CENTRE FOR MEDIA TRANSITION

Model Defamation Amendment Provisions 2022 (Consultation Draft)

Stage 2 Review of the Model Defamation Provisions. Part A: Liability of Internet Intermediaries for Third Party Content

Submission to Meeting of Attorneys-General

16 September 2022

About the Centre for Media Transition

The Centre (CMT) was established in 2017 as an applied research unit based at the University of Technology Sydney (UTS). It is an interdisciplinary initiative of the Faculty of Arts and Social Sciences and the Faculty of Law, sitting at the intersection of media, journalism, technology, ethics, regulation, and business.

Working with industry, academia, government and others, the CMT aims to understand media transition and digital disruption, with a view to recommending legal reform and other measures that promote the public interest. In addition, the CMT aims to assist news media to adapt for a digital environment, including by identifying potentially sustainable business models, develop suitable ethical and regulatory frameworks for a fast-changing digital ecosystem, foster quality journalism, and develop a diverse media environment that embraces local/regional, international and transnational issues and debate.

This submission was prepared by:

- Professor Derek Wilding, Co-Director, Centre for Media Transition
- Dr Sacha Molitorisz, Senior Lecturer in Law, Centre for Media Transition
- Dr Michael Davis, Research Fellow, Centre for Media Transition

CONTACT

Centre for Media Transition
University of Technology, Sydney
PO Box 123, Broadway NSW 2007

cmt@uts.edu.au
+61 2 9514 9669

cmt.uts.edu.au

Introduction and summary

Thank you for the opportunity to contribute to this review. This submission follows the structure of the Background Paper, responding to the Recommendations.

For us, one of the most important aspects of the reforms concerns the changes to treatment of third party comments on the websites and social media pages of news organisations. In short, this involves removing the liability that has arisen as a result of the decision in *Fairfax v Voller* [2021] HCA 27. We understand it is intended this would be covered by either Recommendation 3A or 3B. Our view on this is as follows:

- We favour an approach that combines a safe harbour where the identity of the poster can be ascertained with the extended defence of innocent dissemination where the safe harbour does not apply. In addition, we would like to see the safe harbour extended to cover situations where the intermediary presents the parties with a forum for resolving the matter through means such as alteration or removal of the content or publication of a correction or apology. Our view is that, whatever else the Stage 2 reforms achieve, they should help push intermediaries towards establishing a process for complainants to easily submit complaints notices.

Some further key points we make in this submission are as follows:

- We support the proposal for 'mere conduits' (including ISPs), caching services and data storage services to be given an immunity that stops them from being characterised as publishers.
- We support the proposal for an immunity for search results.
- While we support clarification by the Commonwealth of the application of the immunity in the *Online Safety Act 2021* (Cth), we would need to see the final form of amendments to the Model Defamation Provisions before supporting any narrowing of the immunity.

As a more general comment, we wish to signal our support for the attempt by the Defamation Working Party (DWP) to address some complex problems presented by evolving technologies and markets. In particular, we agree with the following statement:

> Given the fast-evolving nature of technology and the time it takes courts to deal with the issues that new and emerging forms of communications bring with them, the case law on the treatment of internet intermediary liability for third-party content in Australia is unsettled and disparate. The role of internet intermediaries in publication, and their ability to avail themselves of the innocent dissemination defence, is an evolving issue (Background Paper, p.31).

While we acknowledge that these evolving technologies, products and services can bring harms for users of online platforms, we reject the idea put by some that protection from some aspects of defamation law should not be offered to 'tech giants'. Although we urge the DWP to set aside some of the intermediaries' own objections – for example, concerns about becoming a 'go-between' in the proposed complaints notice process – it should be recognised that digital intermediaries bring substantial benefits to the community, such as enhanced opportunities for communications and public speech, as well as some significant risks. And crucially, in addressing these risks – while we still have the opportunity to achieve some consistency in treatment of online content and service providers – defamation law needs to work alongside privacy law, regulation of disinformation, the regulatory schemes in the Online Safety Act, the News Media Bargaining Code and more. We also need to be alert to the possibility of overreach on the part of defamation law, when problems are more appropriately addressed by other areas of law. Rather than inconsistent and tangled, defamation reforms ought to aim to be coherent and complementary.

Responses to Recommendations in the Background Paper

Recommendation 1: Mere conduits, caching and storage services

Conditional, statutory exemption from defamation liability for mere conduits, caching and storage services

This protection in s 9A(1) of the MDAPs applies regardless of the knowledge of the service provider of the defamatory content. The immunity is proposed on the basis that the intermediary did not (among other things) initiate publication, edit the content or 'encourage the poster of the matter to publish the material'.

