9 September 2022
Attorneys-General
Review of Model Defamation Provisions
Policy Reform & Legislation
Department of Communities and Justice
By email: defamationreview@justice.nsw.gov.au

Stage 2 Review of the Model Defamation Provisions – Part A
eSafety Commissioner submission

Dear Attorneys-General,

As Australia's eSafety Commissioner, I welcome the opportunity to provide a submission to the Stage 2 Review of the Model Defamation Provisions – Part A Exposure Draft Amendment Provisions (**Draft Amendments**) and Background Paper (**Paper**).

eSafety is Australia's national independent regulator for online safety. Our core objective is to minimise harm to Australians online.

As you may know, eSafety has been engaging closely with the Defamation Working Party on this reform process.

Our submission focuses on the intersection, and at times overlap, between aspects of eSafety's remit under the *Online Safety Act 2021* (**OSA**), particularly the adult cyber-abuse scheme and section 235 of the OSA, and the Draft Amendments.

Adult Cyber-Abuse Scheme and relationship with defamation

Following an extensive consultation and legislative reform process, the OSA commenced in January 2022. This has expanded eSafety's powers and functions, thereby improving the effectiveness, reach and impact of our work.

Amongst other things, the OSA creates a complaints scheme relating to cyber-abuse targeted at an Australian adult. The OSA defines adult cyber-abuse as material targeting a particular Australian adult that is both:

- intended to cause serious harm, and
- menacing, harassing or offensive in all the circumstances.

This adult cyber-abuse scheme operates separately to defamation law.

In eSafety's view, potentially defamatory material that causes purely reputational harm is not enough to meet the adult cyber-abuse threshold of intending to cause serious harm. This is supported by the Explanatory Memorandum to the OSA, which states that the definition of cyber-abuse material 'is not intended to capture 'reputational harm' caused by defamatory material, for example negative online reviews of businesses.'

However, there may be some instances where defamatory material is also assessed as adult cyber-abuse where it can be established that the material was intended to cause serious harm, and it was menacing, harassing or offensive in all the circumstances.

Importantly, where potentially defamatory material is found to be adult cyber-abuse, eSafety takes action on the basis that the material is adult cyber-abuse, and not on the basis that it is potentially defamatory. As such, eSafety does not consider whether any defences may apply

under a defamation cause of action, as this is not necessary or applicable within the context of adult cyber-abuse.

eSafety notes that in many cases the goal of complainants under both defamation law and adult cyber-abuse scheme is the same: to have the online content removed and, as expected, eSafety has found there are incentives on complainants to pursue a matter under the framework of the OSA given the speed and accessibility of redress eSafety is able to provide under our scheme.

Under Part 7 of the OSA, the eSafety Commissioner may require the removal of adult cyber-abuse material by a social media service, a relevant electronic service, a designated internet service, an end-user or a hosting service provider within 24 hours from receipt of a removal notice from eSafety. The Draft Amendments place a 14-day time limit for actions in response to a complaints notice. These very different time frames make the adult cyber-abuse scheme more favourable to complainants who want the content removed. To note, failure to comply with a removal notice can lead to a civil penalty of up to 500 penalty units. eSafety may also consider several other enforcement options.

Since the commencement of the OSA on 23 January 2022 until 30 June 2022, roughly 35 per cent of adult cyber abuse complaints made to eSafety were assessed as involving potentially defamatory material. The vast majority of these complaints were assessed as intending to cause purely reputational harm and therefore did not meet the adult cyber-abuse threshold.

It is also important to note that the processes are fundamentally different in nature, with defamation a private cause of action between individuals, whereas eSafety provides a government safety net for the removal of seriously harmful online content targeting Australians.

Proposed considerations for Attorneys-General

While the two schemes are independent, there are interdependencies between how the schemes may operate in practice, in instances where both schemes are dealing with the same piece of material. eSafety will continue to administer its schemes with independence, proportionality and in line with its own legislative framework. However, we are raising the below considerations for the Attorneys-General to consider to ensure the schemes don't have the practical effect of undermining or conflicting with each other.

Questions that we would encourage the Attorneys-General to consider include:

- If eSafety issues a removal notice, which requires material to be removed within 24 hours, how would this affect the timeframes under a defamation cause of action?
- If content is removed under eSafety's adult cyber-abuse scheme, how would such removal affect any cause of action under defamation law and the complainant's prospects for damages?
- What is the impact of removal of the potentially defamatory content that is the subject of a complaints notice under another scheme (such as the regulatory schemes under the OSA) on the defences proposed in recommendation 3A and 3B?

