DIGITAL
RIGHTS
WATCH

Submission to the Senate Standing Committees on Environment and Communications

regarding the

Internet Search Engine Services Online Safety Code

September 2025

Who we are

Digital Rights Watch is a charity founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness, and freedom. Digital Rights Watch educates, campaigns, and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website: www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

Tom Sulston | Head of Policy | tom@digitalrightswatch.org.au

Elizabeth O'Shea | Chair | lizzie@digitalrightswatch.org.au

Lucinda Thorpe | Privacy Campaigner | lucinda@digitalrightswatch.org.au

Contents

General comments and recommendations

We thank the committee for the opportunity to make a submission on this important legislation and direct their attention to our previous work in this area, including but not limited to:

- 2025 Submission to the OAIC on the Children's Online Privacy Code[1]
- 2024 Submission to the Environment and Communications Legislation Committee on Online Safety Amendment (Social Media Minimum Age) Bill[2]
- 2024 Submission to the eSafety Commissioner on Draft Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) under the Online Safety Act 2021[3]
- 2024 Submission to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts regarding the statutory review of the Online Safety Act 2021[4]
- 2022 Submission to the Select Committee on Social Media and Online Safety regarding their Inquiry into Online Safety and Social Media[5]

We note from the 2024 passage of the Online Safety Amendment (Social Media Minimum Age) Bill that the submissions from numerous expert institutions given to the committee were overwhelmingly in favour of rejecting the bill. Nothing in the 10 months that have since passed has given us cause to reconsider.

A simple ban of young people from social media will harm them. Young people, especially those in a minority group or remote areas of Australia, depend on the internet and social media to reach "their people". When we limit their ability to do so, there is no replacement. They will simply be cut-off from key parts of society. Instead of an outright ban, we should focus our efforts on better regulation of social media algorithms and the targeting of

[1] https://digitalrightswatch.org.au/2025/08/08/submission-to-the-oaic-regarding-the-childrens-online-privacy-code/

[2] https://digitalrightswatch.org.au/2024/11/22/submission-online-safety-amendment-social-media-minimum-age-bill-2024/

[3] https://digitalrightswatch.org.au/2024/11/22/submission-phase-2-industry-codes/

[4] https://digitalrightswatch.org.au/2024/06/25/submission-review-online-safety-act/

[5] https://digitalrightswatch.org.au/2022/01/13/submission-inquiry-into-social-media-and-online-safety/

content to drive advertising revenue, which would make children safer without restricting their ability to participate in society.

The Internet Search Engine Services Safety Code and Social Media Minimum Age bans remain a set of regulations that are not merely ineffective in reducing online harms, but will actually *increase* the level of online harms that face child and adult Australians alike.

Better regulation of Internet Search Engines and Social Media companies is definitely required but the current safety codes under consideration are not adequate, as we demonstrate in this submission.

To that end, we call on the committee to reject in their entirety the online safety codes for both Internet Search Engines and Social Media Minimum Age, and delay implementation of the codes until meaningful consultation with expert organisations in the field can inform a better policy direction.

1: Privacy and Data Protection Implications of Age Verification

The introduction of age verification for online content raises profound concerns about privacy, data protection, and proportionality. Invasion of privacy is inherent in any system that requires individuals to prove their age before accessing certain material. Such invasions may be permissible if they are demonstrably necessary, proportionate, and subject to clear limitations. However, in the present context, where the policy is aimed at restricting young people's access to online platforms and adult content, the evidence does not support these justifications.

There is no compelling proof that age verification measurably reduces the consumption of pornography by young people. Instead, what is clear is that these systems create significant risks to individual privacy, increase the likelihood of data exploitation, and may inadvertently harm the very groups they claim to protect.

The tools available on the market are of poor quality and often unreliable. While regulators have identified multiple methods for verification, each comes with critical shortcomings that either compromise privacy, allow circumvention, or both.

