can create prospects for surveillance, security breaches, leaks, data sales or criminal misuse of identifying information.[22] All age-verification techniques must be consistent with privacy and data protection principles. If this cannot be guaranteed, other approaches to protecting children from online harms may be preferable.

23. The use of age-verification techniques should also be context-specific and proportionate. These techniques may be required where age-verification is necessary to prevent children from engaging in illegal activity, such as buying weapons, alcohol or participating in online gambling, and where the potential for harm is high, like pornography websites, but may be disproportionate in other contexts.

24. For example, the United Kingdom's Age Appropriate Design code of practice (UK Code), is non-prescriptive and highlights a range of potential

age-verification measures for services to consider, of varying levels of strength. These range from 'self-declaration', where a user simply states their age, to 'hard-identifiers' requiring the provision of ID.[23] Notably, it recommends against giving users no choice but to provide hard identifiers. This is because some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age-verified services at all, even if they are age-appropriate. Requiring hard identifiers may also have a disproportionate impact on the privacy of adults.

Recommendation 3: The Office of the eSafety Commissioner consider context and proportionality in the piloting and proposed use of age-verification techniques.

25. Children's privacy is more complex than adult's right to privacy, due to the particular vulnerability of children; parental rights to raise their child; and children's changing capacities and development that affect, for example, the application of consent mechanisms.

26. In acknowledgement of these unique considerations, the Commission continues to support the recommendation of the Privacy Act Review to introduce a Children's Online Privacy Code. This Code would provide specific guidance on upholding the best interests of the child (discussed at section [4]) in the design of services and collection and use of children's data,[24] including in relation to age verification.

27. This code could be modelled on the UK Age Appropriate Design Code, which places the best interests of the child as a primary consideration in the design and development of online services that children are likely to access.[25] The views of children should be sought and taken into account in the development of this Code.

Recommendation 4: A Children's Online Privacy Code be introduced as a priority, including prior to the introduction of large-scale age verification measures.

3.4 Online education resources

28. Education remains a foundational safeguard against harmful sexual attitudes and behaviours. Sex education which is inclusive of gender and sexualities may increase resilience in people to violent and sexist pornography. Research has also shown it may reduce the likelihood of LGBTIQ+ young people seeking out information from pornography websites due to inadequate sex education (in a study by eSafety, 58% of LGBTIQ+ felt current sex education was insufficient).[26]

29. Further research from eSafety has shown that a third of young people said their parents were not equipped to support them to manage the impacts of pornography (41% of LGBTIQ+ young people) and 38% claimed that education should also be provided to parents and carers to assist them.[27]

30. Young LGBTIQ+ people are significantly more likely to believe that there are some positive impacts of online pornography than their straight counterparts. This may be driven, in part, due to a lack of appropriate sex education in schools. For example, one third of LBGTIQ+ secondary students have never heard of LBGTIQ+ being inclusively discussed as part of sex health education.[28] Research has affirmed that some pornography can be validating and affirming for those who are not represented in mainstream media and sex education – especially LGBTIQ+ young people.[29].

31. The Commission recognises the importance of education and awareness raising to support and protect children and young people, and address some of the specific harms associated with online pornography. The recommendations made by eSafety to the Australian government to develop evidence-based, age-appropriate educational resources about online pornography; develop complementary resources for parents, carers, frontline workers, and educations; and ensure greater national coordination and collaboration with respect to respectful relationships education, should be progressed.[30]

Recommendation 5: The recommendations made by the Office of the eSafety Commissioner directed towards education and awareness

raising – specifically Recommendations 5 & 6 in the *Roadmap to age verification* – should be progressed.

32. The Roadmap discusses several age assurance mechanisms which may be trialled during the pilot. Despite assurances about privacy and anonymity the Commission remains concerned about the use of biometrics (discussed below) and digital identity mechanisms to determine age.

33. There is a genuine danger in the 'sexual privacy' of gender minorities or sexual minorities being violated. Information which can determine a person's sexuality if leaked during a data breach may present a real threat of harm to them.

3.5 Biometric verification tools

34. The age verification pilot, as noted in the Roadmap, will test facial recognition technologies (FRT) to estimate a person's age. Based on information in the Roadmap, it does not appear that either one-to-one or one-to-many matching will be conducted via FRT.

35. However, the collection and use of sensitive biometric information raises serious human rights concerns. Concerns have been raised about accuracy and bias when FRT is used to analyse, for example, non-masculine features or non-white skin tones.[31] The Commission has also made various recommendations with respect to the use of FRT in its Final Report[32] and *Privacy Act 1988* (Cth) submission calling for greater regulation of biometric technologies.

36. These risks are exacerbated by the absence of legislation addressing FRT. In the absence of FRT-specific regulation, such as that proposed by the University of Technology Sydney's Model Law (Model Law),[33] the Commission has previously called for a moratorium on the use of FRT and other biometric technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement.[34]

37. The Model Law on FRT provides a clear example of the type of law reform that is needed to protect against the risks FRT poses to human rights.[35] This includes the provision that FRT developers and deployers must complete a Facial Recognition Impact Assessment of the potential harms,

including the potential human rights risk. This Facial Recognition Impact Assessment would be registered, publicly available and could be challenged by the regulator or interested parties.

38. While it may be useful to use FRT in the pilot program to provide valuable insights, consideration needs to be given to the identified human rights concerns both in terms of any pilot program and subsequently any decision to mandate this technology as a final form of age verification.

Recommendation 6: Facial recognition technologies are an inappropriate form of mandatory age verification process until facial recognition technology specific legislation is introduced.

39. Voice age analysis tools are canvassed in the Roadmap and also present human rights concerns. The accuracy of the tool is limited by a person's ability to read and speak clearly in ways that correlate to assumed biological age. People who have difficulty with enunciating clearly due to disability may face additional barriers. Equally children experience puberty at different ages, with some experiencing drops in their vocal range much earlier than others. The accuracy may also be impacted by accents or low language fluency.[36]

40. Human rights concerns surrounding bias, accessibility and fairness were also raised during eSafety's consultations with young people and their Youth Council.[37] When developing policy which effects children and young people, their views must be a central consideration.

