Submission to the Office of the eSafety Commissioner

regarding the

Draft Consolidated *Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material)* under the *Online Safety Act 2021*

22 November 2024

DIGITAL RIGHTS WATCH

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[1]

[1] Learn more about our work on our website: https://digitalrightswatch.org.au/

Who we are

Digital Rights Watch is a charity organisation 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

[redacted] Chair [redacted]

General remarks

Digital Rights Watch (DRW) welcomes the opportunity to provide a submission in response to the Phase 2 Draft Consolidated Industry Codes of Practice for the Online Industry (the Codes). We recognise there are genuine challenges regarding the safety of vulnerable groups, including children, as well as the distribution of unlawful material online. We also recognise the legitimate interest of the Australian government to promote safer online services to individuals across Australia.

As a leading Australian organisation working to protect our collective digital rights, DRW is primarily concerned with ensuring an appropriate balance is struck with regard to the impact upon individuals' and communities' rights, including any adverse impacts it may have on privacy, digital security, and freedom of speech and expression.

As always, we emphasise that privacy and digital security are essential to uphold safety. Questions of legitimacy, proportionality, and reasonableness also must be carefully considered in any rights-balancing activity when determining online safety policy interventions. Digital Rights Watch is contributing to this consultation in the spirit of seeking to ensure that Australia's approach to online safety does not end up disproportionately undermining safety in the quest to enhance it.

Over the years, Digital Rights Watch has actively participated in Australia's online safety policy space. Since the inception of the Online Safety Act 2021 (OSA), we have consistently engaged with the Office of the eSafety Commissioner and other relevant government bodies and industry groups to provide a human rights-focused perspective to the consultation and policy development process.

Digital Rights Watch has played an active role in previous consultations regarding the Online Safety Act which remain relevant to the draft industry codes, including submissions to:

- Submission to the initial Online Safety Legislative Reform Consultation (February 2020)
- Submission on the proposed *Online Safety Bill*, (February 2021)
- Submission in response to the Restricted Access Systems discussion paper (September 2021) and draft declaration (November 2021)
- Submission on the draft Basic Online Safety Expectations (November 2021) and the later proposed amendments (March 2024)
- Submission to the Inquiry into Online Safety and Social Media (January 2022)
- Submission on the draft online safety Industry Codes (October 2022) and the subsequent draft Industry Standards (January 2024)
- Submission to the Online Safety Act Review (June 2024)

Digital Rights Watch welcomes the opportunity to participate in public hearings or further consultations and to provide comment and feedback on future specific proposals.

Age assurance technologies

We recognise that a core component of these Codes calls for the implementation of age assurance measures in limiting access to platforms and services based on age.

These Codes have been drafted before the government's $6.5million trial into the efficacy of age assurance measures has produced any findings. We appreciate the discussion paper recognises the current "immature" state of such measures, but we suggest the risks involved with age assurance technologies should lead to their exclusion from the Codes, rather than hope that future effective technologies will materialise.

Digital Rights Watch has provided extensive feedback through submissions, participation in roundtables, and discussions regarding the challenges of age assurance and age verification systems from the perspective of both privacy and digital security risks, as well as with regard to the challenges of effective technical implementation.

Our views on this issue have not changed since our previous submissions, and are summarised below for ease of reference:

1. Age verification is privacy-invasive, which can undermine the objective of reducing online harm. Most forms of age verification require the user to provide additional personal information beyond what is justifiable needed for proof-of-age in order to be effective. Incentivising companies and government agencies to collect, use, and store additional personal information in order to conduct age verification creates additional privacy and security risks which, in turn, can exacerbate online harms. There are significant, if not insurmountable, challenges to implementing age verification in a way that is both effective, as well as minimising privacy and security risk.[2]

2. Age Verification and Restricted Access Systems have been considered in Australia and overseas in the past but have failed to be implemented due to their overreach, blunt approach, unreasonable impact upon individual's privacy, and the creation of adverse digital security risks.

3. Other suggested "age assurance" processes such as age estimation based on face scanning also create privacy risks due to their use of biometric data, introduce the risk of inaccurate age classification, and are likely to have disproportionate negative impacts on marginalised communities. As precise biological age cannot be determined by an image of a human face, the use of this method guarantees that there will be adult individuals misclassified as children and prevented access to lawful material, as well as children misclassified as adults. Facial recognition technology has high rates of error across race and gender, which can result in significant differences in human age estimators across gender and race.[3]

---

[2] For further exploration of these issues, see for example, QUT Digital Media Research Centre submission in response to the calls for evidence regarding age verification and restricted access systems, Dr Zahra Stardust, Lucinda Nelson and Abdul Obeid. 14 September 2021. https://eprints.qut.edu.au/213887/1/2021_DMRC_and_ADMS_submission_re_age_verification_and_restricted_access_systems.pdf

[3] Guo, G., & Mu, G. (2010, June 13-18). Human age estimation: What is the influence across race and gender? IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, San Francisco, CA, USA. https://doi.org/10.1109/CVPRW.2010.5543609.

