To: DIGI

Re: Submission to Phase 2 Draft Industry Codes

Thank you for the opportunity to make a submission to the Phase 2 Draft Industry Codes.

Assembly Four is a collective of sex workers and technologists based out of Naarm, Australia. We collaborate with sex workers across the globe to create products and services that help sex workers to thrive online. Assembly Four was founded on the belief that impact is more important than profit. We strongly believe that having the ability to make decisions about our bodies and sexual lives is a fundamental human right. Anyone should be able to make these choices without fear, violence or discrimination. Sex workers are still fighting for this right.

Assembly Four has been involved in the development of Australia's online safety framework since 2019. Our investment in contributing to this process derives from our experience in navigating online discrimination, both as a business associated with the adult industry and as sex workers ourselves. Online spaces are already hostile and discriminatory towards sex workers. Sex workers experience deplatforming, shadow banning, breaches to data privacy, targeted outing, financial discrimination from payment providers and general online harassment. Given the stigma and discrimination levied at sex workers, privacy and anonymity/pseudonymity is central to sex workers being able to conduct their work online safely. Key concerns with the prioritisation of age assurance within the current draft Codes include: onerous and unfeasible compliance requirements placed on sole-trader sex workers and the serious privacy risks of associating legal identities with online platform accounts used for work purposes.

Assembly Four has co-authored a joint submission with Scarlet Alliance, New Zealand Sex Workers Collective, Digital Rights Watch, Blood-Ed, The Woodhull Foundation, NSW Council for Civil LIberities, Eros Association, Australian Injecting Illicit Drug Users League, [redacted] This separate and brief submission aims to drive home our specific concerns about the privacy risks inherent to age assurance processes.

If you have any questions or require clarification, please do not hesitate to reach out to [redacted]

Regards,
Assembly Four.

Introduction

Assembly Four has provided consultation and submissions to the Federal Government, the eSafety Commission and the industry associations since the beginning of the *Online Safety Act 2020* (*OSA*) inquiries in 2019. Throughout this time our position has remained consistent and firm - **we do not support age assurance and age verification as effective means of ensuring online safety** - yet our concerns remain unreflected in the proposals at each stage. These draft codes are no exception to this. At each stage, despite collective efforts to curb the progression of the online safety framework, we feel our concerns have been continually dismissed as the eSafety Commission pushes further down the path of prioritising a prohibitive stance via age assurance rather than seeking to address more complicated societal concerns.

We would like to note that the recent federal development of the *Online Safety Amendment (Social Media Minimum Age) Bill* 2024 takes a broad and prescriptive approach to age verification and age assurance. Comparatively, within the draft Codes we can see attempts have been made to take a more nuanced approach to age assurance - which we appreciate. However, our stance remains that we do not support age assurance and age verification as an effective means of ensuring online safety.

This submission will briefly cover: notes on the broader regulatory context wherefrom we write this submission, our concerns with age assurance, prohibition and privacy under the Codes and a few specific recommendations.

Broader regulatory context

Whilst we acknowledge that the broader regulatory context is not controlled by the Industry Bodies who are drafting these codes, it would be amiss for us to not take the opportunity to highlight our **on-going concerns around significant legislative review and reform taking place concurrently with the design of these codes and how these changes may impact the codes and the subsequent operations of them.** We understand that the development of the online safety framework has been siloed into different bodies of governance. However, given the major changes proposed by the federal government and eSafety Commission **we expect that the various bodies involved demonstrate a higher level of collaboration.** The recent *Online Safety Amendment (Social Media Minimum Age) Bill* 2024 occurring prior to the acceptance of the Phase 2 codes and the upcoming age assurance trial, to us, demonstrate a lack of collaboration that is frustrating to observe - and no doubt costly to the Australian public.

Beyond this, we note the incongruence between the speed at which the online safety framework has developed compared to how stymied the *Privacy Act 1988* Review and the proposed reform of the *National Classification Code* has become. It concerns us that the development of these codes has occurred by reference to outdated privacy and content classification frameworks. As such, we believe that **the *Privacy Act* Review must be prioritised to ensure that any further policy developments associated with the *OSA* reflect the realities of contemporary privacy concerns and rights.**

Concerns with age assurance, prohibition and privacy.