In order to address these concerns, we suggest that language be included in either the Draft Amendments or the explanatory memorandum accompanying the amendments to ensure litigants understand how the Draft Amendments would operate if action is taken by eSafety or others, including content removal, under a different regulatory scheme.

More broadly, eSafety encourages the Attorneys-General to consider ways of making defamation redress more accessible. In addition to the speed and efficiency of eSafety's processes, some complainants may come to eSafety seeking removal of material because the cost of a defamation cause of action is prohibitive. Providing accessible and financially affordable legal support, such as through funding for community legal centres to assist people with a defamation action, may contribute towards complainants availing themselves of the scheme most suited to their needs.

Recommendation 1 and 2

In eSafety's view, it appears that if recommendations 1 and 2 are implemented, there would be no incentive for those exempted to respond to a complaints notice, as proposed in recommendations 3A and 3B. From eSafety's experience, hosting service providers can perform an important role in the removal of online material. Exempting hosting service providers does not incentivise them to assist complainants.

Recommendation 3A and 3B

In eSafety's view, recommendation 3A does not appear attractive to a complainant who wants material removed and does not want to commence proceedings for reasons such as cost and publicity etc. Recommendation 3B appears to be a more effective route to achieve the outcome most complainants are seeking which is for the removal of the defamatory material without the expense of litigation.

Further, recommendation 3B aligns much more closely with eSafety's effective regulatory schemes which can lead to the removal of harmful content on receipt of a report.

We believe it may be preferable for both models or a 'hybrid model' to be considered that allows the complainant to choose from the options based on their individual position and desired outcomes.

We also note that regardless of the final approach, there are potential privacy concerns that need to be considered with digital platforms handling, verifying and safely securing personal information, including for the purposes of disclosing the personal information of end users to complainants who allege defamation.

eSafety notes that we raised these concerns, as well as broader policy and thematic issues that may be of relevance and interest to Attorneys-General, in its submission to the *Social Media (Anti-Trolling) Bill* consultation of the Senate Legal and Constitutional Affairs Committee.

The Online Safety Act Immunity

As identified in the Paper, section 235(1) of the OSA (OSA Immunity) substantially replicates and replaces the immunity under the *Broadcasting Services Act 1992*, providing:

(1) A law of a State or Territory, or a rule of common law or equity, has no effect to the extent to which it:

(a) subjects, or would have the effect (whether direct or indirect) of subjecting, an Australian hosting service provider to liability (whether criminal or civil) in respect of hosting particular online content in a case where the provider was not aware of the nature of the online content; or

(b) requires, or would have the effect (whether direct or indirect) of requiring, an Australian hosting service provider to monitor, make inquiries about, or keep records of, online content hosted by the provider; or

(c) subjects, or would have the effect (whether direct or indirect) of subjecting, an internet service provider to liability (whether criminal or civil) in respect of carrying particular online content in a case where the service provider was not aware of the nature of the online content; or

(d) requires, or would have the effect (whether direct or indirect) of requiring, an internet service provider to monitor, make inquiries about, or keep records of, online content carried by the provider.

The OSA Immunity will only have effect to the extent that a service is a hosting service provider or internet service provider and:

a) the platform is unaware of the nature of the content; or
b) the requirement would be for the provider to monitor make enquiries about or keep records of online content

Once a provider is made aware of a defamation complaint notice, the immunity afforded under section 235 will cease to apply. However, immunity from a requirement to make inquiries or keep records continues for both a hosting service provider and an internet service provider.

eSafety agrees that the Draft Amendments would not offend and are consistent with the law and policy of the reforms of section 235 of the OSA.

We note the Minister could exempt defamation legislation from falling within the scope of section 235. This declaration could occur through a legislative instrument or with amendments to the OSA. This power sits with the Minister and is the responsibility of the Department of Infrastructure, Transport, Regional Development, Communications and the Arts. While this is a matter for the Minister and Department, eSafety is of the view that this is not necessary as it would not change the operation of the OSA Immunity.

Concluding remarks

As eSafety has stated previously, a coordinated approach between intersecting regulatory schemes is important. While we believe defamation law and the adult cyber-abuse scheme can work in a complementary manner, we also believe it is important to be cognisant of the legislative and operational overlaps.

eSafety's regulatory experience, including the insights gained from administering the adult cyber-abuse scheme since January 2022, underpin and support the points we have put forward in this submission.

Ultimately, eSafety advocates a multi-layered and whole of community approach to online safety in which individuals, organisations, industry players and government have a role to play.

My office and I are happy to provide any further information that would be of assistance.

Yours sincerely,

[redacted]

Julie Inman Grant
eSafety Commissioner