COMMUNICATIONS ALLIANCE LTD

COMMUNICATIONS ALLIANCE SUBMISSION

to the

Meeting of Attorneys-General:
Stage 2 Review of the Model Defamation Provisions
Part A: liability of internet intermediaries for third-party content

Background Paper: Model Defamation Amendment Provisions 2022 (Consultation Draft)

and

Parliamentary Counsel's Committee - Draft d17 Model Defamation Amendment Provisions 2022

16 September 2022

TABLE OF CONTENTS

INTRODUCTION

Communications Alliance welcomes the opportunity to make this submission in response to the Meeting of Attorneys-General Background Paper *Model Defamation Amendment Provisions 2022 (Consultation Draft) and the* Parliamentary Counsel's Committee - Draft d17, *Model Defamation Amendment Provisions 2022* (MDAPs) as part of the Stage 2 Review of the Model Defamation Provisions, Part A: liability of internet intermediaries for third party content.

We acknowledge the substantial work of the Attorneys-General working party in the course of the reform process and welcome that some of our feedback has already been incorporated into the draft MDAPs.

Members of Communications Alliance may make individual submissions.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

About Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see http://www.commsalliance.com.au.

1 STATUTORY EXEMPTIONS FOR A NARROW GROUP OF INTERNET INTERMEDIARY FUNCTIONS, RECOMMENDATIONS 1 & 2

Recommendation 1:

1.1 Recommendation 1 proposes a statutory exemption from defamation for mere conduits, caching and storage services subject to the intermediary not taking certain actions in relation to the matter (e.g., encouraging, editing or promoting the matter).

1.2 The proposed statutory immunity would be available irrespective of whether the intermediary is aware of the allegedly defamatory content or not.

1.3 The draft MDAPs make clear that such an intermediary's compliance with a Commonwealth, state or territory law does not preclude that intermediary from access to the exemption.

1.4 We support the proposed exemptions being applied to mere conduits, caching and storage services, including internet service providers (ISPs), cloud storage services and email services.

1.5 This exemption recognises that where internet intermediaries play a passive role (subject to legal and regulatory obligations, also see our comment at paragraphs 1.7 ff below) in the facilitation of a publication, they should not be liable.

1.6 We also welcome that the exemption would apply irrespective of whether the internet intermediary is made aware of the allegedly defamatory content, as the awareness of the material does not improve or increase the intermediary's abilities to remedy the situation. The remedies available to the intermediary are usually limited, ineffective or can be easily circumvented, and/or would involve blunt and drastic tools with potentially far-reaching consequences beyond the intended removal of the allegedly defamatory content (e.g., cutting off their services to an entire organisation).

1.7 The new Section 9A(2) clarifies that intermediaries can continue to benefit from the exemption, and that the condition in Section 9A(1)(c) that intermediaries not take action in relation to the content (e.g., editing or promoting the content, etc.) does not apply, where the "action [is] taken because it is required by a law of an Australian jurisdiction".

1.8 However, this clarification does not adequately capture the full range of regulatory obligations that intermediaries may need to comply with. The communications sector, in particular, largely operates under a co-regulatory regime, and important sector-wide arrangements are being implemented through various industry Codes and Standards which are enforced by the respective regulators.

1.9 The *C661:2022 Reducing Scam Call and Scam SMS Industry Code* (registered and enforced by the Australian Communications and Media Authority) and the draft *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material)* currently released for public comment and (if registered) enforceable by the eSafety Commissioner are examples of co-regulatory instruments that could require intermediaries to take action in respect of third-party content they carry (e.g., using technical identifiers to 'prioritise' internet traffic).

1.10 However, these Codes do not constitute law, and are only two examples that highlight the general issue with respect to co-regulatory instruments. Communications Alliance has developed, and continues to develop, numerous Codes and Standards that facilitate the operation and interworking of communications networks. Given the

dynamic nature of technology and the rather slow pace of legislative processes, we strongly recommend the inclusion of co-regulatory instruments in Section 9A(2).

1.11 Additionally, we note that the role of internet domain hosts and internet domain name registries and registrars as internet intermediaries has not been clarified. Consider the scenario where a person (the originator) chooses to register a domain name such as www.thiscontentisclearlydematory.com.au. During the registration process, the domain would be checked for availability (i.e., whether such a domain already exists) but not as to whether the domain name itself makes a defamatory statement. Consequently, the domain, if still available, would subsequently be registered by a domain name registrar and hosted by a domain name host. Neither of these two internet intermediaries have any role in the publication and are completely passive. They both ought to be afforded the same conditional, statutory exemption as mere conduits, caching and storage services.

Recommendation 2:

1.12 Recommendation 2 proposes a conditional, statutory exemption from defamation for standard search engine functions.

1.13 The new Section 9A(3)(a), however, limits that statutory exemption to "to search results generated using the search engine from search terms inputted by the user of the engine rather than terms automatically suggested by the engine".