41. These concerns are in addition to the privacy concerns noted above in respect of FRT. The Roadmap identifies other forms of age verification (e.g. digital tokens) which do not utilise biometric information. While the pilot ought to consider all options available, the use of biometrics raises human rights concerns that need to be addressed.

Recommendation 7: The use of biometric technologies as a form of mandatory age verification should not occur without legal protections being introduced to address human rights risks.

4 Best interests of the child

42. Children now grow up engaging with online environments which pose both risks and opportunities for children to realise their rights and contribute to the world around them.[38] The child's 'best interests' principle should be at the forefront of all business in the digital industry:

> The best interests of children should be the priority requirement for all internet based businesses. This would include strong default privacy settings and human rights by design requirements. There should be a requirement to comply with children's rights principles, such as demonstrated under the National Principles for Child Safe Organisations in the physical world. This would include a requirement to assess and report the impact on the rights of children at every stage of design, implementation and operation.[39]

43. Online safety measures should be developed in accordance with art 3 of the CRC, which requires that the best interests of the child be a primary consideration in all actions concerning them. This is one of the four guiding principles of the CRC.[40]

44. This requires consideration for 'all children's rights, including their right to seek, receive and impart information, to be protected from harm and to have their views given due weight'[41] in addition to ensuring transparency over the criteria applied to determine best interests.[42] Where rights are limited to protect children from online harms, limitations must be lawful, necessary and proportionate.

45. Children's safety should not be construed narrowly and should recognise the importance of children's autonomy and choice over their private lives. A best interests approach may require implementing clear boundaries to prevent practices that both infringe upon children's rights and are contrary to their best interests.

46. Digital platforms should be required to demonstrate that their services meet the best interests of the child principle.[43] This would include considerations of privacy, security of personal data, protection from harm, a voice to express their views, and the ability to seek, receive and convey information.[44] The Basic Online Safety Expectations for regulated service providers would benefit by placing the best interests of the child at the forefront of design and operation of services accessed by children.

Recommendation 8: The best interests of the child should be a primary consideration of all digital platforms.

47. Best interests considerations should not be based on assumptions about what is in the interests of children. Their views should be actively considered when considering changes to the OS Act and how they may impact them.[45] This would require broad consultations and input from children, young people, parents and schools. It is also important to include, for example, children and young people from diverse backgrounds, including those who are Aboriginal and Torres Strait Islander, culturally and linguistically diverse, living with disability, and from refugee backgrounds, to understand the full spectrum of experiences, views and opinions held by children and young people. These consultations will require child-specific methodologies.

48. The Commission stresses the need to engage with all experts that understand the lived experiences, risks and opportunities posed by the digital environment on children. As children are the experts of their own lives, they should be made a priority in consultations.

Recommendation 9: Children and young people should be consulted on changes to the *Online Safety Act 2021* (Cth) which may impact their experiences online.

5 Education

49. The same rights that people have offline must also be protected online.[46] Online safety literacy is essential to ensure human rights are protected and promoted.

50. Technology, and how people use it, is evolving at a rapid pace. New and emerging technologies pose a particular risk to human rights. The work of eSafety in producing Tech trends and challenges position papers plays a pivotal role in educating and raising awareness for people and policy makers across the country, as well as ensuring that eSafety is giving early consideration to emerging technologies and risks.

51. Increased support for the Tech trends and challenges work would better promote online safety at a time when new technologies are proliferating at an unprecedented rate. In particular there are several emerging technologies which will likely need to be considered in the near future, with neurotechnology being just one example.

Recommendation 10: The Australian Government increase support for proactive educative and policy initiatives such as the Tech trends and challenges initiative by the Office of the eSafety Commissioner.

52. Specific education around human rights and child rights relevant to digital environments should also be provided to parents and guardians, educators, and children to improve online safety literacy.

53. Parents, guardians, and educators should be equipped to support children to access the benefits of online environments so that children are not excluded from beneficial opportunities to engage online. It is also critical that parents, guardians, and educators are aware of potential risks and harms in online spaces, and available remedies and supports.

54. The Commission supports the work of eSafety to provide education on online safety and privacy to parents, guardians, educators, and children, including through schools.[47] The Commission encourages this work to also include training for parents, guardians and educators on how to respect children's evolving autonomy, capacity, and privacy online, as part of a child rights-framework.

55. All educational materials should be tailored to accommodate users at different age ranges, and with different levels of pre-existing technological literacy.

Recommendation 11: The Australian government should facilitate the ongoing provision of rights-based education initiatives tailored to parents, guardians, educators and children at different age ranges.

6 Penalties

56. Civil penalties within the OS Act have not kept pace with global regulatory regimes. Under the relevant legislation, civil penalties can be up to 500 penalty units ($156,500 for individuals or $782,500 for corporations as at 22 April 2024) for a variety of offences.[48]

57. Other Australian regimes regulating digital environments have significantly higher penalties, with serious breaches under the *Privacy Act 1988* (Cth) resulting in penalties of up to $50,000,000 for a body corporate.[49]

58. Ireland, the EU and UK all apply significantly higher penalties for noncompliance with online safety legislation, often based on a percentage of global revenue. For example, in Ireland platforms may incur penalties up to €20 million or 10% of annual turnover.[50]

59. The global platforms the OS Act seeks to regulate have accumulated significant wealth, with many large technology companies having a greater market cap than entire countries' GDP.[51] For example, recent reporting suggested that Meta's first quarter 2024 revenue would be (USD) $34.5–37 billion.[52]

60. Civil penalties are intended to serve as a deterrent against legislative noncompliance. Due to the significant earnings of platforms, current penalties under the OS Act are insufficient. A near one-million-dollar fine is inadequate when an organisation is earning billions in profit.

61. The OS Act must be updated to reflect global regulatory changes to penalty provisions and ensure that fines operate as an effective deterrent.

Recommendation 12: Civil penalties under the *Online Safety Act 2021* (Cth) be increased and articulated as a percentage of platform turnover.

