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)

August 2022

NSW GOVERNMENT

Disclaimer

This document has been prepared by the Department of Communities and Justice for general information purposes. While every care has been taken in relation to its accuracy, no warranty is given or implied. Further, recipients should obtain their own independent advice before making any decisions that rely on this information.

Contents

Introduction and consultation process 3

Executive summary 4

Part A policy recommendations 8

Background 13

Context 16

Part A terminology 21

Recommendations 1 and 2: Conditional, statutory exemption for a narrow group of internet intermediary functions 22

Recommendations 3A and 3B: Two alternative options for a new defence for internet intermediaries 31

Recommendation 4: Clarify interaction with the *Online Safety Act 2021* immunity 44

Recommendation 5: New court powers for non-party orders to remove online content 47

Recommendation 6: Considerations when making preliminary discovery orders about originators 52

Recommendation 7: Offers to make amends to be updated for online publications 56

Savings and transitional provisions for Part A 59

Appendix A: Categorising internet intermediaries 61

Appendix B: NSW Bar Association proposal 64

Appendix C: *Broadcasting Services Act/Online Safety Act* provisions 65

Introduction and consultation process

This paper is released together with the Part A consultation draft Model Defamation Amendment Provisions 2022 (**draft Part A MDAPs**).

The purpose of this paper is to explain the policy rationale behind the draft Part A MDAPs. This includes how they are intended to address the key points raised by stakeholders in response to Part A of the Stage 2 Discussion Paper, released in April 2021.

On 12 August 2022, the Meeting of Attorneys-General (**MAG**) agreed that this paper and the draft Part A MDAPs should be released for public consultation. This does not represent an endorsement of the policy recommendations or draft amendments by the MAG or the Defamation Law Working Party. A decision on this will be made following the exposure draft consultation process.

Consultation draft Model Defamation Amendment Provisions 2022 have been also prepared for Part B of the Stage 2 Review. Please refer to the separate policy paper for information about Part B.

Consultation process

Interested individuals and organisations are invited to provide written submissions in response to the draft Part A MDAPs.

Submissions should be sent:

- By email to: defamationreview@justice.nsw.gov.au, or
- By mail to Policy, Reform & Legislation, NSW Department of Communities and Justice, Locked Bag 5000, Parramatta NSW 2124

The due date for submissions is Friday 9 September 2022.

Please note that the contents of the submissions may be made published, unless otherwise advised. If you wish for your submission to remain confidential, please clearly identify this when you make your submission.

If you are interested in participating in the consultation but are unable to make a written submission, please contact us at: defamationreview@justice.nsw.gov.au.

Executive summary

Australia has uniform defamation legislation, the Model Defamation Provisions (**MDPs**), enacted by each state and territory.

Part A of the Stage 2 Review of the MDPs addresses the liability of internet intermediaries in defamation law for the publication of third-party content online. The premise of Part A is that due to the broad test for determining who is a publisher under the common law, an internet intermediary is anyone who participates in the facilitation of the publication other than the person who authors the content in the first place (**the originator**).

The term 'internet intermediaries' is used to cover a broad range of functions such as internet service providers, content hosts, search engines and social media platforms. It also includes those who use online platforms to host forums that invite third-party comments. This was considered in the High Court decision in *Fairfax Media Publications Pty Ltd & Ors v Voller* [2021] HCA 27. The High Court held, following the common law's traditionally broad approach to the element of publication, that the media companies were the publishers of third-party comments on their Facebook pages responding to news stories they posted.

The purpose of the Part A work is to reform the model laws to strike a better balance between protecting reputations and not unreasonably limiting freedom of expression in the various circumstances where third parties publish defamatory matter via internet intermediaries.

While stakeholder views on Part A differ, there is general agreement on the need to clarify the law in this area. Many were of the view that any reform should focus the dispute between the complainant and the originator of the matter in question. A common concern was the potential chilling effect on free speech of defences that require internet intermediaries to remove content to avoid liability. A number of stakeholders submitted that it is not fair to hold an internet intermediary liable for third-party content of which they are unaware.

At the same time, legal stakeholders emphasised that a complainant should not be left without a remedy, in particular that the matter in question should either be defended or removed from the internet. Otherwise, there is a real risk of failure to provide a remedy where the originator is unidentifiable or unwilling to respond. Many stakeholders emphasised that in the context of third-party content published online, the remedy most sought after by complainants is for the matter to be removed expeditiously, without the need for litigation.

A range of reforms are proposed to address the Part A issues comprehensively

For Part A, a range of potential reforms have been developed to respond comprehensively to the full spectrum of internet intermediary liability for third-party content. These recommendations are the basis of drafting instructions issued to the Parliamentary Counsel's Committee to prepare the draft Part A MDAPs for consultation.

Recommendations 1 & 2: Conditional, statutory exemption for a narrow group of internet intermediary functions

In the development of defamation law, it has been argued that certain traditional intermediaries (e.g.

telephone lines and postal services) are so passive in the facilitation of publication that they should not be considered publishers. They are 'mere conduits'.