With reference to the methods of age verification described in 5.1(v) Compliance Measures:[6]

A: Matching of photo identification

Matching of photo identification is the usual manner in which Australians identify themselves in the physical world. However, when required online, there are a variety of issues with this approach. Most obviously, the ability of children to procure photo ID, perhaps by borrowing that of a parent or older sibling. There are a number of channels through which a person may purchase a fake ID, either Australian or foreign.

But it's not just ineffective, there are also privacy risks and these will be felt most keenly by those people who are not trying to bypass the system - those

[6] Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material)

entering their genuine ID. Firstly, the individual's identity will be shared and stored with a large internet platform - one of the companies who regularly invade our privacy in order to sell targeted advertisements at us.

The pervasive collection of Australians' identity papers as they navigate the internet, either through search or social media, will set an expectation that our IDs are safe to share on the Internet. We believe that this will lead to a proliferation of identity theft and fraud as unscrupulous criminals set up honeypots to harvest Australians' identities.

B: Facial recognition and age estimation

Biometric systems are notoriously unreliable, especially for people of colour, women, and young people whose physical development varies significantly.[7][8]

Research has found that facial recognition technology becomes increasingly inaccurate as children age, reflecting the fact that children grow and develop at different rates.[9] This was reaffirmed by the recent Age Verification Trial which found facial recognition errors are inevitable, especially for people close to the age threshold (e.g. 14-17), furthermore such inaccuracies are compounded by the subject being a person of colour or a woman.[10] Of the ages targeted by the ban, older teens are the demographic most likely to access pornand yet the demographic least likely to be deterred by such age-gating measures.[11]

The use of facial recognition technology introduces large-scale biometric data collection, with heightened risks of breaches and misuse. Australia's privacy

[7] Evershed, Nick, and Josh Nicholas. 2025. "Social Media Ban Trial Data Reveals Racial Bias in Age-Checking Software: Just How Inaccurate Is It?" *The Guardian*, September 19, 2025. https://www.theguardian.com/news/2025/sep/19/how-accurate-are-age-checks-for-australias-under-16s-social-media-ban-what-trial-data-reveals.

[8] Kayee Hanaoka, Mei Ngan, Joyce Yang, George W. Quinn, Austin Hom, and Patrick Grother, *Face Analysis Technology Evaluation: Age Estimation and Verification*, NIST Internal Report 8525 (Gaithersburg, MD: National Institute of Standards and Technology, 2024), page 36 https://doi.org/10.6028/NIST.IR.8525.

[9] Ibid.

[10] *Age Assurance Technology Trial: Part D—Age Estimation*, "Analysis of Acceptability Characteristics," findings 69-76, Age Check Certification Scheme (August 2025), https://ageassurance.com.au/wp-content/uploads/2025/08/AATT_Part_D_DIGITAL.pdf.

[11] Maree Crabbe, Michael Flood, and Kelsey Adams, "Pornography Exposure and Access among Young Australians: A Cross-Sectional Study," *Australian and New Zealand Journal of Public Health* (2024), Results section, https://doi.org/10.1016/j.anzjph.2024.100135.

laws are not strong enough to accommodate the mass uptake of such sensitive information. The restricted sites such as porn sites will be handling sensitive biometric data without the guarantee of guardrails as to the deletion, use, retention or protection of such data. Australian sites will only have to apply to the Australian Privacy Principles if they generate over 3 million AUD in revenue in a year.[12] Furthermore, If the data is stored overseas governments may be able to access incredibly sensitive data regarding Australians.[13] Such intimate details of Australians can enable foreign governments to generate detailed profiles of Australian citizens undermining Australia's national security.

Unlike a password or a security token, once biometric data is compromised, it cannot be revoked or reissued. Underscoring the importance of strict data security protocols.

C: Credit card checks

Credit card checks assume that everyone who has a credit card is over the age of 18 and everyone over the age of 18 has a credit card. Credit cards are increasingly unpopular with young adults who prefer debit cards, creating a barrier for young adults to access the internet.[14] Furthermore, many individuals over the age of 18 cannot access credit cards.[15][16]

[12] Office of the Australian Information Commissioner, "Small Business," OAIC, accessed [date you accessed it], https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/small-business.