1.14 We support the exemption for search engine functions. The publication of search results is driven by the user conducting a search query, and the user is the sole recipient of the results generated by their search query. The search engine has no interest in the content, it merely provides the search function via an automated process and provides access to third party content. Importantly, as indicated in previous submissions, it cannot remove the content in question from the internet and the effectiveness of the tools to remedy the situation is debatable, depending on the circumstances and virality of the content.

1.15 However, we note with concern that the proposed exemption does not include auto-complete functions. Search terms that are auto-completed are highly beneficial to users as they help save time and, importantly, avoid or correct spelling mistakes, for a search that they already intended to undertake.

1.16 This is especially true on mobile devices where inputting search terms is more cumbersome and more prone to spelling mistakes due to 'fat fingers'. We note that already today, it appears that more than two thirds of all searches in Australia are completed on mobile devices.[1]

1.17 It is also not clear how the proposed MDAPs intend to deal with search terms inputted via voice recognition software where the search term may not have been recognised by the software (for example due to an accent, speech impediment or disability) and, consequently, the software returns a suggestion for a search term that the user then can accept or reject.

1.18 The results generated in response to auto-completion, either after a keyboard input or a voice prompt, are the same that would have been generated if the user had typed the search term or used the correct voice prompt (the user may have even used the

[1] Refer to https://www.sistrix.com/blog/the-proportion-of-mobile-searches-is-more-than-you-think-what-you-need-to-know/ as accessed on 9 Sept 2022. We understand that the figures reported under the heading "Almost two thirds of all searches are already carried out on the mobile phone" constitute an average across the countries evaluated in the sample and appear to exclude Australia. However, given Australia's very high smart phone penetration (one of the highest in the modern world), it appears likely that Australia would not deviate from the average or, if so, only upwards.

correct prompt, but it may not have been recognised due to accent, speech impediment or disability!).

1.19 Consequently, it appears that the exemption from immunity for search terms that are suggested by the search engine would be of limited utility to the allegedly defamed person but potentially result in a significant loss to all users as search engines would be incentivised to limit the use of and innovation in such functionalities, given the potential high stakes involved with a case brought against a search engine for an allegedly defamatory matter where a search result had been presented through a suggestion by the search engine. Therefore, we ask that search results suggested by the search engine not be excluded from the statutory immunity.

2 TWO ALTERNATIVE OPTIONS FOR A NEW DEFENCE FOR INTERNET INTERMEDIARIES, RECOMMENDATIONS 3A & 3B

2.1 We have highlighted in previous submissions the challenges for intermediaries to adjudicate claims over allegedly defamatory content, particularly in general public debate and movements, such as Black Lives Matter or the #MeToo movement, that are of considerable public benefit.

2.2 Consequently, any legislative change has to carefully consider to what extent it incentivises intermediaries to over-remove content in order to minimise exposure to potential litigation.

2.3 Recommendation 3A proposes to create a safe harbour for internet intermediaries (those that do not meet the conditions for statutory exemption under the new MDAP 9A), with the purpose of focusing the dispute between the complainant and the content originator. Recommendation 3B, in contrast, does not prevent claims against intermediaries where the original poster is identifiable.

2.4 Therefore, of the two alternatives, Recommendation 3A bears slightly less risk of over-removal of content and we lend our support to this Recommendation. In the following, we focus our comments on key issues with that Recommendation.

2.5 Under the proposed Section 31A, Recommendation A, the internet intermediary automatically has a complete defence if the complainant knew the originator's identity or with 'reasonable steps' available to an ordinary person could have identified the originator.

2.6 We ask that 'reasonable steps' be more clearly defined in the MDAPs themselves. Doing so will avoid unnecessary disputes and provide certainty for complainant and defendants alike.

2.7 'Reasonable steps' in this context should be clearly defined to mean the complainant doing at least all of:

- searching in online and offline directories for information regarding the originator; and
- attempting to contact the originator directly through online methods (such as the chat or comment functions on which the originator has previously communicated).

If contact has been made:

- The complainant should wait at least a week for a response.
- If the originator responds but the complainant's concerns are not resolved, the complainant could be given a right to substituted service using the same contact method (for example, by email). This should not be used as the basis for escalating the complaint to the subordinate third party.

2.8 Following on from the above, Section 31A(3), Recommendation A, also ought to include a requirement for the complainant to set out in the complaints notice the 'reasonable steps' that the complainant has taken to identify the originator.

2.9 Section 31A(3)(b)(ii), Recommendation A, should also be amended to specify that the details of the location where the matter could be accessed must include the webpage address (URL). The current drafting only specifies the identification of the URL as a suggested example rather than a compulsory detail to be included, when in reality it is most likely a technical necessity. Additionally, the section should require the notice to specify other information that would allow the intermediary to accurately identify the matter itself (e.g., listing a URL containing several blog posts, without further identifying which blog post is the offending one, will not allow the intermediary to identify the offending blog post).

