Internet Society
Australia Chapter

Internet Australia

ABN 36 076 406 801

internet.org.au

Phone: **+61414366605/419603171**

Address: **PO Box 1705,**
North Sydney,
NSW 2059 Australia

Email: **info@internet.org.au**

February 13, 2021

Comment on the Online Safety Legislative Reform: Discussion Paper

Thank you for the opportunity to comment on this paper...

Internet Australia largely supports the proposed enhancements to the Online Safety Regime. We do, however, have two general concerns with the proposed changes.

The first is the proposed breadth of power of the eSafety Commissioner. Under the proposed scheme, the Commissioner would be given discretion to determine when content is not only illegal, but 'seriously harmful'. [page 41] The Commissioner would 'assess' content to 'determine' if it meets the definition of 'seriously harmful content' and may – but not must – have regard to the Classification Code. [page 41] Industry and the public should have clarity on what the term means and guidelines should be developed to provide a basis on which such determinations could be made. Providers should also be able to appeal such determinations.

The paper also suggests that:

> *… the eSafety Commissioner would have a power to determine by legislative instrument that the expectations apply to other specified types of service providers based on similar criteria to that required under the transparency reporting criteria, including numbers of reports received and response times to requests.[page 22]*

Later in the paper, there is reference to the Minister 'determining by legislative instrument' whether to exempt or exclude ancillary service providers. [page 53] It is assumed that the first reference to the eSafety Commissioner determining 'by legislative instrument' is a mistake, and that wherever the suggestion of determination by legislative instrument occurs, it would be the Minister doing so. If that is not the case, we believe it is totally inappropriate to suggest that the eSafety Commissioner be given what amounts to legislative power.

Our other general concern is addressing adult cyber bullying, now occurring through platforms as well. It has become almost as serious an issue for adults as it is for children, and should receive very close to the same level of concern as is given to child abuse material.

Our response to the individual questions asked in the Discussion Paper are below

> *1. Are the proposed high level objects appropriate? Are there any additions or alternatives that are warranted?*
>
> *2. Is the proposed statement of regulatory policy sufficiently broad to address online harms in Australia? Are there aspects of the proposed principles that should be modified or omitted, or are there other principles that should be considered?*

IA supports the inclusion of both Objects and a statement of Regulatory Policy in the proposed legislation. Both are important in interpreting the Act and providing guidance for industry, the public, and regulators. IA would add to the statement of Regulatory Policy that the proposed "practical measures" should be developed in close collaboration with the online service provider sector.

IA considers that the proposed high level objectives are appropriate and would add: to ensure complaint handling mechanisms are in place that are easily accessible and responsive.

> *3. Is there merit in the BOSE concept?*
>
> *4. Are there matters (other than those canvassed in the Charter) that should be considered for the BOSE? Are there any matters in the Charter that should not be part of the BOSE?*
>
> *5. What factors should be considered by the eSafety Commissioner in determining particular entities that are required to adhere to transparency reporting requirements (e.g. size, number of Australian users, history of upheld complaints)?*
>
> *6. Should there be sanctions for companies that fail to meet the BOSE, beyond the proposed reporting and publication arrangements?*

While there may be merit in the BOSE concept, IA struggles to see what additional value would be gained from having such an element in the new legislation. The issues which it appears to be canvassed are already very well encompassed within the Online Safety Charter and the proposed additional Objectives and Regulatory Policy. Having separate documents encompassing the same issues appears to us to be duplicative and potentially confusing.

As a general principle IA believes that the standards of transparency reporting requirements should be the same for all service providers. This is based on our view that, given that the scale and nature of the potential harm to users from cyber abuse, these are unlikely to be lessened by the scale of operation of the service provider. In this context, IA would not support the government adopting the model used by Germany where providers with more than two million users are subject to the transparency obligations.

It follows from this that IA advocates that transparency reporting mechanisms and requirements should be simple enough for small service providers to be able to implement. There may also be a case for regulatory forbearance to allow smaller service providers the time to become compliant with new reporting regimes.

The online service provider sector in Australia has a clear and strong history of close collaboration with the e-Safety Commissioner and IA would expect that this collaborative behaviour is likely to continue. On this basis, the Government should not rush to implement additional penalty measures unless a clear case for their necessity can be demonstrated.