[13] CIS Cyber Threat Intelligence Team, *"The Chinese Communist Party (CCP): A Quest for Data Control,"* Center for Internet Security, August 14, 2024, https://www.cisecurity.org/insights/blog/the-chinese-communist-party-ccp-a-quest-for-data-control.

[14] Afterpay, **"**Young Australians Moving Away from Credit Cards: New Survey," *Afterpay Access* (Australia), accessed 2025, https://www.afterpay.com/en-AU/business/access/news/gen-z-credit-card-ick-report.

[15] Kenji Sato and Steve Austin, "Credit Ratings and 'Well-Intended' Banking Reforms Mean Older Australians Can Be Easily Denied Credit Cards," *ABC News* (Australia), April 17, 2024, https://www.abc.net.au/news/2024-04-17/why-seniors-are-being-refused-credit-cards/103728528.

[16] Centre for Social Impact, *Measuring Financial Exclusion in Australia* (National Australia Bank, April 2014), 9, https://www.nab.com.au/content/dam/nabrwd/documents/reports/financial/2014-measuring-financial-exclusion-in-australia.pdf.

Credit cards can easily be borrowed or stolen, making them a poor proxy for proving age. If credit card checks become commonplace, it will be easier for scammers to make fraudulent requests for credit card information creating new opportunities for scams, fraud, and exploitation.

D: Digital ID systems

When digital ID was first proposed, assurances were given that strong safeguards, including a “double-blind” system, would prevent unnecessary data collection.[17] These assurances are now being rolled back.[18]

Forcing citizens to hand over government-issued identification in order to access lawful online content is grossly disproportionate. It represents a step toward a dystopian model of identity-linked internet access, incompatible with democratic freedoms.

E: Parental vouching systems

There is no reliable way to verify that the person providing “parental consent” is, in fact, a legitimate guardian. Furthermore, the system assumes standard familial relations and does not account for complicated family dynamics.[19]

Requiring parental permission could deter young people from seeking access to vital support services, particularly those related to sexual health and LGBTQ+ identity.[20] For many young people, parental involvement in these matters is unsafe or impossible.

[17] Justin Hendry, “Govpass: The DTA’s Answer to Australia’s Digital ID Problem,” *iTnews*, March 4, 2020, https://www.itnews.com.au/news/govpass-the-dtas-answer-to-australias-digital-id-problem-538856.

[18] *Departmental Responses to the Maddocks Privacy Impact Assessment Recommendations*, Recommendation 3, “Transparency about the Operation of the Identity Exchange,” Department of Finance (Australia), November 2024, https://www.digitalidsystem.gov.au/sites/default/files/2024-11/departmental_responses_to_the_maddocks_privacy_impact_assessment_recommendations_nov2024_0.pdf.

[19] *Age Assurance Technology Trial: Part H – Parental Consent*, “Inclusivity and Guardianship Complexity in Parental Consent Mechanisms,” (Stockport, United Kingdom: Age Check Certification Scheme, August 2025), 75, https://ageassurance.com.au/wp-content/uploads/2025/08/AATT_Part_H_DIGITAL.pdf.

[20] Elizabeth Murray, Nina Thomas, and K.E. Rogstad, “Confidentiality Is Essential if Young People Are to Access Sexual Health Services,” *International Journal of STD & AIDS* 17, no. 8 (August 2006): 525-529, https://doi.org/10.1258/095646206778145686. Wikidata

It is also telling that a parent is not, under the code, able to consent to their child being allowed to access systems that the Code has determined must be age-gated away from them. In this way, the Code disempowers parents from being able to act in the best interest of their child.

F: AI-driven profiling

Some proposals rely on companies inferring a user's age from behavioural data.[21][22] This approach reinforces the data-extractive business models of online platforms, incentivising the collection of ever more granular personal data. AI-driven profiling requires the entity to already have this data stored in its database. This provides entities with a legally-grounded excuse to surveil users and collect granular personal data.

Such systems are error-prone and context-blind. For example:

- An adult who frequently consumes child-oriented content (e.g., animated films) might be misclassified as a child.
- A child accessing adult content might be classified as an adult, defeating the intended purpose.
- A child uses their parents Youtube account, resulting in a varied user watch history

These inaccuracies could lead to arbitrary access restrictions while legitimising harmful forms of surveillance capitalism.