6.1 Various offences

62. The current penalties under the OS Act are not proportionate to the relevant offence. As noted in the Issues Paper, the maximum penalty

applies equally to failures to take down child sexual exploitation material as it does failures to remove cyberbullying.

63. Further consideration should also be given to whether offending relates to a specific case or more systemic non-compliance. Civil penalties should reflect the gravity and systemic nature of offending. This is especially important if penalties are to be increased.

Recommendation 13: Civil penalties should be proportionate to both the offence and the offending behaviour.

6.2 Enforceability

64. Enforcing domestic penalties against international platform companies is a difficult task, exacerbated by many regulated platforms not having a local presence.

65. In its Final Report, the Select Committee on Foreign Interference through Social Media recommended new transparency reporting requirements that were enforceable through fines.[53] This required all large social media companies operating in Australia to have an Australian presence in order to ensure enforceability.[54] While this relates to foreign interference regulation, and not online safety, it does highlight the challenges of ensuring compliance in a global operating environment, and the need for global platforms to have a physical presence in Australia or some mechanism by which to assist with the enforcement penalties. Statutory duty of care

66. To date online safety has, in part, focused on take-down measures to ensure digital spaces are safeguarded. This approach emerged from broadcasting regulation on a case-by-case basis.[55] However there was only a small group of broadcasters in any jurisdiction, so managing content could be handled in this way. In today's digital age, where any individual can potentially produce enormous amounts of content, this approach is insufficient.

67. The imposition of a duty of care on digital platforms would address some deficiencies in the historical case-by-case approach. It moves away from 'whack-a-mole' content moderation by regulators, to focus on building

systems and digital environments which are safe by design.[56] The strengthening of risk assessment and transparency mechanisms will be essential in any proposed statutory duty of care placed upon platforms. This would place obligations on platforms to consider risk and mitigate harm in their technical systems and processes.

Recommendation 14: The Australian Government place a statutory duty of care upon digital platforms to safeguard end users.

7 Respecting human rights

68. The Issues Paper states that governments must consider how to uphold a range of 'fundamental' human rights. The use of the term 'fundamental' human rights may suggest a form of hierarchy (i.e. if there are fundamental rights, there must also be ancillary rights). However, all human rights are indivisible and afforded equal status - meaning there is no hierarchy. When considering human rights online, the Commission recommends consideration of which human rights will be most affected – as opposed to which are 'fundamental'.

69. While many rights may be affected in online spaces, the human right to freedom of expression requires specific consideration.[57] Consideration of freedom of expression online is especially important because digital platforms provide opportunities for realising the benefits of free speech.[58] This was highlighted by the United Nations (UN) Human Rights Council in its 2018 resolution calling on member states to protect access and dissemination of information online and condemning all undue restrictions of freedom of opinion and expression online that violate international law.[59]

70. While digital platforms can facilitate and promote free speech, they can also exacerbate harms. The 2018 UN Human Rights Council resolution also stressed the importance of combating advocacy of hatred on the Internet.[60] The same rights that people have offline must also be protected online. The right to free speech online is not absolute, and its exercise 'carries with it special duties and responsibilities'.[61] For example, where online posts promote or incite violence there is a clear need to censor that content, and this can be done without impermissibly restricting freedom

of speech. However, there may be legitimate discussion on controversial topics which reasonable minds may differ on – the removal of such content may be an impermissible restriction of free speech.

71. It is acknowledged that for freedom of speech to flourish online, the 'digital town square' in which discourse occurs should be a safe space for expression. If not, the voices of marginalised groups may be silenced out of fear in engaging in hostile online spaces. Creating online spaces where free expression can flourish has traditionally been important to protect minority interests, noting that 'anyone who has studied a skerrick of history knows that protecting free speech is about giving voice to the powerless against the majority and established interests'.[62]

72. The OS Act must carefully balance these competing considerations to ensure freedom of expression is protected, while also providing a safe space for democratic discourse.

Recommendation 15: The statutory review of the *Online Safety Act 2021* (Cth) directly considers the human rights impacts of proposed reform, including specifically the impact on freedom of expression.

8 Online hate

73. The Commission's National Anti-Racism Framework Scoping Report (2022) highlights the online environment as a space where racism, dehumanisation and cyberbullying occur, and misinformation and disinformation spread. Threats of online hate may also be aligned with extremist ideology and include incitement to violence.

74. In the Commission's consultations for the Scoping Report, participants broadly advised the Commission that current standards and regulatory mechanisms do not adequately protect users from online hate.[63]

75. Emphatic calls were raised regarding more accountability for regulators and social media platforms, due to the dehumanising and violence-inciting online content that often goes unregulated.

76. In the Commission's Scoping Report, hate crimes experts advised of the unique ways the online environment facilitates the spread of hate and racism.

77. Bad actors online often adapt their methods or wordings of harassment to circumvent moderation, and/or amplify their messages through algorithms. This may turn individual incidents into a public harm.

78. Additionally, online hate can be carried out in roundabout ways through racist curation of information or stories. In their research, Australian Muslim Advocacy Network notes that this can amount to 'an aggregate harm of dehumanising an outgroup to an ingroup audience' over time, rather than it being targeted against individuals.[64]

79. The Australian Muslim and Jewish communities are commonly targeted by online hate in the form of severe and disturbing threats.[65] There are concerns that the laws to address this behaviour are inadequate, and a number of law reform proposals are currently being considered.

8.1 Risks of the online environment in promoting extremism

80. In April 2024, the Commission provided a submission to the Senate Legal and Constitutional Affairs Reference Committee's Inquiry into right-wing extremist movements in Australia. It highlighted the threat of extremism, including right-wing extremism, in Australia and the role of the online environment in enabling it.

81. The Commission's Scoping Report notes that organisations involved in relevant research – such as the Australian Hate Crime Network and Australian Muslim Advocacy Network – recognise that extremist movements are often driven by the 'violent denial of diversity'.[66]

82. This violent denial of diversity proliferates online, threatens an inclusive society, and has potential to escalate into hate crimes and violence, harming diverse individuals and communities – particularly those that are negatively racialised.