4. Mandatory age verification is likely to act as a deterrent for many adults accessing legal content, and may prompt people of all ages toward less safe and secure internet services in order to circumnavigate providing personal information.[4]

5. The majority of suggested approaches to age verification are easily bypassed with the use of common technologies such as Virtual Private Networks (VPNs), significantly diminishing their effectiveness.[5]

The combination of these factors are likely to result in a system which is unduly invasive in data collection, creates new privacy and security risks by holding information on individuals, and yet is unlikely to be effective at preventing people under the age of 18 from accessing restricted content. If these underlying issues are not addressed, the outcome may be a system that is not simply ineffective but actively harmful.

Introducing industry-wide age assurance measures is particularly fraught in Australia, where we do not have a federally enforceable human rights framework to protect people's right to privacy. This places Australian users at an elevated risk of harm compared to other jurisdictions with stronger privacy protections, and we submit that this legislative context must be taken into account when comparing these codes with, for example, approaches in the United Kingdom.

We recommend there be no mandate for untested technology, such as those used for age assurance.

Pause further development until the Codes can be aligned with the government's ongoing reform agenda

We have previously raised concerns regarding both the timing and the consultation processes throughout the development of the entire online safety regime to date. Unfortunately, the Codes follow the alarming trend of only providing civil society and other relevant stakeholders with an extremely short timeframe to provide feedback on a complex regulatory scheme. These proposals stand to have significant impact upon the way that people are able to use digital services as well as their fundamental human rights, and require appropriate time for community groups, small businesses and civil society organisations to consider and meaningfully respond.

In addition to this, the Codes are being developed ahead of significant regulatory reform that is highly likely to impact the way the Codes are implemented. While we understand the desire to move quickly, doing so runs the risk of creating an overly complex, contradictory, and constantly changing regulatory landscape.

The Codes should be consistent with broader government policy and related regulation. For instance, the outcome of the review of the Privacy Act is likely to have a direct impact upon the Codes. Personal privacy is crucial to online safety for many people, especially

[4] Blake, P. (2018). Age verification for online porn: more harm than good? Porn Studies, 6(2), 228– 237.
[5] Yar, M. (2019). Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. Policing: An International Journal, 43(1), 183–197.

vulnerable populations, and so any industry code providing guidance for online safety must integrate best practices for privacy protection.

In addition to the $6.5million trial into the efficacy of age assurance measures, we note that the government has introduced new legislation aimed at enforcing 16 as the minimum age to use social media.[6] This further complicates requirements for platforms to adhere to regarding access to content and protecting the rights of users. A fragmented and potentially contradictory legislative environment could lead to overcapture, where platforms seek cost-minimising approaches to compliance that limit users' access to lawful content (including content outside the remit of the Codes), and introduce severe privacy and security risks.

We suggest that further development of the Codes is paused until such a time that the Codes can align with, and give effect to, relevant legislation currently under review, including the Privacy Act.

Use clear and consistent definitions of Class 1C and Class 2 material

The Codes include various interpretations of Class 1C and Class 2 material, such as 'high impact pornography', 'high impact nudity', and 'seriously harmful material'. Specifically, the Codes use the terms 'high impact online pornography' to describe all Class 1C and Class 2A material. These phrases communicate a moralistic interpretation of content, rather than useful definitions, and contribute to a culture that stigmatises adult content.

For simplicity and accuracy, the Codes ought to exclusively employ the clear and consistent definitions, i.e. Class 1C and Class 2 material, as necessary.

Provide a transparent appeals process

We support the recommendations made by Scarlet Alliance in their submission regarding a transparent appeals process. The Online Safety Act enacts a broad-scope regulatory framework for all forms of internet technology, including search engines, apps and app stores, social media services, messaging platforms, and websites. Services have extensive obligations in relation to complaints mechanisms, but no obligations in relation to appeals processes for miscategorised or maliciously reported content.

Given the high risks of overcapture in relation to class 2 content, the Codes should create equal obligations for platforms to provide equally weighted transparent complaints mechanisms and appeals processes that comply with procedural fairness expectations already understood in Australian law.

Limit the burden of compliance on businesses

Much of the Codes have been drafted from the perspective of large, well-funded platforms who may have access to central trust and safety teams or dedicated policy teams who can interpret and implement the regulations.

---

[6] https://www.pm.gov.au/media/press-conference-parliament-house-canberra-32, *Online Safety Amendment (Social Media Minimum Age) Bill 2024*

A healthy platform ecosystem is one with a mix of enterprise, small and medium businesses, as well as independent content creators who may make a living from creating and sharing content that fall under these Codes. The high regulatory cost of compliance may see many of these actors exit the ecosystem, entrenching the power and reach of well-funded, international platforms. This consequence ought to be considered when analysing the cost-benefit of new Codes.

There is also a risk that an overly cumbersome burden of compliance will not encourage platforms to create safer environments, but rather restrict access for all users by geography. In the US, where age verification laws have been introduced in several states, Pornhub has blocked access to all users in those states.[7] As reported in The Guardian, users in those states have resorted to using virtual private network (VPN) connections to get around the block.[8]

[7]Age Verification in the US. Retrieved November 22, 2024, from https://www.pornhub.com/blog/age-verification-in-the-news

[8] Taylor, J. (2024, October 22). Adult content sites without age checks may be blocked from Australian search results under draft code. The Guardian. https://www.theguardian.com/australia-news/2024/oct/22/australia-adult-content-sites-age-restrictions-blocked-search