Stakeholder views were sought on whether equivalent internet intermediary functions should have statutory protection from defamation liability for third-party content. A statutory exemption would apply irrespective of whether the intermediary is made aware of the defamatory content. A large number of stakeholders agreed that such an exemption should be based on the principle of passivity. Given the breadth of the protection, some stakeholders submitted that an exemption should be granted on a restrictive basis.

Two, statutory, conditional exemptions are recommended:

- **Recommendation 1**: A conditional, statutory exemption from defamation liability for mere conduits, caching and storage services
- **Recommendation 2**: A conditional, statutory exemption from defamation liability for standard search engine functions

Recommendation 1 would cover internet intermediary functions including Internet Service Providers (**ISPs**), cloud services and email. These internet intermediaries are not generally the subject of defamation claims and (in the case of ISPs in particular) are unlikely to be considered publishers under the common law test. While Recommendation 1 would not substantially change the law, it recognises that where internet intermediaries play an entirely passive role in the facilitation of a publication, they should not be liable.

Recommendation 2 would apply only to narrowly defined 'standard search engine functions', subject to conditions. Recommendation 2 presents an important change to the law. Search engines have been the subject of defamation claims in Australia and the High Court has confirmed that a search engine may be a publisher of search results. However, the treatment of search engines in Australia diverges from other comparable jurisdictions.

The rationale for Recommendation 2 is that in performing their standard functions, search engines have no interest in the content. The publication of the search results is prompted in the first instance by the user typing in a search query and the user is also the recipient. The search engines simply use an automated process to provide access to third-party content. The proposed exemption would not cover autocomplete functions provided by some search engines, or content that is paid advertising.

Stakeholder submissions in favour of an exemption for search engine functions also emphasised that search engines are unable to remove content from the internet, they operate on a massive scale and have no relationship with the originator. Another consideration is the significant social and economic value of search engines.

Recommendations 3A and 3B: Two alternative options for a new defence for internet intermediaries

For the most part, stakeholder submissions supported the introduction of a new defence for internet intermediaries, although there were a range of views regarding the right approach.

Two **alternative** models are considered the most viable:

- **Recommendation 3A:** Model A – safe harbour defence for internet intermediaries, subject to a simple complaints notice process, or
- **Recommendation 3B:** Model B – innocent dissemination defence for internet intermediaries, subject to a simple complaints notice process

A common goal for both models is to clarify the law for the benefit of complainants, internet intermediaries and originators. Both models would provide for:

- basic prescribed contents for the complaints notice to the internet intermediary

- a specific period of time in which the internet intermediary is to act
- an internet intermediary not being ineligible for the defence simply because it has a practice of monitoring for or taking down unlawful content (i.e. practising good behaviour)
- the internet intermediary being denied the defence if it is actuated by malice

The purpose of **Recommendation 3A** is to focus the dispute between the complainant and the originator. It provides a complete defence if the complainant already has sufficient information about the originator to issue a concerns notice or commence proceedings.

If the complainant does not have this information, the internet intermediary can avail itself of the defence if, with the consent of the originator, it provides that information to the complainant. Otherwise the intermediary must prevent access to the content within 14 days.

The purpose of **Recommendation 3B** is to recognise that internet intermediaries should not be liable for third-party defamatory content where they are merely a subordinate distributor and lack knowledge of the defamatory content. Once the internet intermediary has received a complaints notice, it must prevent access to the matter within 14 days in order to be able to rely on the defence.

One key difference between Model A and Model B is that Model B does not provide an automatic defence (or safe harbour) where the complainant has sufficient information about the originator to issue a concerns notice or commence proceedings.

Recommendation 4: Clarify interaction with the Cth *Online Safety Act 2021* immunity

Put simply, section 235(1) of the Commonwealth *Online Safety Act 2021* provides that a law of a state or territory, or common law or equity has no effect if it:

- subjects an Australian hosting service provider or ISP to liability where they are not aware of the nature of the online content or
- requires an Australian hosting service provider or ISP to monitor online content

Stakeholders have consistently submitted that the interaction between the *Online Safety Act 2021* immunity and defamation law is uncertain. Key reasons given for this are that it is not clear:

- which internet intermediaries are covered
- what constitutes 'awareness' of the online content that defeats the immunity

Recommendation 4 is that the Commonwealth Government should give close consideration to whether an exemption from section 235(1) of the *Online Safety Act 2021* for defamation law is desirable, in the interests of clarity of the law.

Recommendations 5 and 6: Clarification and enhancement of court powers

Courts in defamation proceedings (as in other civil proceedings) will generally only grant orders against defendants that are party to the proceedings. In some circumstances though, even if a complainant has obtained judgment against an originator, it may be difficult to enforce a remedy. For example, where the originator is unable to remove content (it may have 'gone viral') or simply refuses to do so. In these circumstances, despite not being party to the proceedings, internet intermediaries may be in a good position to assist.

Recommendation 5 would empower courts to make orders against non-parties to prevent access to defamatory matter online. This would be in circumstances where the court grants interim or final judgment for the complainant in an action for defamation.