We support the proposal for 'mere conduits' (including ISPs), caching services and data storage services to be given an immunity that stops them from being characterised as publishers. We think this is a proportionate approach and a more efficient way of enabling these intermediaries to provide their services without being first deemed to be a publisher and then needing to establish a defence.

However, we note the concerns of our colleagues at Macquarie University Law School (see submission from Dr Harry Melkonian) on the ambiguity in the concept of 'encouraging' posters to make comments. We agree with their observation that 'If it means nothing more than providing a blank space with words saying something to the effect, "place your comments here" then almost anything will amount to legal encouragement.' Accordingly, we support their suggestion that 9A(1)(iii) be deleted.

Recommendation 2: Search engines

Conditional, statutory exemption from defamation liability for standard search engine functions

As with Recommendation 1, this protection would apply regardless of the knowledge of the service provider of the defamatory content. But it will only apply to the results of the 'automated process for the user to generate the search results' where the user enters the search terms (not where the search engine uses auto-complete in entering the search terms). It does not apply where the search results are 'promoted or prioritised by the search engine provider because of a payment or other benefit'.

We support in principle the proposal for an immunity for search results. Specifically:

- we support the idea that search engines should not be liable for URLs supplied or even for snippets (ie, 'short extracts') or images taken from webpages and included as part of automated search results;
- we support the limitation on the exemption in MDAP s 9(4) which excludes commercially promoted search results, although we note that it may be difficult to know whether commercial arrangements are in place (adding to the rationale for some more general form of regulatory oversight of algorithmic practice, separate from defamation law).

However:

- we do not support the limitation in the exemption found in MDAP s 9A(3)(a) which excludes auto-suggested search terms.

As our Macquarie colleagues note, imposing liability where search engines use auto-complete does not reflect how search engines operate.

We also note some suggestions have been made for amendments to draft s 9A(3) and (4); for example, clarification of 'short extract' and ensuring that 'promoted' does not include ranking of search results on grounds other than revenue to the intermediary. We think it is reasonable that the MAG consider these suggestions.

In addition, we think it would be desirable for search engines to be required to offer an accessible complaints system in order to gain the benefit of the immunity. We do not suggest something in the same terms as the complaints notice system in the MDAPs, as we do not see this tied to facilitating defamation actions. But there will be circumstances where users wish to challenge the content of search results; requiring search engines to provide an easily accessible complaint channel could assist in the resolution of matters concerning defamation as well as other content. We have recently published research on dispute resolution by social media providers; some of the same principles can apply to search engines. Encouraging intermediaries to adopt standards for internal complaint handling and submitting to some form of escalated external complaint handling, for example, would have benefits beyond potentially defamatory content, but it is important that amendments to defamation law do not preclude reforms in other areas.

We have also previously argued that a right to erasure should be introduced into law, and specifically into the *Privacy Act 1988* (Cth). (See pp 18-19 of our 2020 submission to the Attorney-General's Department on the Privacy Act Review Issues Paper). The introduction of the right to erasure in Australia would mean that individuals would be able to request that search engines such as Google remove certain specified links from being returned when searches are conducted. This would enable some defamatory material to be removed, as well as some other material that ought not be returned. In Europe, the right to erasure was codified with the implementation of the GDPR in 2018, and has not imposed unreasonable regulatory or financial burdens. The introduction of a right to erasure in Australia would ensure that digital platforms are made to be more responsible and accountable for the personal information they hold, and its introduction would be even more desirable if search engines were to be given a statutory exemption from defamation liability.

Recommendations 3A and 3B: Social media, forum administrators etc including online news sites – liability for third-party content

Two alternative options for a new defence for internet intermediaries:

- **Model A – safe harbour**
- **Model B – extended defence of innocent dissemination**

The Background Paper offers two approaches intended to provide some level of protection to social media, forum administrators and others who publish third party content. Importantly, this would indemnify news media in relation to comments made by readers in response to the articles a news publisher posts on its own website or on its social media pages. It would not apply to the news articles themselves. Accordingly, it would address the problem seen in *Fairfax v Voller*, in which the High Court found that news publishers were liable for third party comments.

We note recent commentary stating that the MDAPs would not apply as intended – that they would cover social media services such as Facebook, but not forum administrators (such as the news media publishers who operate Facebook pages or provide comments streams on their own sites). **If the drafting of the MDAPs (for example the definition of 'digital intermediary') does not adequately cover forum administrators including**

news publishers in respect of third party comments, we urge the DWP to revise the draft MDAPs to ensure that it does provide the intended coverage.