83. The Scoping Report notes that hate crime impacts not only the victim but also the victim's community and 'does significant damage to personal security, social belonging, inclusion, participation, and cohesion'.[67]

8.2 Misinformation and disinformation

84. Hate crime experts consulted for the Scoping Report also noted that misinformation and disinformation are tools of extremist movements that also spread online.[68] The Commission acknowledges the impact of misinformation and disinformation in undermining the promotion and protection of human rights in Australia more broadly.

85. At the same time, there are examples around the world of information being opportunistically labelled as misinformation or disinformation to delegitimise alternative opinions and justify censorship. For example, the Center for International Media Assistance have examined what they describe as the global 'proliferation' of national laws designed to combat misinformation and disinformation in recent years. The Center expressed concern about the potential for these laws to be 'weaponised', resulting in a stifling of independent media and weakening of digital rights.[69]T

86. There is a clear need to combat misinformation and disinformation, however there is also a real risk of different perspectives and opinions being targeted when doing so. Robust safeguards for freedom of expression must form part of any measures taken to combat misinformation and disinformation in order to ensure that Australia's democratic values are not undermined. Striking the right balance between combatting misinformation and disinformation and protecting free expression is an ongoing challenge.

87. The Commission will shortly be commencing a project focusing on misinformation and disinformation as it relates to racism and anti-racism, as well as its intersections with climate change, civic participation, misogyny, the rights of LGBTQIA+ peoples, and other human rights issues.

88. This project will involve a scoping review and diagnostics seeking to understand the threat of misinformation and disinformation to human rights in Australia and the potential role of the Commission, as the national human rights institution, to support efforts to combat it. The Commission will then develop, pilot and evaluate a number of strategies to combat misinformation and disinformation in the immediate, intermediate and long term. It will be informed by scoping consultations, actor mapping and analysis of current trends.

Recommendation 16: The Australian Government address the legislation's limitations regarding cyber abuse and better protect individuals targeted by online hate, including racial hatred and its intersection with religious discrimination.

Recommendation 17: The Australian Government introduce provisions that protect communities targeted by online hate, including racial hatred and its intersection with religious discrimination.

Recommendation 18: Under the *Online Safety Act 2021* (Cth) Online Content Scheme, consider establishing industry codes that require:

- **adequate moderation and regulation mechanisms across platforms, particularly in relation to online hate**
- **action to address misinformation and disinformation**
- **adequate transparency and accountability mechanisms to ensure that online moderation and regulation designed to address online hate and misinformation and disinformation also provide appropriate protections for freedom of speech.**

9 Technology-facilitated abuse

89. With the rapidly evolving nature and accessibility of technology has come an increased risk of harm of perpetrators misusing it.

90. Technology-facilitated violence often manifests as a form of gendered violence and abuse, with perpetrators utilising mobile, online and other technologies to stalk, monitor, threaten, sexually harass and abuse victims.[70]

91. While all people can experience technology-facilitated abuse, some victim-survivors are more likely to experience it within family, domestic and sexual violence, and struggle to access support.[71] eSafety has previously found that:

- 99.3% of Australian family, domestic and sexual violence practitioners had clients who experienced technology-facilitated family and domestic violence
- 62.3% of Australian adults surveyed (18-54) had experienced technology-facilitated sexual violence
- 72% of Australians who used a dating app or website experienced sexual violence
- Perpetrators of technology-facilitated sexual violence are more likely to be men than women
- 9060 image-based abuse reports were handled by eSafety in 2022-2023, a 117% increase from the previous year.[72]

92. Research also demonstrated that Aboriginal and Torres Strait Islander women, sexuality and gender-diverse people, culturally and racially marginalised women, women with disability and women who live in rural areas are more likely to experience technology-facilitated violence.[73]

93. In particular, eSafety has reported on the experience of LGBTIQ+ teens and the fact that they are more likely than the national average to have experienced hurtful and hateful online interactions.[74] This, in part, is a result of LGBTIQ+ teens being online more frequently than non-LGBTIQ+ teens, due to the sense of safety and, sometimes, anonymity the online world provides them to connect, explore, seek support and express themselves.[75]

94. According to *The Economist*, some of the commonest forms of technology-facilitated violence include misinformation and defamation (67%), cyber harassment (66%), hate speech (65%), impersonation (63%), hacking and stalking (63%), 'astroturfing' (a coordinated effort to concurrently share damaging content across platforms, 58%), video and image-based abuse (sharing intimate photos or videos without consent, 57%), 'doxxing' (publishing private personal information, 55%), violent threats (52%), and unwanted images or sexually explicit content (43%).[76]

95. There is also a significant problem in the workplace, with 1 in 7 Australian adults surveyed engaging in workplace technology-facilitated sexual harassment.[77] According to ANROWS, sexist and gender discriminatory attitudes and the endorsement of sexual harassment myths are the two

most common predictors of self-reported workplace technology-facilitated sexual harassment.[78]

96. Given the rapid nature of the development of these technologies, the law and appropriate support systems are failing to keep up.[79] Support workers in family, domestic and sexual violence organisations often struggle to respond to technology-facilitated violence and protect the safety of victim-survivors, and this may partly be due to a lack of technical knowledge.[80]

9.1 Human Rights Concerns

97. Failure to protect against technology-facilitated violence against women is a breach of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). This was confirmed through General Recommendation 35, adopted by the CEDAW Committee in 2017, which noted that violence against women can take a number of forms and occur in a range of settings, 'from private to public, including technology-mediated settings'.[81]

98. Technology-facilitated gender-based violence has been identified and recognised as a global problem, with 58% of young women and girls globally having experienced online harassment on social media platforms.[82]

99. Technology-facilitated violence formed a key aspect of the 67th session of the Commission on the Status of Women (CSW67) in 2023. The priority theme of CSW67 was 'Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls'.

100. In the agreed conclusions to CSW67, technology-facilitated violence was defined as 'any act that is committed, assisted, aggravated or amplified by the use of information communication technologies or other digital tools which results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringements of rights and freedoms. These are forms of violence that are directed against women because they are women and/or that affect women disproportionately'.[83] States were further called upon to take action to prevent harm coming to women and girls in online spaces.