There would also be a requirement to give notice to the non-party internet intermediary. This is to ensure that the internet intermediary has the opportunity to make submissions about whether the order should be made.

Recommendation 6 relates to preliminary discovery orders issued by courts against internet intermediaries to provide information about the originator. Some stakeholders raised concerns about the low threshold for such orders. There may be privacy and safety concerns where the location information of a dissident or domestic violence victim may be disclosed.

Australian courts can, and do, take into account considerations of proportionality, privacy and the risk of abuse of process in exercising the discretion to make preliminary discovery orders. However, there may still be a risk that such orders are abused or have a chilling effect.

Recommendation 6 is that where court rules allow a complainant to seek a preliminary discovery order from an internet intermediary in order to obtain information about an originator for the purposes of commencing defamation proceedings, the court should consider: the objects of the MDPs; and any privacy, safety or public interest considerations which may arise should the order be made. This recommendation does not provide a new avenue to seek preliminary discovery, it simply applies this requirement over the general rules.

Recommendation 7: Mandatory requirements for an offer to make amends to be updated for online publications

Part 3 of the MDPs establishes a process for parties to settle disputes without the need for litigation, by requiring the complainant to notify the publisher of the defamatory matter, and allowing sufficient time for the publisher to make a reasonable 'offer to make amends'.

There are a number of mandatory requirements for what a reasonable offer to make amends must include. One of these is an offer to publish a reasonable correction or clarification of the matter in question. Stakeholders have pointed out that internet intermediaries may simply not be able to comply with these mandatory requirements. For example, a search engine would be unable to publish a correction regarding a publication. They also submitted that in the context of third-party content published online, the remedy most sought after by complainants is to have the matter removed.

Recommendation 7 is to amend the mandatory requirements for the content of an offer to make amends to allow the publisher to prevent access to the matter in question. This would be instead of the mandatory requirement for an offer to publish a reasonable correction or clarification of the matter in question.

Part A policy recommendations

Seven recommendations for reform are proposed to address the issue of internet intermediary liability in defamation law for third-party content.

Recommendation 1: Conditional, statutory exemption from defamation liability for mere conduits, caching and storage services

See draft Part A MDAPs Sch 1 [2], draft section 9A

Introduce a new statutory, conditional exemption from liability in defamation law for:

a) Mere conduits, including Internet Service Providers (**ISPs**) that supply internet carriage services to the public

b) Caching services

c) Services that enable the storage of data

The statutory exemption would apply irrespective of whether the internet intermediary is made aware of the allegedly defamatory content. This is a very broad protection so the exemption would apply on the condition that:

- The internet intermediary did not initiate the process of publication or select the intended recipient(s), and
- The internet intermediary did not encourage, edit or promote the matter*

*The draft Part A MDAPs make clear that if a mere conduit, caching or storage service takes action in compliance with a Commonwealth, state or territory law, this does not preclude access to the exemption.

In any defamation proceedings, the statutory exemption is to be determined by a judicial officer. It should be determined as soon as practicable before the trial commences unless the judicial officer is satisfied there are good reasons to postpone the determination to a later stage.

Recommendation 2: Conditional, statutory exemption from defamation liability for standard search engine functions

See draft Part A MDAPs Sch 1 [2], draft section 9A

Introduce a new statutory exemption from liability in defamation law for:

- the use of automated tools to search the internet to return search results, identifying and linking to third-party websites, based on the search terms input by users

The statutory exemption would apply irrespective of whether the search engine is made aware of the allegedly defamatory content. This is a very broad protection so the immunity would apply on the basis that:

- the search engine's role in the process of publishing the matter is of a solely technical and automatic nature
- in performing its function, the search engine has no monetary or other particular interest in promoting the content outside of the search engine's normal functioning

In any defamation proceedings, the statutory exemption is to be determined by a judicial officer. It should be determined as soon as practicable before the trial commences unless the judicial officer is satisfied there are good reasons to postpone the determination to a later stage.

Recommendation 3A: Model A – Safe harbour defence for digital intermediaries, subject to a simple complaints notice process (Alternative to Recommendation 3B)

See draft Part A MDAPs Sch 1 [6], draft section 31A

Introduce a defence for publications involving digital intermediaries (Model A). The purpose of Model A is to focus the dispute between the complainant and the originator.

Elements of the defence

It would be a defence to the publication of defamatory digital matter if the defendant proves:

- it was a digital intermediary in relation to the publication (that is a person, other than the author, originator or poster, who provided an online service in connection with the publication of the matter),
- at the time of the publication, it had a mechanism that was easily accessible by members of the public for submitting complaints notices, and
- if the complainant duly gave the digital intermediary a complaints notice — within 14 days the digital intermediary either:
  a) with the poster's consent, provided the complainant with sufficient information to enable a concerns notice to be issued or proceedings commenced against the poster, or
  b) took the access prevention steps in relation to the publication, if any, that were reasonable in the circumstances.

In order to obtain the poster's consent, the internet intermediary would need to provide the poster with a copy of the complaints notice. This is so the poster has sufficient information based on which they can choose to defend the publication.

