eros the adults only association

**via osareview@communications.gov.au**

21 June 2024

To whom it may concern,

## Statutory review of the Online Safety Act 2021

The Eros Association is Australia's industry association for adults-only retail, wholesale, media and entertainment. We write in relation to the statutory review of the *Online Safety Act 2021*.

**1. Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?**

Without expressing any views on the objects of the *Online Safety Act 2021*, we do believe the review should consider recommendation 19 of the House of Representatives Select Committee on Social Media and Online Safety regarding possible models of a single regulatory framework that would simplify regulatory arrangements.[1] Were this to be adopted, this would necessitate expansion of the objects of the *Online Safety Act 2021*.

**2. Does the Act capture and define the right sections of the online industry?**

Without expressing any views on whether the *Online Safety Act 2021* captures the right sections of the online industry, we do believe that ways in which sections of the online industry are defined can be confusing. For example, the terminology of "designated internet services" does not make it readily apparent that this applies to websites. We recommend that the Act use clearer terminology in defining sections of the online industry rather than unclear terminology such as "designated internet services".

**3. Does the Act regulate things (such as tools or services) that do not need to be regulated, or fail to regulate things that should be regulated?**

One of the major problems of the *Online Safety Act 2021* is that the category of class 1 material is incredibly broad. To address this, the eSafety Commission has developed separate designations of "class 1A material", "class 1B material", and "class 1C material", the latter of which comprises particular online pornography, including fetish material. This acknowledges the relative severity and potential for harm associated with different types of material.

However, this designation is not incorporated in the *Online Safety Act 2021*, which takes an all-encompassing approach to class 1 material. The definition of class 1

[1] House of Representatives Select Committee on Social Media and Online Safety, *Social Media and Online Safety* (2022) 155.

material in the Act, is reliant on the Classification Guidelines, which are woefully out of date. The Government has proposed to establish a Classification Advisory Panel to undertake a review of the Classification Guidelines, which we welcome. We are, however, concerned that the establishment of such a body could take time and thus further delay reforms to the Classification Guidelines. In the meantime, we recommend that amendments be made to the Act to distinguish between class 1A, class 1B, and class 1C material, with definitions mirroring that in the eSafety Industry Codes Position Paper.

**4. Should the Act have strengthened and enforceable Basic Online Safety Expectations?**

In our view, the Basic Online Safety Expectations do not need to be further strengthened since their amendment in May 2024.

We do not object to the additional expectations under the Basic Online Safety Expectations being made enforceable (potentially through incorporation into section 46 of the *Online Safety Act 2021*). However, the reasonable steps that service providers can take to meet the core or additional expectations should not be made enforceable; they are indicators of steps that can be taken to meet the core and additional expectations and should not be compulsory but left to service providers' discretion.

**5. Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the code drafting process be improved?**

As the Issues Paper states:

*Industry codes and standards are being implemented through a two-phased approach. Phase 1 focused on Class 1 [A and B] material, including child sexual exploitation and abuse material, pro-terror material and extreme crime and violence material. Six codes are now in operation, and standards for the two additional sections of industry are being determined. Phase 2 will focus on Class 2 material (material that would be classified R18+ or X18+, including pornography and other high impact material) and remaining Class 1 [C] material (material depicting a small set of fetish practices).*[2]

Whilst we are still awaiting the implementation of the industry codes and standards, we are concerned that Draft Online Safety (Designated Internet Services - Class 1A and Class 1B Material) Industry Standard 2024 contains at least 38 compliance measures that could be significantly consolidated to reduce repetition and duplication. In this regard, we recommend that the code and standard drafting process be improved by further consultation with industry and an impact analysis of each code and standard in line with guidance from the Office of Impact Analysis.

[2] Department of Infrastructure, Transport, Regional Development, Communication and the Arts, *Statutory Review of the Online Safety Act 2021: Issues Paper* (2024) 13.

**6. To what extent should online safety be managed through a service provider's terms of use?**

The Basic Online Safety Expectations include expectations about service providers' terms of use. As stated above, we do not believe the Basic Online Safety Expectations need to be further strengthened since their amendment in May 2024. We further believe that it is appropriate that certain aspects of online safety be managed through service providers' terms of use, as outlined in the Basic Online Safety Expectations, and not through legislation.

