Director – Strategy and Research,
Online Safety, Media and Platforms Division,
Department of Infrastructure, Transport, Regional Development, Communications and the Arts,
GPO Box 594
Canberra, ACT 2601

Dear Sir/Madam,

SUBMISSION IN RELATION TO THE STATUTORY REVIEW OF THE ONLINE SAFETY ACT 2021 (THE REVIEW)

The Consumer Electronics Suppliers Association (**CESA**) welcomes the opportunity to provide feedback to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts in relation to statutory review of the *Online Safety Act 2021* (**the Act**).

CESA is a leading national, industry body representing manufacturers and suppliers of equipment used to access online services. CESA members include major brands of connected TV devices, as well as certain brands of computers and smartphones and are a regulated section of the online industry, as defined under the Act. A list of CESA members is published on the CESA website.

CESA has been involved in and engaged with the Office of the eSafety Commissioner and other industry stakeholders in relation to the development of industry codes under the Online Content Scheme. We will continue to work with stakeholders to promote and support measures to improve online safety for Australians particularly for children and vulnerable adults.

CESA believes that industry play an important role in providing practical technical expertise and supports principle-based, harmonised regulations and industry codes. However, it is imperative that expectations and compliance measures are tailored to the role, nature and purpose of the service, platform or devices and are commensurate with the level of risk of online harm.

CESA members are concerned of the potential risk of overreach of the powers in the Act insofar as they extend to device manufacturers and suppliers under the Online Content Scheme particularly in circumstances where the majority of devices supplied in Australia are:

- based on global designs and that local suppliers have limited control implementing "Australia-only" compliance requirements. It is therefore imperative that any changes to the Act harmonises with global approaches and with other regulatory frameworks such as the current Cybersecurity reforms; and
- multi-purpose, technically complex and may not have the capability to scan and filter material in order to limit access to specific types of content.

Further, any regulations must be flexible to keep pace with technological advancements, not stifle innovation and respect end-user privacy and digital freedoms.

It is important that the above considerations underpin the development of recommendations to the Minister in respect of proposed changes to the Act in relation to:

- Australia's regulatory approach to online services, systems and processes
- protecting those who have experienced or encountered online harms
- penalties, and investigation and information gathering powers
- international approaches to address online harms, and
- regulating the online environment, technology and environmental changes.

As a matter of good regulatory practice, any proposed changes to existing laws should not only properly assess the level of harm but importantly should seek to address the underlying cause.

Kindly refer to the annexed Schedule outlining CESA's response to the questions raised in the Issues Paper dated April 2024. Responses have been provided in relation to questions that are of interest to CESA members.

CESA would welcome the opportunity to work closely with the Department as the Review process progresses.

Schedule of CESA's Response to the Questions Raised in the Issues Paper

Part 2 – Australia's regulatory approach to online services, systems and processes

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

The overarching objective of the Act to improve and promote online safety for Australians are sufficient.

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

Yes, however the obligations should vary based on the role, nature and risk associated with a particular goods or service. A broad brushed regulatory approach imposes an unnecessary and disproportionate regulatory burden on industry. A better approach would be to regulate high risk services and platforms rather than sections of the industry

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?

Regulation should be focussed on tools or services base which based on evidence and assessment are classified as being 'high risk'. The current definitions are too broad and do not adequately take into account the specific nature and manner in which a tool, device or service is used nor does it address the underlying cause of the issue.

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

No comment

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 codes drafting process be improved?

Given the complexity with developing codes for a broad range of services, it is essential that sufficient (and realistic) time is allocated for development of codes and that extensive consultation is undertaken with wider industry stakeholders.

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

No comment

7. Should regulatory obligations depend on a service providers' risk or reach?

Regulatory obligations should primarily be risk-based however reach should be factor in determining the risk level.

Part 3 – Protecting those who have experienced or encountered online harms

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

Thresholds based on classifications under the National Classification Scheme should be reviewed to ensure that they are suitable and applicable to new technologies and media.

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

No comment

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?

No comment

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

Yes

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)?

Restricting children's access to age inappropriate content should be regulated under the Act however care should be taken to ensure that the application of age assurance has regard to international and industry developments and any learning from the planned pilot program.

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

No comment

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?

Yes however complaints will need to be properly assessed.

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?

Blocking access whilst effective is a short term 'fix'. More focus should be given on developing regulations that address the underlying cause and implement programs designed to educate and facilitate behavioural changes.

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

No comment

Part 4 – Penalties, and investigation and information gathering powers

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

Yes

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

Current penalties are adequate however higher penalties should apply for serious or systemic breaches.

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

No comment

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

No and if business disruption sanctions were to apply, they should only be utilised in cases of significantly serious and repeated breaches.

Part 5 – International approaches to address online harms

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

No comment

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

No comment

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

Yes

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?

No comment

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?

No comment

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

Yes, there should be safeguards to protect human rights, privacy and digital freedoms by ensuring that regulatory changes take these matters into consideration and by incorporating mechanisms that afford regulated parties procedural fairness including providing avenues for review or appeal.

Part 6 – Regulating the online environment, technology and environmental changes

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?

No comment

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

Regulations should focus on high-risk systems and platforms targeting the underlying cause. The current broad-brush framework covering all sections of the industry and in the case of the Online Content Scheme, utilising an unsuitable content classification scheme is fraught with risk of inhibiting innovation and interfering with end-user's privacy.

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?

No comment

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

No comment

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

No comment

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

No, the current governance structure is prone to overlap and duplication with multiple and overlapping regulatory frameworks in place dealing with online safety e.g. privacy, workplace health and safety, cybersecurity and eSafety. The current structures should be reviewed and streamlined or centralised.

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?

No specific comment but would note that a safe online environment is a shared responsibility of Government, industry and end-users.