Safeguard for good behaviour

A digital intermediary would not be ineligible for the defence solely because it took steps to detect, identify or prevent access to defamatory content, unlawful content or content

incompatible with its terms of service.

Malice exclusion

The defence would be defeated if the complainant establishes that the defendant was actuated by malice in providing the online service used to publish the digital matter.

Complete defence where complainant can identify the poster

A complaints notice may only be given if, after taking reasonable steps, the complainant was not able to obtain sufficient information to enable a concerns notice to be given to the poster or proceedings to be commenced. A complainant would not be expected to hire a private investigator or seek an order for substituted service or preliminary discovery to meet the reasonable steps requirement.

The complaints notice

The prescribed information for a complaints notice would be:

- the name of the complainant
- the location where the matter can be accessed (for example, a webpage address)
- an explanation of why the complainant considers the matter to be defamatory and if the complainant considers the matter to be factually inaccurate, a statement to that effect
- the serious harm to reputation caused, or likely to be caused by the publication of the matter
- the steps taken to identify the poster

Recommendation 3B: Model B – innocent dissemination defence for digital intermediaries, subject to a simple complaints notice process (Alternative to Recommendation 3A)

See draft Part A MDAPs Sch 1 [7], draft section 31A

Introduce a new defence for publications involving digital intermediaries (Model B). The purpose of Model B is to recognise that internet intermediaries should not be liable for the publication of third-party defamatory content where they are merely subordinate distributors and are not aware of it.

Elements of the defence

It would be a defence to the publication of defamatory digital matter if the defendant proves:

- it was a digital intermediary in relation to the publication (that is a person, other than the author, originator or poster, who provided an online service in connection with the publication of the matter),
- at the time of the publication, it had a mechanism that was easily accessible by members of the public for submitting complaints notices, and
- if the complainant duly gave the digital intermediary a complaints notice — within 14 days the digital intermediary:
    - took the access prevention steps in relation to the publication, if any, that were reasonable in the circumstances.

Safeguard for good behaviour

A digital intermediary would not be ineligible for the defence solely because it took steps to detect, identify or prevent access to defamatory content, unlawful content or content incompatible with its terms of service.

Malice exclusion

The defence would be defeated if the complainant establishes that the defendant was actuated by malice in providing the online service used to publish the digital matter.

The complaints notice

The prescribed information for a complaints notice would be:

- the name of the complainant
- the location where the matter can be accessed (for example, a webpage address)
- an explanation of why the complainant considers the matter to be defamatory and if the complainant considers the matter to be factually inaccurate, a statement to that effect
- the serious harm to reputation caused, or likely to be caused by the publication of the matter

Recommendation 4: Commonwealth Government to consider an exemption for defamation law from the *Online Safety Act 2021* immunity

The Commonwealth Government should give close consideration to whether an exemption from section 235(1) of the *Online Safety Act 2021* for defamation law is desirable, in the interests of clarity of the law.

Recommendation 5: Empower courts to make non-party orders to prevent access to defamatory matter online

See draft Part A MDAPs Sch 1 [8], draft section 39A

Amend the MDPs to provide that where a court grants an interim or final order or judgment for the complainant in an action for defamation, the court may order a person who is not a party to remove, block or disable access to the online matter within the scope of such order or judgment.

The power should require notice to be given to the person who is not a party before the order is made.

Recommendation 6: Courts to consider balancing factors when making preliminary discovery orders

See draft Part A MDAPs Sch 1 [5], draft section 23A

Amend the MDPs to provide that, where court rules allow a complainant to seek a preliminary discovery order from an internet intermediary in order to obtain information about an originator for the purposes of commencing defamation proceedings against them, the court should take into account:

- the objects of the MDPs
- any privacy, safety or public interest considerations which may arise should the order be made

Recommendation 7: Mandatory requirements for an offer to make amends to be updated for online publications

See draft Part A MDAPs Sch 1 [3], draft section 15(1A)(b) and Sch 1 [4], draft section 15(1B)

Amend the mandatory requirements for the content of an offer to make amends in clause 15 to:

- provide an alternative to clause 15(1)(d) by allowing the publisher to offer to remove, block or disable access to the matter in question. This would be instead of the requirement for an offer to publish, or join in publishing, a reasonable correction of, or a clarification or additional information about, the matter in question.
- make clear that if the alternative is used by the publisher, clause 15(1)(e) would not be mandatory either

Background

In November 2004, the then Standing Committee of Attorneys-General agreed to enact model provisions in recognition of the need for uniform defamation law in Australia. States and territories subsequently enacted the MDPs through legislation.

All states and territories are parties to the Model Defamation Provisions Intergovernmental Agreement (**IGA**). The IGA establishes the Defamation Law Working Party (**DWP**) which is required, amongst other functions, to report to Attorneys-General on proposals to amend the MDPs and to act as a forum for discussion of issues affecting the protection of reputation, freedom of expression and publication.

The Stage 2 Review of the MDPs

A NSW led Stage 1 Review of the MDPs was completed in July 2020 with Attorneys-General agreeing to a range of amendments that have now been enacted in most states and territories.