**7. Should regulatory obligations depend on a service provider's risk or reach?**

We support regulatory obligations being based on a service provider's risk or reach, as per European Union legislation.

However, there are certain aspects of this legislation that we oppose, including age verification or age estimation (as required under section 81 of the *Online Safety Act 2023* (UK)), for the reason that it has severe privacy implications and that there is already a regulatory system in place for restricted access to pornography under the Online Safety (Restricted Access Systems) Declaration 2022.

**8. Are the thresholds that are set for each complaints scheme appropriate?**

As the Issues Paper notes, "of all the complaints schemes in the Act, the Online Content Scheme [that regulates online pornography] has the broadest scope in terms of who can make a complaint, the services regulated, and the basis for making a complaint."[3] In our view, the thresholds set for complaints under the Online Content Scheme are appropriate, though we do note that we are still awaiting industry codes and standards for class 1C and class 2 material.

**9. Are the complaints schemes accessible, easy to understand and effective for complainants?**

In our view, complaints under the Online Content Scheme are accessible, easy to understand, and effective. In 2022-23, 1501 complaints were made to the eSafety Commissioner about sexually explicit material.[4] This large volume of complaints suggests that the complaints scheme is accessible for complainants. In our experience, many of these complaints have been directed against adult retailers.

We appreciate that the eSafety Commissioner has in the past reached out to us as a relevant industry association to help ensure that online platforms are meeting their obligations under the Online Content Scheme and to provide eSafety with an understanding of the work that is being undertaken by the industry to work towards

[3] Department of Infrastructure, Transport, Regional Development, Communication and the Arts, *Statutory Review of the Online Safety Act 2021: Issues Paper* (2024) 25.

[4] Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2022-23* (2023) 218.

compliance with the Scheme in order to determine what action it should take in relation to any complaints received.

**10. Does more need to be done to make sure vulnerable Australians at the highest risk of abuse have access to corrective action through the Act?**

It is unclear whether vulnerable Australians face particular barriers to accessing corrective action through the *Online Safety Act 2021*, so we recommend that the eSafety Commissioner undertake further research on any barriers that vulnerable Australians face in accessing corrective action under the Act before any reforms are made to the regulatory framework.

**11. Does the Commissioner have the right powers to address access to violent pornography?**

Sexual violence is currently refused classification under the Guidelines for Classification of Films 2012 and is class 1 material under the *Online Safey Act 2021*. It is regulated by the Online Content Scheme and, in our view, the eSafety Commissioner has adequate powers under this Scheme to address access to pornography depicting sexual violence.

A significant issue, however, is that fetishes are placed in the same class as class 1 material. Please see our response to question 3 (above) that discusses this issue further. In light of this, we recommend that the Government urgently bring forward a proposal to the Standing Council of Attorneys-General to remove the absolute prohibition on legal fetishes within the X18+ category, in line with recommendation 9-15 of the Review of Australian Classification Regulation.

**12. What role should the Act play in helping to restrict children's access to age inappropriate content (including through the application of age assurance)?**

The Online Safety (Restricted Access Systems) Declaration 2022 already restricts children's access to pornographic content through its requirement for access-control systems that incorporate reasonable steps to confirm that a person accessing this content is an adult.

**13. Does the Commissioner have sufficient powers to address social media posts that boast about crimes or is something more needed?**

We make no comment in response to this question.

**14. Should the Act empower 'bystanders', or members of the general public who may not be directly affected by illegal or seriously harmful material, to report this material to the Commissioner?**

As the Issues Paper notes, "of all the complaints schemes in the Act, the Online Content Scheme [that regulates online pornography] has the broadest scope in terms of who can make a complaint, the services regulated, and the basis for

making a complaint."[5] As such, members of the general public may already report material that is in breach of the Online Content Scheme to the eSafety Commissioner.

**15. Does the Commissioner have sufficient powers to address harmful material that depicts abhorrent violent conduct? Other than blocking access, what measures could eSafety take to reduce access to this material?**

We make no comment in response to this question.