Recommendation 19: The development of regulatory frameworks, designed and implemented in accordance with the Office of the eSafety Commissioner's Safety by Design Framework, to ensure service provider responsibility, transparency and accountability. These safeguards must be retrofitted or designed into the development of technology to ensure the protection of women and girls from technology-facilitated violence.

Recommendation 20: Appropriate funding to women's safety services, to ensure they are equipped to provide support to people who experience technology-facilitated violence.

10 Image-based abuse and cyber-flashing

101. While generative artificial intelligence (AI) is revolutionising the way in which people work, access information and interact with content, it also raises concerns regarding the protection of human rights, with the safety of women and girls being of particular concern.

102. AI has allowed for the amplification of existing methods, and increased the potential for, avenues for technology-facilitated gender-based violence.[84]

103. In many cases, the law has failed to keep up with the rapid evolution of technology. We are particularly seeing this with the emergence of image-based abuse.

104. As defined by eSafety, image-based abuse is when a person 'shares, or threatens to share, an intimate image or video of someone without their consent' (the image can be real or fake).[85] It further notes that the intimate image or video can show, or appear to show:

- a person's genital area or anal area (whether bare or covered by underwear)
- a person's breasts (if the person identifies as female, transgender or intersex)

- private activity (for example getting undressed, using the toilet, showering, having a bath or engaging in sexual activity)
- a person without attire of religious or cultural significance that they would normally wear in public (such as a niqab or turban).[86]

105. Similarly, instances of cyber-flashing have also increased with the use and development of technology. Cyber-flashing is the sharing of unsolicited sexual images via social media, message or Bluetooth.[87]

106. In circumstances where these images are sent via Apple's 'AirDrop' feature, additional concerns are at play given the sender would need to be within approximately a 20-30m radius of the person receiving them.[88] As such, the victim may feel that their physical safety is also at risk.[89]

107. Regulation of various platforms, particularly in an online space where accountability is hard to monitor, is complex. Where regulation in this space does exist, particularly on social media platforms, the onus is frequently on the victim to block people, content or comments and report them to the platform. However, few tools exist that can identify patterns of harmful behaviour or block people en masse.

108. The introduction of the *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024* (Cth) into the Australian Parliament on, 5 June 2024, aims to address an existing gap in the law with respect to the extremely harmful and pervasive nature of image-based abuse.

109. The Bill creates a criminal offence targeting the creation and non-consensual sharing of sexually explicit material online, including material that has been created or altered using technology, such as AI. The offence of sharing the sexually explicit material carries a serious criminal penalty of up to 6 years imprisonment, and 7 years imprisonment for the aggravated offence of also creating the material that is shared without consent.

110. While this legislation is a step in towards ensuring that the law catches up with technology, the details of the legislation need to be carefully assessed to ensure there are no unintended consequences, and any law reform should be supported with practical education and training so that the law can be appropriately applied and enforced once introduced.

Recommendation 21: The provision of funding for age-appropriate education around consent, which includes consent in online spaces, for children and young people from a range of backgrounds and life experiences, including children and young people with disability and from LGBTIQ+, First Nations and culturally or racially marginalised backgrounds.

Recommendation 22: The implementation of legislation providing protection from technology-facilitated violence, which includes extensive consultation with experts to ensure there are no unintended consequences, and practical education and training so that the law can be appropriately applied and enforced once introduced.

Recommendation 23: Work with industry to develop regulatory frameworks (using a safety-by-design approach), education and awareness training, information guidelines for users and consumers of technology, as well as clear warnings of any breaches to user codes or terms, with clear reporting pathways and accountability for acts of technology-facilitated violence.

11 Emerging technologies

111. The Commission recently published its Protecting Cognition: Background Paper on Neurotechnology and Human Rights (Background Paper) which discusses the impact of neurotechnologies and human rights. Neurotechnologies can be defined as:

> … those devices and procedures used to access, monitor, investigate, assess, manipulate and/or emulate the structure and function of the neural systems of natural persons.[90] They are meant to either record signals from the brain and 'translate' them into technical control commands, or to manipulate brain activity by applying electrical or optical stimuli.[91]

112. It is likely that neurotechnologies will be increasingly developed and deployed in consumer settings.[92] They may also be integrated into online services such as games and social media – aspects of which may be covered by the OS Act.[93] As noted in the Background Paper:

> This is particularly where there is a risk of child sexual exploitation, violent terrorist acts and violent extremism, and other forms of abuse within eSafety's regulatory remit.[94]

113. As the OS Act and functions of eSafety are reviewed in anticipation of rapidly emerging technologies, greater consideration should be given to the future role that neurotechnologies will have in the everyday lives of people living in Australia. To assist in this work eSafety should conduct further research into this emerging technology.

Recommendation 24: The Office of the eSafety Commissioner should be encouraged to conduct research and publish a position statement on neurotechnologies as part of its Tech trends and challenges initiative.

12 Recommendations

114. The Commission makes the following recommendations.

Recommendation 1: The Office of the eSafety Commissioner consider the full spectrum of child rights, including children's right to privacy and protection, in considering its role and powers to address the posting of material promoting criminal activity.

Recommendation 2: The Office of the eSafety Commissioner's Age Verification Pilot be supported and appropriately resourced.

Recommendation 3: The Office of the eSafety Commissioner consider context and proportionality in the piloting and proposed use of age-verification techniques.

Recommendation 4: A Children's Online Privacy Code be introduced as a priority, including prior to the introduction of large-scale age verification measures.

Recommendation 5: The recommendations made by the Office of the eSafety Commissioner directed towards education and awareness raising – specifically Recommendations 5 & 6 in the Roadmap to age verification – should be progressed.

Recommendation 6: Facial recognition technologies are an inappropriate form of mandatory age verification process until facial recognition technology specific legislation is introduced.

Recommendation 7: The use of biometric technologies as a form of mandatory age verification should not occur without legal protections being introduced to address human rights risks.

Recommendation 8: The best interests of the child should be a primary consideration of all digital platforms.