During the Stage 1 Review, Attorneys-General agreed there should be a second stage of reforms to focus on the responsibilities and liability of digital platforms for defamatory content published online as well as other new and emerging issues affecting defamation law.

In April 2021, a Discussion Paper for the Stage 2 Review of the MDPs was released for public consultation. It has two parts:

- Part A (led by NSW) addresses the question of internet intermediary liability in defamation for the publication of third-party content.
- Part B (led by Victoria) considers whether defamation law has a chilling effect on reports of alleged unlawful conduct to police and statutory investigative bodies. It looks at whether absolute privilege should be extended to these circumstances.

Almost 50 written submissions were received from stakeholders in response to the Stage 2 Discussion Paper. Four stakeholder roundtables were held in September and early October 2021 to discuss the key issues.

Part A– liability of internet intermediaries

At common law, the definition of publisher in defamation law is very broad. Anyone who takes part in publication 'in any degree' can be regarded as a publisher.

The responsibility of the individual or organisation that authors or creates the content in the first place is not in question (**the originator**). They are a publisher and will be regarded as potentially liable in defamation (subject to the availability of defences). The purpose of Part A is to address the question of liability in defamation law of everyone else who participates in the publication of third-party content online. These are the **internet intermediaries**.

The Stage 2 Discussion Paper outlined five key issues:

- Issue 1: Categorising internet intermediaries
- Issue 2: Immunities and defences
- Issue 3: Complaints notice process
- Issue 4: Power of courts to order that material be removed
- Issue 5: Power of courts to order that internet intermediaries reveal the identity of originators posting on their platforms

Issue 2: Immunities and Defences presented a range of options for reform to clarify or modify the liability of internet intermediaries in respect of third-party content. The options represented a spectrum of liability, from least change to the status quo, to broadest immunity from liability for internet intermediaries.

Criteria for assessing reform options

As noted in the Stage 2 Discussion Paper, the criteria for assessing the Part A options for reform are: the objects of the MDPs and one additional criterion. Clause 3 of the MDPs sets out the following objects:

a) To enact provisions to promote uniform laws of defamation in Australia, and

b) To ensure that defamation law does not place unreasonable limits on freedom of expression and, in particular, on the publication and discussion of matters of public interest and importance, and

c) To provide effective and fair remedies for persons whose reputations are harmed by the publication of defamatory matter, and

d) To promote speedy and non-litigious methods of resolving disputes.

The additional criterion for the purpose of the Stage 2 Review is:

- To ensure that defamation law does not stifle technological innovation or the emergence of new online services and activities that have both a social and economic benefit to society.

Stakeholder views

There were a number of over-arching points made by stakeholders through the consultation process.

Most stakeholders agreed that there is a need to clarify the law in Australia regarding internet intermediary liability for the publication of defamatory matter by third parties. Technology sector stakeholders also submitted that Australian law is out of step with comparative jurisdictions.

Many stakeholders argued that the Stage 2 Review should aim to ensure that the focus of the dispute is between the complainant and the originator of the matter in question. It was submitted by many that defamation law should primarily work to hold the originator accountable for their statements. Stakeholders pointed out that some defamatory publications are defensible (e.g. they may be true or an expression of honest opinion). In these cases, it is the originator, and not the internet intermediary, that is in the best position to defend the publication.

At the same time, legal stakeholders in particular emphasised that a complainant should not be left without a remedy, and that the matter in question should either be defended or removed from the internet. There is a real risk of failure to provide a remedy where the originator is unidentifiable or unwilling to respond. Defamatory publications on the internet can quickly spread far and wide, and persist for a long period of time – potentially doing serious harm to a person's reputation. In the view of these submissions, the basic policy underlying defamation law of protection of reputation needs to be respected, and not fundamentally undermined by overly protective defences.

A range of stakeholders also expressed concerns about the potential chilling effect of defences that effectively require internet intermediaries to remove matter in order to avoid liability. These stakeholders were concerned that discussion of matters of public interest could be stifled, and that take down procedures were open to abuse by those who seek to have legitimate content removed for ulterior motives. Some stakeholders emphasised that it is the courts, and not the internet intermediaries, that should be the arbiters where a publication is in dispute.

Finally, a number of stakeholders made the point that it is not fair for an internet intermediary to be liable where they are unaware or could not reasonably have knowledge of the matter. Clear notice of the allegedly defamatory content should be required for the internet intermediary to be in the frame of potential liability.

Reforms in this area need to balance these concerns.

Context

International developments

The Stage 2 Discussion Paper briefly outlined the approaches in other jurisdictions including: the United Kingdom (**UK**), the United States of America (**USA**) and Canada.[1] Since the Stage 2 Discussion Paper was released in May 2021, there have been some further developments. The DWP has also given closer consideration to the approach in the European Union (**EU**).

European Union

At the end of 2020, the European Commission published the draft text of the Digital Services Act[2] (**EU DSA**), which will replace the E-Commerce Directive[3]. The Digital Services Act will update and harmonise safety and liability rules for 'intermediary services' operating in the EU.