7. Is the proposed expansion of the cyberbullying scheme for children to designated internet services and hosting services, in addition to relevant electronic service and social media services, appropriate?

8. Is the proposed take-down period of 24 hours reasonable, or should this require take-down in a shorter period of time?

9. What are the likely compliance burdens of the proposed changes to the cyberbullying scheme on small and large businesses?

10. What other tools could the eSafety Commissioner utilise to effectively address cyberbullying in the circumstances where social media service and end-user notices are not well suited to the particular service upon which the cyberbullying has occurred?

In principle, IA supports the expansion of the cyberbullying scheme to cover other relevant online services and the required takedown time shortened from 48 to 24 hours. However, a final response to the question will depend upon the frequency and complexity of the requirements that will be placed on smaller service providers and cannot easily be answered in the abstract. Clearly, there must be consultation with industry, particularly smaller providers, before the scheme is expanded.

11. Is the proposed application of the cyberbullying and cyber abuse schemes to designated internet services and hosting services, relevant electronic service and social media services, appropriate?

12. Is the proposed take-down period of 24 hours reasonable, or should this require take-down in a shorter period of time?

13. Do the proposed elements of a definition of adult cyber abuse appropriately balance the protection from harms with the expectation that adults should be able to express views freely, including robust differences of opinion?

14. Should the penalties differ under a cyber abuse scheme for adults and the cyberbullying scheme for children?

15. What additional tools or processes, in addition to removal notices, could be made available to the eSafety Commissioner to address cyber abuse occurring across the full range of services used by Australians?

The 24 hour time frame is reasonable and it is not clear that a shorter time frame would be possible. Again, this is a matter for consultation with industry.

IA supports the tighter definition of cyberbullying as it applies to adults. IA notes, however, that cyberbullying of adults can cause considerable harm to individuals and the scheme must provide sufficient mechanisms for an impacted individual to have the perpetrator identified and the bullying stopped.

The growing role of cyber bullying in cases of domestic violence in Australia is a development which needs to be of greater concern to governments. In this context, the government should revisit the question of sanctions against the perpetrator(s) of the bullying as well as issues relating to service providers.

> *16. Is the proposed take-down period for the image-based abuse scheme of 24 hours reasonable, or should this require take-down in a shorter period of time?*
>
> *17. Does the image-based abuse scheme require any other modifications or updates to remain fit for purpose?*
>
> *18. What additional tools or processes, in addition to removal notices, could be made available to the eSafety Commissioner to address image-based abuse being perpetrated across the range of services used by Australians?*

IA largely agrees with the current image based abuse scheme as it is currently formulated.

> *19. Is the proposed application of the take-down powers in the revised online content scheme appropriate?*
>
> *20. Are there other methods to manage access to harmful online content that should be considered in the new Online Safety Act?*
>
> *21. Are there services that should be covered by the new online content scheme other than social media services, relevant electronic services and designated internet services?*
>
> *22. Is the proposed take-down period of 24 hours for the online content scheme reasonable or should this require take-down in a shorter period of time?*
>
> *23. Which elements of the existing co-regulatory requirements should be retained under the new Act?*

IA notes that, in the commentary on the proposed changes, material that is 'seriously harmful' is said to be akin to material that is illegal. Further, there is suggestion that material could be declared as seriously harmful by legislative instrument, with the eSafety Commissioner having a role in the process. Using the process of declaring material by legislative instrument should only be exercised by a member of Parliament. Further, because such declaration will impact on a range of providers, it should only be done after consultation with stakeholders.

Again, shortening the 24 hour timeframe should only be done after consultation, particularly with smaller providers who may not have the requisite capacity to meet earlier timeframes.

IA supports the relevant code development process which ensures consultation with all relevant stakeholders.

> *24. To what extent would an expanded accreditation scheme for opt-in tools and services assist parents and carers in mitigating the risk of access by minors to potentially harmful content?*
>
> *25. What categories of tools and services should be included in an accreditation program, aside from content filters?*

26. What are the likely costs of developing and maintaining an accreditation scheme for opt-in tools and services to assist parents and carers in managing access to online content by minors?