Recommendation 9: Children and young people should be consulted on changes to the *Online Safety Act 2021* (Cth) which may impact their experiences online.

Recommendation 10: The Australian Government increase support for proactive educative and policy initiatives such as the Tech trends and challenges initiative by the Office of the eSafety Commissioner.

Recommendation 11: The Australian government should facilitate the ongoing provision of rights-based education initiatives tailored to parents, guardians, educators and children at different age ranges.

Recommendation 12: Civil penalties under the *Online Safety Act 2021* (Cth) be increased and articulated as a percentage of platform turnover.

Recommendation 13: Civil penalties should be proportionate to both the offence and the offending behaviour.

Recommendation 14: The Australian Government place a statutory duty of care upon digital platforms to safeguard end users.

Recommendation 15: The statutory review of the *Online Safety Act 2021* (Cth) directly considers the human rights impacts of proposed reform, including specifically the impact on freedom of expression.

Recommendation 16: The Australian Government address the legislation's limitations regarding cyber abuse and better protect individuals targeted by online hate, including racial hatred and its intersection with religious discrimination.

Recommendation 17: The Australian Government introduce provisions that protect communities targeted by online hate, including racial hatred and its intersection with religious discrimination..

Recommendation 18: Under the *Online Safety Act 2021* (Cth) Online Content Scheme, consider establishing industry codes that require:

- adequate moderation and regulation mechanisms across platforms, particularly in relation to online hate
- action to address misinformation and disinformation
- adequate transparency and accountability mechanisms to ensure that online moderation and regulation designed to address online hate and misinformation and disinformation also provide appropriate protections for freedom of speech.

Recommendation 19: The development of regulatory frameworks, designed and implemented in accordance with the Office of the eSafety Commissioner's Safety by Design Framework, to ensure service provider responsibility, transparency and accountability. These safeguards must be retrofitted or designed into the development of technology to ensure the protection of women and girls from technology-facilitated violence.

Recommendation 20: Appropriate funding to women's safety services, to ensure they are equipped to provide support to people who experience technology-facilitated violence.

Recommendation 21: The provision of funding for age-appropriate education around consent, which includes consent in online spaces, for children and young people from a range of backgrounds and life experiences, including children and young people with disability and from LGBTIQ+, First Nations and culturally or racially marginalised backgrounds.

Recommendation 22: The implementation of legislation providing protection from technology-facilitated violence, which includes extensive consultation with experts to ensure there are no unintended consequences, and practical education and training so that the law can be appropriately applied and enforced once introduced.

Recommendation 23: Work with industry to develop regulatory frameworks (using a safety-by-design approach), education and awareness training, information guidelines for users and consumers of technology, as well as clear warnings of any breaches to user codes or terms, with clear reporting pathways and accountability for acts of technology-facilitated violence.

Recommendation 24: The Office of the eSafety Commissioner should be encouraged to conduct research and publish a position statement on neurotechnologies as part of its Tech trends and challenges initiative.

Endnotes

[1] United Nations Committee on the Rights of the Child, *General Comment 24 on children's rights in the child justice system*, UN Doc CRC/C/GC/24 (18 September 2019) para 22.
[2] Faith Gordon, 'Children's Rights and Media Wrongs' in the Digital Age' (2020) 14 *Court of Conscience Issue* 77.
[3] Chris Cunneen, Sophie Russell, 'Social Media, Vigilantism and Indigenous People in Australia' in Biber, K. and Brown, M (ed) *The Oxford Encyclopedia of Crime, Media, and Popular Culture* (2017, Oxford University Press) 7, 15.
[4] Faith Gordon, 'Children's Rights and Media Wrongs' in the Digital Age' (2020) 14 *Court of Conscience Issue* 77.
[5] UN General Assembly, *United Nations Standard Minimum Rules for the Administration of Juvenile Justice ("The Beijing Rules"),* 40th sess, UN Doc A/RES/40/33 (29 November 1985), 208.
[6] Chris Cunneen, Sophie Russell, 'Social Media, Vigilantism and Indigenous People in Australia' in Biber, K. and Brown, M (ed) *The Oxford Encyclopedia of Crime, Media, and Popular Culture* (2017, Oxford University Press) 7, 15.
[7] Chris Cunneen, Sophie Russell, 'Social Media, Vigilantism and Indigenous People in Australia' in Biber, K. and Brown, M (ed) *The Oxford Encyclopedia of Crime, Media, and Popular Culture* (2017, Oxford University Press) 7, 15.
[8] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 7.
[9] Joseph A. Cannataci, '*Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy*', 46th sess, UN Doc. A/HRC/46/37 (2021) 15 [96].
[10] Joseph A. Cannataci, '*Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy*', 46th sess, UN Doc. A/HRC/46/37 (2021) 21-22 [127].
[11] Joseph A. Cannataci, '*Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, on Artificial Intelligence and Privacy, and Children's Privacy*', 46th sess, UN Doc. A/HRC/46/37 (2021) 21-22 [127].
[12] 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.
[13] Our Watch, *Pornography, Young People and Preventing Violence against Women* (Background Paper, 2020) 14.
[14] Our Watch, *Pornography, Young People and Preventing Violence against Women* (Background Paper, 2020) 14.
[15] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 7.
[16] eSafety Commissioner, *Mind the Gap: Parental Awareness of Children's Exposure to Risks Online* (Report, February 2022) 47.
[17] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 7.
[18] eSafety Commissioner, *Accidental, Unsolicited and in your Face. Young People's Encounters with Online Pornography: A Matter of Platform Responsibility, Education and Choice* (Report, September 2023) 5.
[19] eSafety Commissioner, *Accidental, Unsolicited and in your Face. Young People's Encounters with Online Pornography: A Matter of Platform Responsibility, Education and Choice* (Report, September 2023) 5.