Chapter II of the EU DSA retains the established liability exemptions for intermediary services in the E-Commerce Directive. There is a general exemption from liability for mere conduits providing passive transmission services, and caching services providing temporary caching or storage services;[4] and for 'hosting' services where they did not have actual knowledge of illegal activity, are not aware of facts or circumstances from which the illegal activity or content is apparent, and act expeditiously to remove it upon obtaining such knowledge or awareness.[5] The prohibition against a general requirement for digital intermediaries to monitor third-party content for illegality is also retained.[6] However, a new provision clarifies that voluntary own-investigations by digital intermediaries will not disqualify them from liability exemptions.[7]

A significant change is that the text of the EU DSA is not a directive. Rather, the text of the EU DSA will be directly adopted by all states as a regulation with a common text, ensuring a more harmonised approach across the EU.

On 5 July 2022 the European Parliament adopted the EU DSA with some amendments to the original draft text. The EU DSA final text is now awaiting official publication. It is anticipated that the EU DSA will come into force by early 2024.[8]

United Kingdom

As a result of the UK's withdrawal from the EU, the UK is no longer subject to EU law, including the E-Commerce Directive, which prevented the UK Government from imposing liability on digital

1 Stage 2 Discussion Paper, from p 18.

2 Digital Services Act 2020/0361(COD), as updated by amendments made by the EU Parliament (**EU DSA**). The text of the provisional agreement (pending publication of the final text) of the EU DSA is available on the European Parliament website at https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html

3 *Directive 2000/31 EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* (**E-Commerce Directive**).

4 See E-Commerce Directive Articles 12 and 13; EU DSA Articles 3 and 4.

5 E-Commerce Directive Article 14; EU DSA Article 5.

6 E-Commerce Directive Article 15; EU DSA Article 7.

7 EU DSA Article 6.

8 See https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

platforms as long as they do not have actual knowledge of illegal activity on their platforms, or similar provisions under the incoming EU DSA.

On 12 May 2021, the UK Government issued an exposure draft of its Online Safety Bill.[9] The Bill creates duties of care for social media platforms and search engines to mitigate risks in relation to the dissemination of content which is illegal (i.e. criminal content such as terrorism or child abuse material)[10] or 'harmful' content which, although it may be legal, may be significantly psychologically or physically harmful to children or adults.[11] On 24 March 2022, the UK Government introduced a revised version of the Bill and on 4 July 2022, a House Committee released a report recommending further amendments.[12]

Scotland

The *Defamation and Malicious Prosecution (Scotland) Act 2021* (**Scottish Act**)[13] came into full force on 8 August 2022.[14] The Scottish Act fully codifies the common law of defamation in Scotland and brings several aspects of Scottish defamation law into line with the *Defamation Act 2013* (UK).

Section 3 contains novel deeming provisions concerning secondary publishers of 'electronic statements'. A person will not be deemed to be an 'editor' of an 'electronic statement' if the person's involvement with the statement is only '*publishing the same statement or providing a means to access the statement (for example a hyperlink) in a manner which does not alter the statement*' or '*marking the person's interest in, approval of or disapproval of the statement in a manner which does not alter the statement (typically by means of a symbol)'*. These deeming provisions are subject to the proviso that the person's involvement *'does not materially increase the harm caused by the publication of the statement'*. Subsection 3(6) provides that the Scottish Ministers may by regulation modify subsections 3(3) and 3(4) to *'add, amend or remove activities or methods of disseminating or processing material'* in order to take account of *'technological developments'* or '*changes in how material is disseminated or processed*' (s 3(7)). Section 4 provides that the Scottish Ministers may by regulations specify categories of persons '*who are to be treated as publishers of a statement for the purposes of defamation law*'.

United States

In the USA, there have been continued calls for reform of section 230 of the *Communications Decency Act 1996*, although there has as yet been no bill introduced to Congress in response to the June 2020 U.S. Department of Justice recommendations for section 230 reform.[15] These recommendations include a carve out to the section 230 immunity for internet intermediaries that purposefully facilitate or solicit content that violates federal criminal law or are wilfully blind to criminal content on their platforms, and where a platform was provided with a court judgment that the content is unlawful, and does not take appropriate action.

9 Online Safety Bill 2021 (UK).

10 Online Safety Bill 2021 (UK), s 41.

11 Online Safety Bill 2021 (UK), ss 45 and 46.

12 House of Commons, Digital, Culture, Media and Sport Committee, *Amending the Online Safety Bill, First Report of Session 2022-23, Report, together with formal minutes relating to the Report*, available at https://committees.parliament.uk/publications/22894/documents/168085/default

13 Available at https://www.legislation.gov.uk/asp/2021/10/contents

14 Defamation and Malicious Publication (Scotland) Act 2021 (Commencement and Transitional Provision) Regulations 2022, available at https://www.bailii.org/cgi-bin/format.cgi?doc=/scot/legis/num_reg/2022/ssi_2022154_en_1.html , p 4.