**16. What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?**

Technological solutions alone will not stop children from accessing online pornography. A focus on regulating industry diminishes the role of parental engagement and education, which was a key aspect of the *Protecting the Age of Innocence Report*.[6]

In our view, there is a need to invest in better sex education in schools and other educational settings to encourage safer and affirming sex practices, boost sexual literacy and set realistic expectations about sex. Sex education is important to challenge sexual violence and violence against women and gender diverse people. The eSafety Commissioner can also play a role in developing resources to support online safety and navigating adult content online.

**17. Does the Act need stronger investigation, information gathering and enforcement powers?**

The eSafety Commissioner has broad investigatory and information gathering powers, including powers to obtain end-user identity information or contact details.[7] In the period 2022-23, 24 notices were given by the eSafety Commissioner requiring a service provider to provide end-user identity information or contact details.[8]

The Issues Paper states that "scant data collected [is] by many services. For example, some services collect only IP information and an email address [... whereas] user information is of most assistance when it includes telephone numbers and/or financial information."[9]

---

[5] Department of Infrastructure, Transport, Regional Development, Communication and the Arts, *Statutory Review of the Online Safety Act 2021: Issues Paper* (2024) 25.

[6] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the Age of Innocence: Report of the Inquiry into Age Verification for Online Wagering and Online Pornography* (2020) [3.122].

[7] *Online Safety Act 2021* s 194.

[8] Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2022-23* (2023) 215.

[9] Department of Infrastructure, Transport, Regional Development, Communication and the Arts, *Statutory Review of the Online Safety Act 2021: Issues Paper* (2024) 36.

We have concerns about the privacy implications of sharing identity or contact information about end-users, and would be extremely concerned if the *Online Safety Act 2021* were to mandate the collection of end-user personal information, such as telephone numbers or financial information. This would have severe privacy implications and should be considered in the wider context of the Privacy Act review.

The Issues Paper also raises the issue of enforceability of penalties upon platforms based overseas, to which we would draw the Department's attention to the findings of Kennett J in *eSafety Commissioner v X Corp* [2024].[10]

**18. Are Australia's penalties adequate and if not, what forms should they take?**

In our view, the penalties under the *Online Safety Act 2021* are largely adequate, but consideration should be given to including penalties based on the percentage of a platform's global revenue, so that the penalties do not have an unfairly detrimental effect on small businesses, and penalties based on the nature and volume of offences.

**19. What more could be done to enforce action against service providers who do not comply, especially those based overseas?**

There are currently two matters by X Corp against the eSafety Commissioner before the Administrative Appeals Tribunal that may go to the question of enforcement action against service providers that are based overseas. We believe that the Department should await the outcome of these matters before deciding any amendments to enforcement actions under the *Online Safety Act 2021*.

**20. Should the Commissioner have powers to impose sanctions such as business disruption sanctions?**

The eSafety Commissioner should not have powers to impose business disruption sanctions; such sanctions should only be able to be imposed by courts in cases of extreme non-compliance.

**21. Should the Act incorporate any of the international approaches identified above? If so, what should this look like?**

The Basic Online Safety Expectations include an expectation that a service provider will take reasonable steps to ensure safe use.[11] In May 2024, the Basic Online Safety Expectations were amended to include a best interests of the child principle (namely, an additional expectation that a service provider "take reasonable steps to ensure that the best interests of the child are a primary consideration in the design

[10] *eSafety Commissioner v X Corp* [2024] FCA 499 (13 May 2024) [38]-[54].
[11] Online Safety (Basic Online Safety Expectations) Determination 2022 s 6(1).

and operation of any service that is likely to be accessed by children"[12]) and to strengthen the expectations regarding reports and complaints.[13]

As stated above, we do not believe the Basic Online Safety Expectations need to be further strengthened since their amendment in May 2024. Please also see our response to our response to question 4 (above) regarding enforceability.

**22. Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?**

As stated above, we do not believe the Basic Online Safety Expectations need to be further strengthened since their amendment in May 2024. However, if it were to be determined that the Basic Online Safety Expectations need to incorporate and formalise a duty of care towards service users, the Department should outline the scope and nature of a duty of care framework, including potential models of implementation and operation, before making any further amendments to the Basic Online Safety Expectations.