[20] See generally Diana Warren and Neha Swami, *LSAC Annual Statistical Report* (Australian Institute of Family Studies, Report, 2018).
[21] Jordan Baker, 'Kicked down the road': Australians to wait for Porn Passport' *Sydney Morning Herald* (online, 30 August 2023) <https://www.smh.com.au/politics/federal/kicked-down-the-road-australians-to-wait-for-porn-passport-20230830-p5e0nk.html>.
[22] Digital Rights Watch, '*Restricted Access Systems*' (webpage) <https://digitalrightswatch.org.au/2021/09/21/submission-restricted-access-system/>.
[23] Information Commissioner's Office, *Age appropriate design: a code of practice for online services*, (Report, September 2020) 34.
[24] Attorney-General's Department, Privacy Act Review (Report, 2022) 54.
[25] Information Commissioner's Office, *Age appropriate design: a code of practice for online services*, (Report, September 2020) 24.
[26] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 14 & 64.
[27] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 58.
[28] South Australian Commissioner for Children and Young People, *Sex education in South Australia: What Young People need to Know for Sexual Health and Safety*, (Report, 2021) 18.
[29] Researchers have noted that the abusive scripts and unequal power dynamics found in mainstream, heterosexual pornography, can also shape the acts and depictions in LGBTQ+ pornography. Aggression and stereotyped gender roles and constructions of masculinity and femininity also feature in same-sex pornography videos. See Kimberly Seida & Eran Shor, 'Aggression and Pleasure in Opposite-Sex and Same-Sex Mainstream Online Pornography: A Comparative Content Analysis of Dyadic Scenes' (2021) *The Journal of Sex Research* 58(3).
[30] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 74.
[31] Australian Human Rights Commission ('AHRC'), '*Human Rights and Technology Final Report 2021*' (Final Report, 2021) 120.
[32] AHRC, '*Human Rights and Technology Final Report 2021*' (Final Report, 2021) recs 2, 9 & 15.
[33] See generally Human Technology Institute, '*Facial Recognition Technology Towards a Model Law*' (University of Technology Sydney, Report, September 2022).
[34] AHRC, '*Human Rights and Technology Final Report 2021*' (Final Report, 2021) rec 20.
[35] See generally Human Technology Institute, '*Facial Recognition Technology Towards a Model Law*' (University of Technology Sydney, Report, September 2022).
[36] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 19.
[37] eSafety Commissioner, *Roadmap for Age Verification* (Roadmap, March 2023) 18.
[38] National Children's Commissioner, Submission No. 64 to House of Representatives Select Committee on '*Social Media and Online Safety*' (Submission, 24 January 2022) 4.
[39] Anne Hollands, National Children's Commissioner, Australian Human Rights Commission (AHRC), Committee Hansard, 2 March 2022, 1-2.
[40] Committee on the Rights of the Child, '*General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*', UN Doc. CRC/C/GC/25 (02 March 2021) 12-13.
[41] Committee on the Rights of the Child, '*General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*', UN Doc. CRC/C/GC/25 (02 March 2021) 13.
[42] Committee on the Rights of the Child, '*General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*', UN Doc. CRC/C/GC/25 (02 March 2021) 13.
[43] Anne Hollands, National Children's Commissioner, AHRC, Committee Hansard, 2 March 2022, 3.

[44] National Children's Commissioner, Submission No. 64 to House of Representatives Select Committee on '*Social Media and Online Safety*' (Submission, 24 January 2022) 4.
[45] Committee on the Rights of the Child, '*General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*', UN Doc. CRC/C/GC/25 (02 March 2021) 16-18.
[46] United Nations Human Rights Council, '*The Promotion, Protection and Enjoyment of Human Rights on the Internet*', res 20/8, 20th sess, UN Doc. A/HRC/RES/20/8 (16 July 2021) 2 [1].
[47] See eSafety, '*Educators'* (Webpage) <https://www.esafety.gov.au/educators>.
[48] See e.g. *Online Safety Act 2021* (Cth) ss 50, 53, 57, 60 & 67.
[49] *Privacy Act 1988* (Cth) s 13G.
[50] See e.g. *Online Safety and Media Regulation Act 2022*.
[51] Visual Capitalist, '*The World's Tech Giants, Compared to the Size of Economies*' (webpage) <https://www.visualcapitalist.com/the-tech-giants-worth-compared-economies-countries/>.
[52] Meta, '*Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend*' (Press Release, 01 February 2024) <https://investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx>.
[53] Select Committee on Foreign Interference through Social Media, '*Final Report*' (Report, August 2023) rec 1, xv [8.43]-[8.44].
[54] Select Committee on Foreign Interference through Social Media, '*Final Report*' (Report, August 2023) rec 1, xv [8.43]-[8.44].
[55] Reset.Tech Australia, '*A Duty of Care in Australia's Online Safety Act*' (Briefing, 17 April 2024) 7.
[56] Reset.Tech Australia, '*A Duty of Care in Australia's Online Safety Act*' (Briefing, 17 April 2024) 7.
[57] *International Covenant on Civil and Political Rights,* arts 19-20; See also *Convention on the Elimination of All Forms of Racial Discrimination,* arts 4-5; Convention on the Rights of the Child, arts 12-13; *Convention on the Rights of Persons with Disabilities,* art 21.
[58] Adrienne Stone, et al., *The Oxford Handbook of Freedom of Speech* (Oxford Academic, 2021) 351.
[5959] United Nations Human Rights Council, '*The Promotion, Protection and Enjoyment of Human Rights on the Internet*, 38th sess, UN Doc. A/HRC/38/L.10/Rev.1 (7 April 2018).
[60] United Nations Human Rights Council, '*The Promotion, Protection and Enjoyment of Human Rights on the Internet*, 38th sess, UN Doc. A/HRC/38/L.10/Rev.1 (7 April 2018).
[61] *International Covenant on Civil and Political Rights,* art 19(3).
[62] Tim Wilson, 'Insidious Threats to Free Speech', *The Weekend Australian,* 5 April 2014, 17.
[63] Australian Human Rights Commission, *National Anti Racism Framework Scoping Report* (December 2022) 130
[64] Australian Muslim Advocacy Network, *Submission No 3 to the Select Committee on Social Media and Online Safety, Parliament of Australia, Inquiry into Social Media and Online Safety* (21 December 2021) 8; See also Australian Muslim Advocacy Network, *Submission No 52 to the Legal Affairs and Safety Committee, Queensland Legislative Assembly, Inquiry into Serious Vilification and Hate Crimes* (12 June 2021) 8.
[65] See generally Andre Oboler, *Measuring the Hate: The Sate of Antisemitism in Social Media* (Report, 2016); Andre Oboler, *Anti-Muslim Hate Interim Report* (Interim Report, 2015).
[66] The violent denial of diversity' is a definition first used by the Khalifer Ihler Global Institute that aims to capture how extremist violence is often driven by a belief that 'peaceful coexistence with someone different from them is impossible, and that violently enforcing this either through forced submission or through eradication of diversity is the solution'. See Australian

Muslim Advocacy Network*, Submission to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Inquiry into and report on matters relating to extremist movements and radicalism in Australia* (12 February 2021) 17– 8.