With the development of the Children's Online Privacy Code at OAIC, children's privacy needs to be protected from intrusive business models, not used as a tool to exclude them from the Internet.

[21] Bucci, Nino, and Nick Visser. 2025. "Australia News Live: Sydney Airport, Social Media Ban, Anthony Albanese, Chris Bowen, Climate Crisis, Carbon Emissions, PNG Treaty, NTWnFB." *The Guardian (Australia)*, September 16, 2025. https://www.theguardian.com/australia-news/live/2025/sep/16/australia-news-live-sydney-airport-social-media-ban-anthony-albanese-chris-bowen-climate-crisis-carbon-emissions-png-treaty-ntwnfb

[22] Age Assurance Technology Trial. 2025. *Part D: Age Estimation*. Age Assurance Technology Trial Final Report. Australian Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. https://ageassurance.com.au/publications/report-d/

2: The expansion of corporate data collection and user profiling capabilities enabled by code compliance requirements;

The requirement to age-gate Australian users will provide some of the world's largest privacy-invading companies with direct access to yet more private data about Australians - whether that's captured with ID documents or inferred with one of the other age-assurance methods.[23]

This constitutes a disproportionate privacy loss for all users, not just the children that the ban seeks to exclude. The Online Safety Codes should instead focus on closing the gaps that internet companies used to profile and monetise Australian internet users, rather than increase the data footprint that these companies enjoy.

By embedding this data-extractive model via age-gating in regulation, the Code makes it even more difficult for Australia to pass much-needed legislation to restrict companies from exploiting Australians' private information to extract huge profits.

For this reason, age-gating should be paused until at least the current round of Privacy Act amendments have been passed.

[23] Privacy Concerns with Facebook," *Wikipedia, The Free Encyclopedia*, last modified September 14, 2025, accessed September 22, 2025, https://en.wikipedia.org/wiki/Privacy_concerns_with_Facebook.

3: The technical implementation and efficacy of age verification and content filtering mechanisms;

Circumvention through technology

The most fundamental flaw of age verification systems is their ease of circumvention. As the restrictions only apply to users in Australia, a teenager can bypass restrictions in minutes by using a Virtual Private Network (VPN) and circumvent the restrictions entirely. This undermines the entire premise of the policy and demonstrates that the invasion of privacy it entails is neither necessary nor effective.

The eSafety Commissioner has issued guidelines requiring platforms to age-gate VPN users.[24] This is impractical and unlikely to succeed for the following reasons:

- Internet Platforms already struggle to identify and restrict VPN users for advertising or licensing purposes which directly affect their bottom line.
- Platforms will struggle to tell if a successfully-identified VPN user originates from Australia, and not a 3rd country which may have less censorious access requirements.
- As John Gilmore famously said back in the 1990s *"The internet treats censorship as damage and routes around it."*[25] It is the nature of the internet that alternative routes to information spring up when existing ones are closed. Young people are more internet-savvy than oppressive regimes trying to censor the Internet and already find ways to access forbidden content.

As with much of the Code, the need for young people to circumvent the age-gates will make them less safe. Many "free" VPNs contain

[24] Kolivos, Eugenia; Isabella Bicego; Joseph Singer. "Under-16 Social Media Ban: eSafety Commissioner's Regulatory Guidelines." *Corrs Chambers Westgarth*, September 18, 2025. Accessed September 22, 2025. https://www.corrs.com.au/insights/under-16-social-media-ban-esafety-commissioners-regulatory-guidelines

[25] "The Internet Treats Censorship as Damage and Routes around It," Quote Investigator, July 12, 2021, accessed September 22, 2025, https://quoteinvestigator.com/2021/07/12/censor/.

privacy-invading surveillance in order to turn a profit.[26] Young people's data, and their browsing habits - especially those for the sort of sites that will be age-gated - will be collected by offshore companies who have no obligation to treat that private data in accordance with Australian law.