As noted, the MDAPs offer two (alternative) approaches to providing this protection for social media services and forum administrators. The Background Paper provides a good example of how the approaches differ. It gives the scenario where someone on social media (let's say it's Facebook) under their own name posts defamatory comments about someone who is a business competitor. The safe harbour approach prevents the defamed party bringing an action against Facebook (it only permits an action against the poster of the comment) whereas the extended innocent dissemination defence allows an action against Facebook, which Facebook can then defend under innocent dissemination if it chooses.

We think both approaches have some commendable elements and some flaws. We deal with these below. On the whole, we prefer Model A (the safe harbour) to Model B (the innocent dissemination defence) although we would like to see:

- an extension of the safe harbour in situations where the intermediary provides a forum for resolution of the matter by the two parties; and
- a combination of the two approaches so that the innocent dissemination defence can be applied in situations where the safe harbour does not apply.

Commendable elements of these approaches

To us, the principle underpinning the safe harbour approach is perfectly reasonable. In the example above, Facebook – which has had no editorial input into this interaction – should not be liable. This approach encourages freedom of expression more generally while still allowing a defamed person a remedy.

More specifically, the safe harbour in Model A includes a requirement that complainants try to ascertain the identity of the person who posted the material. We support this as we think the digital intermediary should not be sued where the person responsible for posting the material is known.

There is also a requirement that online intermediaries establish a process for complainants to easily submit complaints notices. Our recent research on digital platform complaints handling has led us to the view that whatever else the Stage 2 reforms achieve, they should help push intermediaries towards establishing such facilities.

It was also good to see the Background Paper acknowledge the point made by many submitters that an intermediary that receives a complaints notice will lack contextual information and should not be forming a view on the merits of a complaint.

In the extended innocent dissemination defence in Model B, it was good to see an attempt to resolve the two known problems that encourage takedown: clarification of which types of internet intermediaries would be considered 'subordinate distributors'; and clarification of whether mere notification or knowledge of a claim of defamation is required (with actual notice following receipt of a complaints notice).

Flaws of these approaches

In our view, the safe harbour model offered in the paper is flawed in its treatment of circumstances where the identity of the originator cannot be easily ascertained. Further, both the safe harbour model and the innocent dissemination defence model encourage the taking of 'reasonable access prevention steps' without any mechanism for protecting free speech.

It is reasonable to assume that most posters would not consent to having their identity and contact details passed on by the intermediary to the complainant. If they refuse, the intermediary loses the safe harbour protection unless they take 'access prevention steps'. This will encourage intermediaries to take down material without any protections for freedom of speech. The innocent dissemination defence ends up in the same place – 'access prevention steps' – even more quickly than the safe harbour because it doesn't offer an option for consent to have the complainant informed of the poster's details.

Recommendations 3A and 3B therefore in effect propose that Australian law embed a presumption that content which is the subject of a complaints notice is defamatory, fast-tracking its removal without any protection against attempts to censor otherwise legitimate material. This could have the effect of suppressing important content that is in the public interest, such as investigative journalism, or the voices of minorities and vulnerable groups.

Accordingly, we think the DWP has veered too far towards the easy remedy of takedown. This would be less of a concern if, under some other regulatory initiative, platforms were committed to promoting fairness and transparency in assessing content that is the subject of removal requests. But they are not. As a result, the MDAPs need to take on this responsibility in a way that fits with other attempts to regulate intermediaries, or to find a way to minimise what will at times be unjustified censorship. The harm is potentially greater under Model B than under Model A. As the paper explains: 'Under Model B, the internet intermediary must always take reasonable access prevention steps in relation to the publication (if there are any)' (p.32).

We also note a point made at the Stakeholder Roundtable that in respect of either of the proposed approaches, action taken to gain the benefit of the immunity/defence should include action taken by someone other than the intermediary (eg, where the intermediary notifies the poster of a complaint and the poster removes the content).

Our preference: A combined approach

We agree with those submitters who

> expressed a preference for a safe harbour defence, subject to complaints notice or a broader immunity. These stakeholders often viewed the innocent dissemination defence as a back-up or alternative defence should such a safe harbour be lost, or an immunity not apply (p.41).

In our view the legislative fix can and should perform all the following functions:

1. it should provide a safe harbour in situations where the person who posted the material is easily identifiable;
2. it should extend that safe harbour where the intermediary provides a forum for early resolution in matters where the parties agree the matter can be addressed by some action (such as editing content, taking down the post, or some form of explanation or apology);
3. it should provide the intermediary with a defence where the safe harbour is not available (because the identity of the poster is not known, the poster does not respond, and the matter can't be resolved between the parties using the dispute resolution mechanism described in 2) *provided* the intermediary itself acts reasonably (more on this below).

On point 1 we agree with the proposition in Model A that if the complainant knows the originator's identity, an action against the platform should not be available. This will be the case where it is evident who the complainant is, or this could be relatively easily ascertained, or is made known to them in the unlikely event that the intermediary gives the complainant this information in response to a request from them.