[67] Australian Muslim Advocacy Network, *Submission No 52 to the Legal Affairs and Safety Committee, Queensland Legislative Assembly, Inquiry into Serious Vilification and Hate Crimes* (12 June 2021) 19.

[68] Australian Human Rights Commission, *National Anti-Racism Framework Scoping Report* (December 2022) 130.

[69] Sasha Schroeder, Fighting Fake News: How Mis- and Disinformation Legislation is Weaponized Against Journalists (Center for International Media Assistance, 10 August 2023. <https://www.cima.ned.org/blog/fighting-fake-news-how-mis-and-disinformation-legislation-is-weaponized-against-journalists/>.

[70] The Women's Services Network, *Technology and Violence against Women* (webpage) <https://wesnet.org.au/wp-content/uploads/sites/3/2023/02/Technology-and-violence-against-women-Policy-position-statement.pdf>.

[71] eSafety Commissioner, *Literature scan of tech-based family, domestic and sexual violence* (Literature Scan, October 2023).

[72] eSafety Commissioner, *Literature scan of tech-based family, domestic and sexual violence* (Literature Scan, October 2023).

[73] eSafety Commissioner, *Literature scan of tech-based family, domestic and sexual violence* (Literature Scan, October 2023).

[74] eSafety Commissioner, *Tipping the balance: LGBTIQ+ teens' experiences negotiating connection, self-expression and harm online* (Report, June 2024).

[75] eSafety Commissioner, *Tipping the balance: LGBTIQ+ teens' experiences negotiating connection, self-expression and harm online* (Report, June 2024).

[76] The Economist, *Measuring the prevalence of online violence against women* (webpage) <https://onlineviolencewomen.eiu.com/>.

[77] ANROWS, *Workplace technology-facilitated sexual harassment: Perpetration, responses and prevention*, (Research Report, No. 3, April 2024).

[78] ANROWS, *Workplace technology-facilitated sexual harassment: Perpetration, responses and prevention*, (Research Report, No. 3, April 2024).

[79] eSafety Commissioner, *Literature scan of tech-based family, domestic and sexual violence* (Literature Scan, October 2023).

[80] eSafety Commissioner, *Literature scan of tech-based family, domestic and sexual violence* (Literature Scan, October 2023).

[81] UN Committee on the Elimination of Discrimination Against Women, CEDAW General Recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, CEDAW/C/GC/35, 27 July 2017.

[82] Rumman Chowdhury & Dhanya Lakshmi, *"Your opinion doesn't matter, anyway": exposing technology-facilitated gender-based violence in an era of generative AI* (Report, UNESCO, 2023).

[82] UN Economic and Social Council, Commission on the Status of Women sixty-seventh session, E/CN.6/2023/L.3.

[83] UN Economic and Social Council, Commission on the Status of Women sixty-seventh session, E/CN.6/2023/L.3.

[84] Rumman Chowdhury & Dhanya Lakshmi, *"Your opinion doesn't matter, anyway": exposing technology-facilitated gender-based violence in an era of generative AI* (Report, UNESCO, 2023).

[85] eSafety Commissioner, *What you can report to eSafety* (webpage) <https://www.esafety.gov.au/report/what-you-can-report-to-esafety?gad_source=1&gclid=EAIaIQobChMI3_y-rufDhgMVAiCDAx1pEiO6EAMYASAAEgLBE_D_BwE#adult-cyber-abuse>.
[86] eSafety Commissioner, *What you can report to eSafety* (webpage) <https://www.esafety.gov.au/report/what-you-can-report-to-esafety?gad_source=1&gclid=EAIaIQobChMI3_y-rufDhgMVAiCDAx1pEiO6EAMYASAAEgLBE_D_BwE#adult-cyber-abuse>.
[87] eSafety Commissioner, *Unwanted or unsafe contact*, < https://www.esafety.gov.au/key-topics/staying-safe/unwanted-contact#:~:text=This%20is%20when%20you%20receive,is%20sometimes%20called%20%27cyberflashing%27.>.
[88] Monash University, *Cyberflashing – old-style sexual harassment for the digital age*, 2019 <https://lens.monash.edu/@politics-society/2019/09/06/1376441/cyberflashing-the-latest-form-of-digital-sexual-harassment>.
[89] McGlynn, C., & Johnson, K. (2021), *Criminalising Cyberflashing: Options for Law Reform,* The Journal of Criminal Law, 85(3), 171-188.
[90] Organisation for Economic Co-operation and Development ('OECD'), '*Recommendation Responsible Innovation in Neurotechnology*' (OECD Legal Instrument, 2019); OECD, '*Neurotechnology and Society: Strengthening Responsible Innovation in Brain Science*' (policy papers, November 2017) 49.
[91] UNESCO, '*Report of the International Bioethics Committee of UNESCO (IBC) on the Ethical Issues of Neurotechnology*' (Report, 2021) 5.
[92] Australian Human Rights Commission, '*Protecting Cognition: Background Paper on Neurotechnology and Human Rights*' (Background Paper, March 2024) 29-31.
[93] Australian Human Rights Commission, '*Protecting Cognition: Background Paper on Neurotechnology and Human Rights*' (Background Paper, March 2024) 34.
[94] Australian Human Rights Commission, '*Protecting Cognition: Background Paper on Neurotechnology and Human Rights*' (Background Paper, March 2024) 34.