Circumvention through system failure

Every automated system has a margin of error. These systems have very poor margins of error, especially around the key ages of 16 and 18.[27]

The nature of a "line-in-the-sand" age gate exacerbates this - it's extremely hard for a system to differentiate between the same person at the age of 15-and-11 months and 16-and-one-day.

While that may appear to be a small issue, it is actually a large one. The mathematics of large numbers are at play as there are 27 million Australians who will need to prove their age.[28] Were age-verification systems to achieve 99% accuracy, hundreds of thousands of Australians would still be either denied access due to false positives or let in due to false negatives. Internet companies are not equipped to deal with the level of helpdesk calls, so users will simply migrate themselves to other internet systems - most likely those that are not using age-gating and likely to have worse safety protocols.

The real-world accuracy of age-assurance tools will be even worse than the testbed as the systems will face deliberate attempts to spoof them, either in-browser or simply by holding up a photo of an older person. Apps to artificially age a person's photo already exist, and we can imagine teenagers giving them a good workout to break age-assurance systems.[29]

Low confidence in the age assurance trial

We note that internet expert and Chair of Electronic Frontiers Australia John Pane left the Age Assurance Technology Trial's Stakeholder Advisory Board over the rose-tinted nature of its interim report.[30] In his words:

[26] https://www.koi.security/blog/spyvpn-the-vpn-that-secretly-captures-your-screen

[27] Kayee Hanaoka, Mei Ngan, Joyce Yang, George W. Quinn, Austin Hom, and Patrick Grother, *Face Analysis Technology Evaluation: Age Estimation and Verification*, NIST Internal Report 8525 (Gaithersburg, MD: National Institute of Standards and Technology, 2024), page 36 https://doi.org/10.6028/NIST.IR.8525.

[28] https://www.geeksforgeeks.org/maths/law-of-large-numbers/

[29] https://www.crikey.com.au/2024/06/14/selfie-ai-age-verification-tool-filter-trick/

[30] Sadler, Denham. 2025. "'Big, red F': Age Assurance Advisor Hits Out at Final Report." *Information Age*, September 3, 2025.

“It is bad policy, and a gap-ridden technological solution that is easily circumvented by technical means or third-party collusion.”[31]

Lack of research-backed evidence for an age gate

While qualitative research suggests age verification acts as a partial barrier towards accidental viewing of pornography,[32] there is no clear evidence that age verification affects young people’s propensity to view porn.[33]

Furthermore, there is no compelling evidence that restricting access to pornography alone can effectively change misogynistic attitudes or behaviours towards women. Evidence suggests that challenging misogynistic attitudes and behaviours requires long-term programs that address gender inequality, gendered stereotypes and attitudes towards women, rather than restricting access to porn.[34][35] Despite the social media ban and age-gating for internet search, young people will still be able to access the materials generated by online misogynist and hateful "influencers". It will likely be pushed to them via the algorithm, even when they don’t have an account. [36]

https://ia.acs.org.au/article/2025/-big--red-f---age-assurance-advisor-hits-out-at-final-report.html.

[31] Denham Sadler, “‘Big, Red F’: Age Assurance Advisor Hits Out at Final Report,” *Information Age*, ACS, September 3, 2025, accessed September 22, 2025, https://ia.acs.org.au/article/2025/-big--red-f---age-assurance-advisor-hits-out-at-final-report.html.

[32] *Young People, Pornography & Age-Verification* (London: British Board of Film Classification / Revealing Reality, January 2020), 54–55, https://revealingreality.co.uk/wp-content/uploads/2021/07/BBFC-Young-people-and-pornography-Final-report-2401.pdf.

[33] Nair, Abhilash. 2018. “Adult Pornography.” In *The Regulation of Internet Pornography: Issues and Challenges*, Chapter 7. London: Routledge. https://doi.org/10.4324/9781315726892-7.