27. When evaluating opt-in tools and services for accreditation, what criteria should be considered?

There are several arguments in favour of an expanded accreditation scheme for opt-in tools and services to assist parents and carers to mitigate the risk of access by minors to potentially harmful content. The first is simply that it would be consistent with the Government's Online Safety Charter which emphasizes the importance of user empowerment and autonomy and would potentially increase the pool of available tools and other resources. The second is that it would be likely to help to reinforce the impact and reach of the e-Safety Commissioners education efforts.

In the evaluation of tools, obvious criteria would include the effectiveness of the tools, their availability and the ease of their use by the public.

28. Is the proposed scope of content blocking for online crisis events appropriate?

29. Are there adequate appeals mechanisms available?

30. What other elements of a protocol may need to be considered?

The proposed scope of content blocking for online crisis events appears to be appropriate but the discussion paper leaves some serious questions unanswered. There is little or no discussion of what appeal mechanisms may be available to service providers when confronted with a mandatory notice. Nor is there any real discussion of what time limits may be placed on blocking actions or whether the mandatory blocks would become permanent. The paper goes on to say

"The notices would be subject to appropriate appeals, transparency and oversight arrangements to ensure the proper and appropriate use of the power[page 51]" but gives no explanation as to what these might be or to how they would be developed.

Other elements that may need to be considered should include at the very least, some form of appropriate, independent appeals mechanism separate from the office of the e-Safety Commission.

At the voluntary notice level, a system of protocols should be developed in collaboration with industry service providers which would obviate the need to resort to mandatory notices.

31. Is there merit in the concept of an ancillary service provider notice scheme?

32. Are there any other types of services that should be included in the definition of ancillary service provider?

33. Should the definition of search engine provider be broadened to include search functions housed in other services, such as social media services, video hosting services or other services with internal search functionality?

34. Is the requirement that 3rd parties be systemically and repeatedly facilitating the posting of cyberbullying or cyber abuse material, image-based abuse or hosting illegal or harmful content appropriate before the eSafety Commissioner can issue a notice to an ancillary service provider? Should a different threshold be contemplated?

35. Is there merit to making compliance with the ancillary service provider notices mandatory?

IA does support the concept of an ancillary service provider notice scheme, as suggested.

This question on the definition of search engine provider is too vague to have practical application. At some point arbitrary boundary judgements would have to be made if this were to be practically applied and IA considers that such arbitrary judgements should be avoided in the scheme's development.

The proposed threshold is appropriate, but not be made mandatory at this stage.

36. Are the eSafety Commissioner's functions still fit for purpose? Is anything missing?

37. To what extent should the existing functions of the eSafety Commissioner be streamlined? Are there particular functions that need to be maintained, or new functions that should be specified?

38. To what extent should the functions of the eSafety Commissioner be prioritised?

39. What are the likely impacts, including resource implications, on other agencies and businesses of a new Online Safety Act?

At this stage, IA has no further comment on the last set of questions. However, this last section of the paper again raises the issue of the governance arrangements being considered by the Government for the Office of the eSafety Commissioner. IA has already commented in another context that the Office should remain within the ACMA. Given the role of both the ACMA and the Office of the eSafety Commissioner is about electronic communications, and the obvious overlap in jurisdiction, it would make both resource and policy sense that they remain part of the same agency.

SIGNED

Chair Policy Committee Internet Australia Board

About Internet Australia

Founded in 1996, Internet Australia (Internet Society of Australia, ACN 076 406 801; also formerly known as 'ISOC-AU') is the not-for-profit peak organisation representing all Australian Internet users. We are a broad member-based organisation not an industry lobby group.

Our mission – "Helping Shape Our Internet Future" – is to promote positive Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our directors and members hold significant roles in Internet-related organisations and enable us to provide high level policy and technical information to Internet user groups, governments and regulatory authorities.

As the Australian chapter of the global Internet Society, Internet Australia leverages the expertise of a truly global network of experts as well as providing an Australian perspective on global issues. At a global level, the Internet Society is a very active participant in many international forums for policy and regulation development, and is the administrative home for the Internet Engineering Task Force (IETF): the open community of network designers, operators, vendors, and researchers who create the protocols and standards that are fundamental to Internet operation.