Where the identity cannot be established by these means, the intermediary should not be compelled to provide the information or to remove the content without an order from a court, and where the originator has had an opportunity to respond. This will protect both the originator's privacy (in cases where that is important) and the public interest in freedom of speech.

Admittedly, there will still be cases where the identity of the originator is not known, but in our view, this should not result in making the intermediary liable. Instead, it should be the stage at which point 2 kicks in. Again, there may be many instances where agreement is not reached between the parties on some action such as editorial amendments or an apology. But – particularly for social media complaints – there should be at least some circumstances where such action resolves the matter without the involvement of the courts. Accordingly, we also think intermediaries should be encouraged to offer forums in which complainants and those posting content can be brought together to seek agreed outcomes, in some circumstances without the need for the poster to be identified.

Finally, if the safe harbour as described above is not available, the innocent dissemination defence should be available in the circumstances described in the Background Paper and the MDAPs. Although it would still represent a fast track to takedown, the availability of the immunity that precedes it could at least prompt attempts at dispute resolution that do not involve automatic removal.

Recommendation 4: Commonwealth immunity for ISPs and hosting services

Commonwealth Government to consider an exemption for defamation law from the Online Safety Act 2021 immunity

The meaning of 'internet content host' under the *Broadcasting Services Act 1992* (Cth) was impenetrable. The replacement of this term in the Online Safety Act with 'hosting service' has provided some clarity, as it now appears that a search engine or a social media service would not be a hosting service, whereas a data storage service would. Combined with the twin provision on ISPs, the outcome is that ISPs and storage services will not be liable under state and territory defamation law because they are protected by the Commonwealth immunity. This immunity only extends to situations where the ISP or hosting service was 'not aware of the nature of the online content', but the immunity itself protects them against any obligation to monitor content.

It appears that the MDAP proposal offers greater protection because it excludes all aspects of knowledge, including situations where the provider has been put on notice by a complainant, and it applies to search engines as well as ISPs and storage services. However, as the Background Paper notes, there is still some uncertainty over the scope of 'hosting service' and the meaning of 'aware of the nature of' the content. Clarification by the Commonwealth would be desirable, irrespective of the connection to defamation law. The Background Paper notes the Explanatory Memorandum to the Online Safety Act indicates a search engine would not be considered a hosting service, but there is also a discussion in the Background Paper of 'hosting service provider' possibly extending to forum administrators. While we think social media services and forum administrators should have a limited safe harbour and innocent dissemination defence under defamation law, it seems inappropriate to give them the benefit of the Commonwealth immunity designed for conduits and storage services, even if, in effect, it only applies after there is knowledge of the content. There may be situations involving content that is more harmful than defamatory statements where governments need to impose additional obligations on social media services and forum administrators, or at least to apply a different test than 'awareness' (eg negligence).

Given there is as yet no final form of the MDAPs, we are reluctant to support the removal of the immunity in the Online Safety Act. If the protection in the MDAPs is scaled back from what is currently proposed, and these reforms do not provide sufficient protection for mere conduits and storage services, there will be a continuing need for the immunity in the Online Safety Act (even though, as it must apply to other law as well as defamation, it would not be as effective as the MDAP proposal). Even if the final MDAPs do protect ISPs, other 'mere conduits' and storage services in the form currently proposed, it may be preferable to retain the Commonwealth immunity because: there is no assurance that all Australian jurisdictions will implement the MDAPs; those laws could be repealed or amended; and the new Model Defamation Provisions will be subject to judicial interpretation.

Recommendation 5: Court orders against non-party intermediaries

Empower courts to make non-party orders to prevent access to defamatory matter online

We support this recommendation provided the order against the intermediary is only available, as proposed, when an order has also been made against the originator, and the originator (where their identity is known or can be ascertained) has had notice of the application and an opportunity to respond. We would also like to see some guidance on how the orders may be removed or how they might sunset.

Recommendation 6: Preliminary discovery orders against an internet intermediary to obtain information about an originator

Courts to consider balancing factors when making preliminary discovery orders, requiring courts to take into account the objects of the MDPs and any privacy, safety or public interest considerations which may arise should the order be made

While we support the recognition of privacy and freedom of expression, we have some concerns that requiring courts to take such aspects into account will be overwhelmed by perceptions of the importance of protecting reputation. In any event, such orders should not be available until complainants have first attempted dispute resolution offered by the intermediary (as we propose above).

Recommendation 7: Offers to make amends

Mandatory requirements for an offer to make amends to be updated for online publications – for example by using removal of content or restricting access as an alternative to a correction, apology etc.

We support this recommendation.