[34] Wire, Julia, and Esther Flanagan. “A Behavioural Science Approach to Tackling Sexism and Misogyny in Policing: Interventions for Instigating Cultural Change.” *Political Quarterly* 96, no. 2 (April 30, 2024). https://doi.org/10.1111/1467-923X.13395

[35] Collins, Christopher J., Katherine Reid, Jessica Reaves, and Jinnie Spiegler. “A Review of Anti-Misogyny Interventions for Children and Adolescents: Recommendations for the Future.” *Gender and Education*, published online August 28, 2025. https://doi.org/10.1080/09589236.2025.2552805.

[36] https://www.theguardian.com/media/2025/sep/22/under-16s-may-still-see-gambling-violent-far-right-content-under-australia-social-media-ban-simply-by-not-logging-in-zero-neo-nazis

4: Alternative technical approaches to online safety for all users, including young people;

We believe strongly, and the evidence suggests, that better regulation of social media algorithms and targeting of content will have a much greater improvement to children's online safety than a crude ban. Young people, especially those in a minority group or remote areas of Australia, depend on the internet and social media to reach "their people". When we restrict their ability to do so, there is no ready replacement. They will simply be cut-off from important parts of society.

Instead, by restricting and regulating privacy-invasive business models, we rob internet companies of the ability to monetise "shocking" content to drive engagement and advertising revenue. It is this type of content that is most harmful to young people - misinformation, violent imagery, misogyny, and pornography.[37][38][39][40][41]

Instead of incurring the privacy-related and financial costs of internet censorship and age-gates, we could invest more heavily in education for young people and adults on misinformation, sexual health and relationships,

[37] Kops, Maxime Jaqueline, Catherine Schittenhelm, and Sebastian Wachs. "Young People and False Information: A Scoping Review of Responses, Influential Factors, Consequences, and Prevention Programs." *Computers in Human Behavior*, no. 169 (2025): 108650. https://doi.org/10.1016/j.chb.2025.108650

[38] "Screen Violence: A Real Threat to Mental Health in Children and Adolescents." *The Lancet Regional Health – Americas* 18 (March 2023): 100473. https://doi.org/10.1016/j.lana.2023.100473.

[39] Albajara Sáenz, Ariadna. "Adolescence at Risk: Online Misogyny, Mental Health, and the Urgent Need for Action." *ACAMH Blog*, July 28, 2025. Accessed September 22, 2025. https://www.acamh.org/blog/adolescence-at-risk-online-misogyny-mental-health-and-the-urgent-need-for-action/.

[40] "Children and Young People's Exposure to Pornography." *Australian Institute of Family Studies*. Accessed September 22, 2025. https://aifs.gov.au/resources/short-articles/children-and-young-peoples-exposure-pornography

[41] An Unfair Fight – How Algorithms Are Shaping Our Adolescents," *eSafety Commissioner*, April 17, 2025. Accessed September 22, 2025. https://www.esafety.gov.au/newsroom/blogs/an-unfair-fight-how-algorithms-are-shaping-our-adolescents esafety.gov.au.

and how the internet actually works. [42][43] We defer to experts in the field but there is evidence that access to comprehensive sex education means that young people are less likely to use porn as a substitute.[44]

[42] Lewandowsky, Stephan, and Sander van der Linden. E2021. *"Countering Misinformation and Fake News Through Inoculation and Prebunking." European Review of Social Psychology* 32, no. 2 (February): 348-384. Accessed [your access date]. https://doi.org/10.1080/10463283.2021.1876983.

[43] John A. Banas and Stephen A. Rains, "A Meta-Analysis of Research on Inoculation Theory," *Communication Monographs* 77, no. 3 (September 2010): 281-311, https://doi.org/10.1080/03637751003758193.

[44] Marson, Katrina. *Legitimate Sexpectations: The Power of Sex-Ed*. Scribe Publications, 2022.

5: Appropriate oversight mechanisms for online safety codes;

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

7.6 Code review (b)[45]

While it is good and desirable that the technology industry is involved in the administration of the Code, we do not believe that it is appropriate for the industry to mark its own homework in the biennial review of the code's effectiveness. This review needs to be conducted by regulators with parliamentary oversight, such as the OAIC, with input from civil society, having been sufficiently resourced to do so.