**23. Is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?**

The eSafety Commissioner's annual reports provide transparency about its regulatory actions. For example, in the period 2022-23, 13 non-periodic reporting notices were given by the eSafety Commissioner about compliance with Basic Online Safety Expectations,[14] and 5 removal notices were given by the eSafety Commissioner to social media service providers, electronic services, internet services, hosting service providers, and internet search engine providers requiring the removal of (access to) class 1 material.[15] In addition, 630 informal notices were given or informal requests made by the eSafety Commissioner to a service provider in relation to class 1 material.[16]

This suggests that the system is working effectively. However, imposing additional transparency and reporting requirements on industry, above those set out in the Basic Online Safety Expectations, could have severe privacy impacts on service users and regulatory impacts on small businesses.

**24. Should there be a mechanism in place to provide researchers and eSafety with access to data? Are there other things they should be allowed access to?**

As noted above, provision of data to regulators such as the eSafety Commissioner and to researchers does have potentially severe privacy impacts on service users

[12] Online Safety (Basic Online Safety Expectations) Determination 2022 s 6(2A).
[13] Online Safety (Basic Online Safety Expectations) Determination 2022 div 4.
[14] Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2022-23* (2023) 214.
[15] Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2022-23* (2023) 215.
[16] Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2022-23* (2023) 216.

and regulatory impacts on small businesses. In regards to the latter, it is notable that the European Union's Digital Services Act only imposes a duty to share data with authorised researchers on very large online platforms, and recent research has shown the need for privacy protection in any such data-sharing,[17] including in relation to data access for law enforcement, data storage and destruction, and data sharing beyond initial recipients. These matters need to be considered before any mechanism is put in place to allow researchers and regulators access to data.

**25. To what extent do industry's current dispute resolution processes support Australians to have a safe online experience? Is an alternative dispute resolution mechanism such as an Ombuds scheme required? If so, how should the roles of the Ombuds and Commissioner interact?**

As noted above, the Basic Online Safety Expectations were amended in May 2024 to strengthen the expectations regarding reports and complaints.[18] This requires service providers to have and provide information on both internal dispute resolution processes and guidance on how to make a complaint to the eSafety Commissioner. To introduce a further dispute resolution mechanism such as an ombudsperson would overcomplicate dispute resolution processes and make them less accessible and easy to understand, and thus undermine the aim for an effective system for complaints. Please see our response to question 9 (above) in this regard.

**26. Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?**

Disappointingly, the Issues Paper does not properly address the issue of service users' right to privacy. In this regard, we recommend that section 108(4) of the Act be amended to require that the eSafety Commissioner, in making a Restricted Access Systems Declaration, have regard to the extent to which a specific system may interfere with end-users' right to privacy; the extent of any personal information which it may require users to provide; and the strength of any data protection mechanisms in place to protect personal information required to be provided.

**27. Should the Commissioner have powers to act against content targeting groups as well as individuals? What type of content would be regulated and how would this interact with the adult cyber-abuse and cyberbullying schemes?**

We make no comment in response to this question.

**28. What considerations are important in balancing innovation, privacy, security, and safety?**

The House of Representatives Select Committee on Social Media and Online Safety stated in their report that "while privacy concerns are critical to the rights of all

[17] Centre for Democracy and Technology, *Defending Data: Privacy Protection, Independent Researchers, and Access to Social Media Data in the US and EU* (2023).
[18] Online Safety (Basic Online Safety Expectations) Determination 2022 div 4.

internet users, the Committee does not believe that these issues outweigh the fundamental issue of ensuring safety in online environments."[19] In our view, these comments are misplaced. Safety can be ensured while respecting the privacy rights of internet users, but instead it appears that the Committee's remarks have led to responses that tilt the balance in favour of safety whilst failing to respect privacy of internet users (noting, of course, that a failure to protect users' privacy can pose risks to their personal safety and security).

As the Government has acknowledged in relation to end-to-end encryption, "privacy, safety, security and lawful access are not mutually exclusive. It is possible to develop technology that protects the right to privacy, whilst also supporting law enforcement to keep the community safe."[20]

**29. Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?**

We believe that the *Online Safety Act 2021* should remain technology neutral, and focus on online harms rather than the means through which the harm is generated. The Issues Paper explores potential online harms relating to emerging technologies, which we will address in turn.