15 U.S. Department of Justice, *Review of section 230 of the Communications Decency Act of 1996*, available at https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996

Australian regulatory context

On 23 June 2021, the Commonwealth Parliament passed the *Online Safety Act 2021* (**OSA**). The OSA came into effect on 23 January 2022. Relevant elements of the OSA are:

- The introduction of an adult online cyber abuse scheme. 'Adult cyber abuse' is defined as online communication to or about a person who is 18 years or older which is intended to cause them serious harm and is 'menacing, harassing or offensive' in all the circumstances, based on an 'ordinary reasonable person' test.[16] According to regulatory guidance issued by the eSafety Commissioner, the definition is not intended to regulate 'purely reputational damage, bad online reviews, strong opinions or banter'.[17]
- The introduction of Basic Online Safety Expectations for online service providers.[18]
- The 'BSA Immunity' in Schedule 5, cl 91 of the *Broadcasting Services Act 1991* (Cth) has been moved into s 235(1) of the OSA, with the substitution of the term 'Australian hosting service provider' for 'internet content host'.
- The eSafety Commissioner is granted the power to obtain end-user identity information and contact details from online service providers.[19]

On 25 October 2021, the Commonwealth Government released an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021. The Bill would introduce a binding online privacy code for social media services, data brokers and other large online platforms operating in Australia, and would require platforms to verify the age of users.

Recent case law

Fairfax Media Publications Pty Ltd & Ors v Voller [2021] HCA 27

On 8 September 2021, the High Court handed down judgment in *Fairfax Media Publications Pty Ltd & Ors v Voller* [2021] HCA 27.

Mr Dylan Voller was a detainee of the Don Dale Youth Detention Centre in the Northern Territory, which was the subject of a Four Corners Program in 2016. The treatment of detainees exposed in the program prompted the establishment of the Royal Commission into the Protection and Detention of Children in the Northern Territory.

The appellants were media companies that maintained a public Facebook page on which they posted content relating to news stories referring to Mr Voller. A number of third-party Facebook users responded with comments that were alleged to be defamatory of Mr Voller. Mr Voller brought proceedings in the NSW Supreme Court against the appellants, alleging that they were liable for defamation as the publishers of those comments.

The primary judge ordered that a question concerning the issue of publication be decided separately from the balance of the proceedings. The question was whether Mr Voller had 'established the publication element of the cause of action of defamation against the defendant[s] in respect of each of the Facebook comments by third-party users'. The NSW Court of Appeal concluded that the primary judge did not err in answering that question in the affirmative.

The High Court by majority dismissed the appeals and found that the appellants were the publishers of the third-party Facebook user comments.

The majority (Kiefel CJ, Keane and Gleeson JJ, and Gageler and Gordon JJ) held that the liability of a

[16] *Online Safety Act 2021*, s 7.

[17] eSafety Commissioner, *Adult Cyber Abuse Scheme Regulatory Guidance,* eSC RG 3 (December 2021), p 3, available at https://www.esafety.gov.au/sites/default/files/2021-12/ACA%20Scheme%20Regulatory%20Guidance%20%20FINAL.pdf

[18] *Online Safety Act 2021*, Part 4.

[19] *Online Safety Act 2021*, ss 193-195.

party as a publisher depends upon whether that party, by facilitating and encouraging the relevant communication, 'participated' in the communication of the defamatory matter to a third person. The majority rejected the appellants' argument that for a party to be a publisher it must know of the relevant defamatory matter and intend to convey it. Each appellant, by the creation of a public Facebook page and the posting of content on that page, facilitated, encouraged and thereby assisted the publication of comments from third-party Facebook users.

In dissent, Edelman J would have ordered that Mr Voller will establish the publication element of the cause of action for defamation in respect of each of the Facebook comments by third-party users by establishing that the Facebook comment has a connection to the subject matter posted by the defendant that is more than remote or tenuous.

In dissent, Steward J would have ordered Mr Voller will establish the publication element of the cause of action of defamation in relation to those third-party comments which had been procured, provoked or induced by posts made by the appellants on their respective Facebook pages.

The case subsequently settled before trial. This meant that there was no consideration of the balance of the proceedings including the availability of defences – such as innocent dissemination.

Defteros v Google LLC [2021] VSCA 167; [2022] HCATrans 77 (3 May 2022)

On 17 June 2021, the Victorian Court of Appeal handed down *Defteros v Google LLC* [2021] VSCA 167, dismissing Google's appeal from a trial judge's finding that the presentation of hyperlinks in Google's search results published the contents of the hyperlinks to a user who had performed a search on the complainant's name.

On 10 December 2021, Google obtained special leave[20] to appeal this and other points of the Victorian Court of Appeal's decision to the High Court of Australia. The High Court heard oral submissions and reserved its decision on 3 May 2022.[21] The pending judgment will consider the application, and grounds for displacement, of the 'mere hyperlink' principle in relation to the test for publication of defamatory material under Australian defamation law.