7.6 Code review (d)[46]

The review needs to contain, at minimum, a measurable review of the effect of this regulation on children's online safety. It is not sufficient for the review to focus on compliance with the code and new items that may require compliance. That is to say, section (vii) should be considered the ultimate test for the effectiveness of the code. This section needs to be expanded to include actions emerging from Code compliance that may have been detrimental to Australians online, such as loss of privacy, the effects of overzealous censorship, and the effects to young people of an over-sanitised Internet.

[45] Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material)
[46] Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material)

6: Global experience and best practice; and any other related matters.

In July, the UK put into action its Online Safety Act, to a reception that varies between indifference and mockery.[47][48] Private Eye wryly notes that 64% of Britons think that online age verification laws won't work alongside a concomitant increase of VPN services by 6430%.[49] An enterprising and witty software developer has built a system that allows users to generate fake driving licences in the name of their MP.[50]

A petition calling for the Online Safety Act to be repealed has half-a-million signatures and is scheduled to go before parliament.[51]

There is no available evidence that the UK experience has improved online safety for young people. There are no known instances of age-gating working effectively anywhere and we are unable to find any evidence that Australia is likely to be the first.[52]

It is inevitable to conclude that age-restriction will make children less safe online. As social media and search platforms are no longer able to offer services to children, they will be able to become more adult-oriented in a number of ways. They can reasonably reduce their moderation capability as "no children" will be using the service. They can reduce restrictions on advertisements for gambling, porn, alcohol, tobacco, and similar adult products. They will continue to invade our privacy and perpetuate misinformation as this drives "user engagement" and advertising revenue. This will cause harm to adults on these services but we know that large

[47] Tom Williams, "'Unbelievably Easy': Online Age Checks Tricked in UK," *Information Age*, July 29, 2025, https://ia.acs.org.au/article/2025/unbelievably-easy-online-age-checks-tricked-in-uk.html. Information Age

[48] Matthew Smith, "How Have Britons Reacted to Age Verification?" *YouGov*, July 31, 2025, https://yougov.co.uk/technology/articles/52693/how-have-britons-reacted-to-age-verification

[49] Private Eye, Issue 1655 "Number Crunching" https://www.private-eye.co.uk/issue-1655/

[50] https://use-their-id.com/

[51] "Repeal the Online Safety Act," Petition 722903, UK Government & Parliament, opened April 22, 2025. Accessed September 22, 2025. https://petition.parliament.uk/petitions/722903 petition.parliament.uk

[52] "Global Age Verification Measures: 2024 in Review." *EFF Deeplinks Blog*, December 2024. Accessed September 22, 2025. https://www.eff.org/deeplinks/2024/12/global-age-verification-measures-2024-year-review.

numbers of children will use the platforms anyway, despite eSafety's hopes.[53] and they will also be exposed to this content[54]

More bleakly, sexual abusers and predators will simply move to the platforms where children are.[55] By definition, that means those not covered by the safety codes such as online gaming. Even worse, when a child is approached inappropriately on a platform that is subject to the code, they're less likely to get access to safety tools on the platform, and also will be less likely to talk with a safe adult as they're doing something they "shouldn't" and won't want to be punished[56]. In its current form, the Online Safety Code will be doing the opposite of what it intends and putting Australian children more at risk from sexual abuse.

[53] Tom Williams, "'Unbelievably Easy': Online Age Checks Tricked in UK," *Information Age*, July 29, 2025, https://ia.acs.org.au/article/2025/unbelievably-easy-online-age-checks-tricked-in-uk.html. Information Age

[54] Nair, Abhilash. 2018. "Adult Pornography." In *The Regulation of Internet Pornography: Issues and Challenges*, Chapter 7. London: Routledge. https://doi.org/10.4324/9781315726892-7.

[55] "Roblox Grooming Allegations Pedophiles," *MSNBC*, RCNA225877. Accessed September 22, 2025. https://www.msnbc.com/top-stories/latest/roblox-grooming-allegations-pedophiles-rcna225877.

[56] "Potential Effects of the Social Media Age Ban in Australia." *The Lancet Digital Health*, 2025. https://doi.org/10.1016/S2589-7500(25)00024-X.