In May 2024, the Government announced its intention to introduce legislation to ban the creation of "deepfake pornography" that is digitally created or altered (sometimes through generative AI). We await the draft of that legislation before commenting further.

In regard to immersive technologies, recent research on virtual reality pornography has noted "the potential humanising effect of the increased presence and immersion felt by users."[21] As such, it is not correct to frame emerging technologies as solely harmful, given that they may have positive benefits. We are also aware of recommender systems and algorithms making it challenging for users to search for adult content.[22] In this way, emerging technologies can impact adult users' access to online content. In addition, pornography performers and producers are increasingly embracing blockchain technologies because of banking providers and payment channels refusing to provide services to them. In this way, emerging technologies allow for businesses to escape discriminatory practices.

[19] House of Representatives Select Committee on Social Media and Online Safety, *Social Media and Online Safety* (2022) 181.
[20] Australian Government, *Australian Government Response to the House of Representatives Select Committee on Social Media and Online Safety Report* (2023) 15.
[21] Leighton Evans, 'Virtual reality pornography: A review of health-related opportunities and challenges' (2023) 15 *Current Sexual Health Reports* 34.
[22] Gayatri Kapur and Asic Hussain, 'Identifying challenges of Indian users searching for NSFW content in AI-assisted platforms' in Amaresh Chakrabati and Vishal Singh (ed), *Design in the Era of Industry 4.0* (2023, vol 2).

Please see our response to questions 21 and 22 (above) regarding safe use obligations and a statutory duty of care, and our response to question 28 (above) regarding end-to-end encryption.

**30. To what extent is the Act achieving its object of improving and promoting online safety for Australians?**

In our view the *Online Safety Act 2021* and the accompanying regulatory framework is achieving the object of improving and promoting online safety. Any reforms should be balanced against adult users' rights to seek out and access content, including adult content, online.

**31. What features of the Act are working well, or should be expanded?**

In summary, features of the *Online Safety Act 2021* should be expanded as follows:

- section 108(4) of the Act should be amended to require that the eSafety Commissioner, in making a Restricted Access Systems Declaration, have regard to the extent to which a specific system may interfere with end-users' right to privacy; the extent of any personal information which it may require users to provide; and the strength of any data protection mechanisms in place to protect personal information required to be provided;
- the Act should use clearer terminology in defining sections of the online industry rather than unclear terminology like "designated internet services";
- amendments should be made to the Act to distinguish between class 1A, class 1B, and class 1C material, with definitions mirroring that in the eSafety Industry Codes Position Paper;
- the industry code and standard drafting process should be improved by further consultation with industry and an impact analysis of each code and standard in line with guidance from the Office of Impact Analysis; and
- the Government should urgently bring forward a proposal to the Standing Council of Attorneys-General to remove the absolute prohibition on legal fetishes within the X18+ category, in line with recommendation 9-15 of the Review of Australian Classification Regulation.

**32. Does Australia have the appropriate governance structures in place to administer Australia's online safety laws?**

We believe Australia has appropriate governance structures in place to administer Australia's online safety laws. As discussed above in our response to question 25, to introduce further governance structures such as an ombudsperson would overcomplicate dispute resolution processes and make them less accessible and easy to understand, and thus undermine the aim for an effective system for complaints in relation to online safety.

**33. Should Australia consider introducing a cost recovery mechanism on online service providers for regulating online safety functions? If so, what could this look like?**

We do not believe that there should be a cost recovery mechanism on online service providers for regulating online safety functions.

Cost recovery mechanisms in the European Union only apply to very large online platforms and the United Kingdom regulator, Ofcom, is yet to determine details of their cost recovery fee regime. If a cost recovery mechanism is to be introduced, we believe that its introduction should await determination by Ofcom of its cost recovery fee mechanism and should not, in any case, apply to small and medium businesses who already incur significant costs in complying with the Australian online safety regime.

The Eros Association thanks you for your consideration of our submission and welcomes the opportunity to discuss with you further our views on these issues.

**Graeme Dunne**
General Manager
Eros Association

E: [redacted] | www.eros.org.au