Assembly Four argues that the codes do not strike an appropriate balance between user privacy, data security, freedom of expression and online safety. **We believe that continuing to prioritise age assurance methods as a means to 'safeguard children' online will result in an ineffective, costly and harmful framework to both young people and the broader Australian population.** In short, we suggest that the risks to Australian end-user privacy - including risks to data security, exploitation and retention by industry and third party age assurance services - far outweigh the potential (yet un-evidenced) benefits of age assurance. **We believe that the government and eSafety have over-relied on the strategy of prohibition - fundamentally precluding 'balance' as a possibility.**

The development of the online safety framework has relied heavily on the idea that age assurance measures will be effective in prohibiting access to certain kinds of content. On a government policy level, age assurance measures have been firmly welded to the idea that children will be 'safe guarded' if industry can implement and maintain robust and restrictive age assured access points. The idea that children and all Australian end users require a prohibitive approach from the government to ensure our collective online safety is often posited as 'fact' by eSafety and the industry associations. However, there remains a lack of evidence to support the idea that age assurance methods are an effective response to online harms. **Conversely, there is a growing body of evidence suggesting that age assurance measures are not only ineffective, but can cause harm to users such as limiting freedom of speech, compromising privacy and excluding access to online spaces that facilitate self-exploration, community building and education.**[1] A recent Australian

[1] Brage, Lluís & Rosón, Carlos & Alvarez, Manuel & Calderón, Beatriz (2022) 'Characteristics of Online Pornography and Interventions Against its Negative Effects in Young People: Results from an International Delphi Panel' *Journal of Rational-Emotive & Cognitive-Behavior Therapy* 40, pp. 1-13; Yar, Majid. (2019) 'Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK' *Policing: An International Journal* (ahead-of-print);
Livingstone, Sonia & Nair, Abhilash & Stoilova, Mariya & Van der Hof, Simone & Caglar, Cansu. (2024) 'Children's Rights and Online Age Assurance Systems: The Way Forward' *The International Journal of Children's Rights* 32, pp. 721-747; Blake, Pandora. (2019) 'Age verification for online porn: more harm than good?' *Porn Studies* 6, pp. 1-10; Chittick, Kyler (2024) 'Age-verification technologies and the censorship of online pornography in Canada: a critique of Bill S-210: An Act to Restrict Young Persons' Online Access to Sexually Explicit Material' *Porn Studies* 1-8.

study[2] analysed the privacy risks that arise from different methods of age assurance such as: matching drivers' licences, credit cards or passports against government databases, analysing biometric information and profiling online behaviour. The article noted:

> *Privacy, feasibility and accessibility concerns about mandatory age verification have been repeatedly raised by civil society [...]* ***There are open questions about how age verification data would be saved, stored, accessed and shared, given that the systems are usually proprietary and privately implemented.*** *This is especially the case where user profiles could be cross-checked across other government databases such as the electoral roll, risking the unnecessary aggregation of personally identifiable, sensitive information. There is a risk that users could have their browsing histories, sexual preferences and online behaviour recorded on databases that could be sold, shared, hacked or leaked with little regulatory oversight.* ***Such sensitive records would also become highly valuable (and easily exploitable) targets for extortion, blackmail and identity theft.*** *One of the techniques the eSafety Commissioner considered, 'behavioural signalling', requires accumulating multiple data points about users, such as GPS, cookie data, IP address, username, physical address and browsing history. Such data collection has been proven to introduce numerous privacy risks (Zhao et al., 2022).*[3]

In addition to the serious risks of sensitive data retention and breach, **Assembly Four is concerned about the possibility that relevant electronic services may be required to scan all Australian users' communications and messages to detect and remove lawful Class 1C and Class 2 materials.** This proposal is an extreme overstep in government oversight and surveillance and poses serious risks to user privacy and freedom of expression and connection.

We note that the eSafety Commission and the Codes acknowledge that age assurance technologies are 'immature' and come with significant gaps in feasibility and technical efficacy and should run alongside media literacy and education. Further we note that the Codes attempt to strike a balance between privacy and accuracy in prescribing appropriate age assurance measures on a tiered scale, alongside a risk and feasibility framework. However, we are yet to see either the eSafety Commission or the Codes action these acknowledgments in a meaningful way. **From our perspective, as long as age assurance methods are prioritised and mandated in any capacity, the risk to Australian user privacy remains serious and worrisome.**

---

[2] Stardust, Zahra & Obeid, Abdul & McKee, Alan & Angus, Daniel (2024) 'Mandatory age verification for pornography access: Why it can't and won't 'save the children'' *Big Data & Society* 11.
[3] Ibid.

Recommendations

In addition to the recommendations made in our joint submission, we make the following recommendations:

1. **Remove age assurance compliance measures completely.**
2. **Providers of relevant electronic services that allow users under 18 should not be required to scan all Australian user's communications and messages to detect and remove lawful Class 1C and Class 2 materials.**
3. **Australian end-users who engage with online devices or services should not be required to undergo age assurance processes including Australian end-users who wish to access 'high impact services'.**