2.10 Failing to include a requirement for plaintiffs to include such information in their complaints notices to allow the intermediary to identify the location of the matter and the matter itself will likely lead to disputes as to whether a valid complaints notice has been served. We note that a similar approach (of requiring sufficient identification of the relevant matter) has been taken in the *Online Safety Act 2021* (OSA) for removal notices, see for example, OSA Section 77(2), 78(2), 79(2), 88(2), 89(2), and 90(2).

3 PROPOSED ADDITIONAL LIMITATION OF LIABILITY FOR GOOD FAITH ACCESS PREVENTION STEPS TAKEN BY INTERMEDIARIES

3.1 Under the proposed Section 31A, Recommendation A, the internet intermediary also has a complete defence vis-à-vis the complainant if the intermediary removes, blocks, disables or otherwise prevents access to the matter (depending on what may be reasonable in the circumstances). However, vis-à-vis the originator of the matter, the intermediary could still be exposed to civil liability (e.g., under a contractual obligation between the intermediary and originator to post or disseminate the content) for taking down or disabling access to the content.

3.2 We accordingly recommend that a further limitation of liability be incorporated into the MDAPs to the effect that an intermediary will not be liable for damages or any other civil remedy as a result of the intermediary taking any good faith access prevention steps in relation to the publication of the matter (whether pursuant to a complaints notice received under Section 31A(1)(c) or of its own accord). We note that there is precedent for such limitation of liability in Australia's copyright regulatory framework[2].

4 CLARIFY INTERACTION WITH THE ONLINE SAFETY ACT IMMUNITY, RECOMMENDATION 4

4.1 Section 91(1) of Schedule 5 to the *Broadcasting Services Act 1992* provided an immunity for 'internet service providers' and 'internet content hosts' in certain circumstances in relation to third-party material. The OSA substantially replicates and replaces this immunity and defines 'Australian hosting service provider' as 'a person who provides a hosting service that involves hosting material in Australia'.

4.2 We note that if Recommendation 1 is introduced (a conditional, statutory exemption from defamation liability for mere conduits, caching and storage services), this would

[2] Specifically, under Section 37 of the Copyright Regulations 2017, read with Section 116AJ of the Copyright Act 1968.

make the application of the OSA immunity to these internet intermediary functions irrelevant in the context of defamation law.

4.3 The Background Paper notes that "[i]n relation to caching and storage service providers, it appears they may they fall within the definition of 'Australian hosting service provider' in the OSA Immunity"[3]. We agree that this is likely to be true for storage service providers but are less sure that this is the case for mere caching service providers which, if captured at all, may be more likely considered a 'designated internet service provider' under the OSA and, therefore, not be afforded immunity from liability under Section 235 of the OSA.

4.4 The Background Paper notes discussions from submissions as to whether the term 'Australian hosting service provider' as used in the OSA could be interpreted to include 'forum administrators':

> "Stakeholders noted that there is uncertainty as to the scope of the term 'Australian hosting service provider' as used in the OSA. If this term were interpreted to cover a broader range of functions (for example, a forum administrator) – there would be some overlap between the OSA Immunity and the new safe harbour or innocent dissemination defence."[4]

In our opinion (and as the co-drafters of the Online Safety Codes currently released for public consultation) we note that 'forum administrators' would not necessarily fall under the definition of 'Australian hosting service provider' but rather fall under the definition of 'designated internet service providers' and/or 'social media service provider' under the OSA.

4.5 The above highlights that further work on the interaction of the OSA immunity with defamation law is required as it is, in our view, undesirable to create different regimes with different definitions and immunities. (Also refer to our comments at paragraphs 5.3-5.5.)

5 CLARIFICATION AND ENHANCEMENT OF COURT POWERS, RECOMMENDATION 5

5.1 Recommendation 5 proposes a new power for courts to order a non-party to the proceedings to "take the steps the court considers necessary in the circumstances […] to prevent or limit the continued publication or republication of the [defamatory] matter […]".

5.2 We are concerned with the breadth of the suggested language as it could be interpreted to imply an obligation for the intermediary to monitor the internet for resurfacing of the defamatory content or variations thereof.

5.3 Sections OSA 235(1)(d) expressly states that a state or territory law must not impose a duty on an immunised internet intermediary to actively monitor, make inquiries about, or keep records of third-party online content. The OSA included this provision as a result of an intense policy debate which sought to ensure that private organisations are not

[3] p.45, Meeting of Attorneys-General Background Paper Model Defamation Amendment Provisions 2022 (Consultation Draft), Aug 2022
[4] p.46, Meeting of Attorneys-General Background Paper Model Defamation Amendment Provisions 2022 (Consultation Draft), Aug 2022

placed in a position where they could be forced to monitor, on an ongoing basis, the internet for specific content.

5.4 It is, in our view, irrelevant whether the monitoring obligation arises from a legal obligation or from a court order.

5.5 Consequently, we believe that Section 39A ought to require that the court order must specify that the location be identified in a manner that is sufficient to enable the intermediary to identify the location of the publication, such as a webpage address (URL), and that no ongoing monitoring and removal obligation arises. This would align the MDAPs with the intent of the OSA.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507