The mere hyperlink principle[22] is that the publication by the defendant of a hyperlink to a website containing allegedly defamatory material is not presumed, of itself, to publish the contents of the website itself, provided the defendant does not repeat the defamatory imputation in their own publication. The High Court will consider how the mere hyperlink principle applies in Australia in the context of search results.[23]

Barilaro v Shanks-Markovina & Google LLC [2022] FCA 650

Mr John Barilaro, who was formerly the Deputy Premier of New South Wales, sued Google, the owner of YouTube, in respect of two videos posted on that platform by one of its users, Jordan Shanks-Markovina, also known as 'friendlyjordies' (**Shanks**). The applicant also sued Shanks but settled with him prior to trial.

The videos contained commentary on the applicant's performance as a politician. However, various personal matters were also discussed and the tone of the videos was abusive, using numerous racial slurs. Prior to commencing proceedings, the applicant had complained to both Shanks and Google that the videos were defamatory of him, and sought take down of the videos. Both respondents refused to remove the videos for several months after receiving Mr Barilaro's complaints, during which period other users posted derogatory comments about Mr Barilaro in response. Google refused to remove the videos for several months, denied that defamatory imputations arose, raised several 'untenable' defences, and refused to apologise at trial.

---

[20] *Google LLC v Defteros* [2021] HCATrans 216.

[21] *Google LLC v Defteros* [2022] HCATrans 77.

[22] The 'mere hyperlink' principle was established in the leading judgment of Abella J in the Canadian Supreme Court decision in *Crookes v Newton* [2011] SCC 47.

[23] *Trkulja v Google LLC* [2018] HCA 25; *Fairfax Media Publications Pty Ltd & Ors v Voller* [2021] HCA 27.

Prior to trial, Google subsequently admitted that it was liable as a publisher after being put on notice of the defamatory character of the videos, admitted all defamatory imputations and abandoned its defences. The trial proceeded as a hearing on damages only. On 6 June 2022, Rares J awarded $715,000 in damages against Google, including aggravated damages arising out of Google's conduct after receiving Mr Barilaro's complaints.

Part A terminology

The term '**internet intermediaries**' is used throughout this paper to cover a broad range of functions such as internet service providers, content hosts, search engines and social media platforms. For the purposes of the Stage 2 Review, it also includes '**forum administrators**' – individuals or organisations that use online platforms to host forums that allow or invite third-party comments.

One example of a forum administrator was considered in the High Court decision in *Fairfax Media Publications Pty Ltd & Ors v Voller* [2021] HCA 27. The High Court held that the appellant media companies were the publishers of third-party comments on their Facebook pages that were responding to news stories they posted about Mr Dylan Voller.

Further information about **Categorising internet intermediaries** is at **Appendix A**.

The draft MDAPs use the term '**digital intermediary**' instead of 'internet intermediary'. Digital intermediary is a precisely defined term in the MDAPs to mean a person (other than an author, originator or poster of the matter) who provides an online service in connection with the publication of the matter. Online service is defined very widely to include all of the internet intermediary functions in the scope of the Stage 2 Review.

The more general term 'internet intermediary' is used throughout this paper for consistency with the Stage 2 Discussion Paper and the stakeholder submissions. The only exception to this is where the paper is describing a specific draft provision and it is therefore appropriate to use the term digital intermediary as it is defined.

The term '**originator**' is also used throughout this paper to describe any individual that authors or creates content online.

Recommendations 1 and 2: Conditional, statutory exemption for a narrow group of internet intermediary functions

Overview of Recommendations 1 and 2 – exemptions for mere conduits, caching and storage services and standard search engine functions

The Stage 2 Discussion Paper acknowledged that in the development of defamation law, it has been argued that certain traditional intermediaries are so passive in the facilitation of publication that they do not themselves attract liability.[24] For example, telephone lines and postal services have been considered too remote from publication to be considered liable. They are described as 'mere conduits'.

Based on the 'mere conduit' analogy with telephone lines and postal services and on case law elsewhere, it is generally presumed that an ISP which does no more than carry content, is not a publisher. While this view has recently been expressed in obiter by a state appeal court[25] there is no binding higher court authority on this point in Australia.

The Discussion Paper noted that this raises several questions. The first being whether any statutory protection for ISPs from liability in defamation for third-party content is required in Australia. The second question is whether, if statutory immunity were provided to ISPs, it should cover some other internet intermediary functions.

The policy rationale for providing statutory immunity to ISPs and other internet intermediary functions is that they are 'mere conduits' that do not actively participate in the publication – or by extension, sufficiently contribute to the risk of harm to reputation.

A statutory immunity would apply irrespective of whether the intermediary is made aware of the allegedly defamatory content. Given the breadth of this protection, there should be a high threshold for its application.

We recommend the introduction of two conditional, statutory exemptions:

Recommendation 1: A conditional, statutory exemption from liability in defamation law for mere conduits (including ISPs), caching and storage services

Recommendation 2: A conditional, statutory exemption from liability in defamation law for standard search engine functions

As noted above, the protection afforded by a statutory exemption is broad. It is therefore proposed that it should only apply to a narrow set of internet intermediary functions that are sufficiently

[24] Stage 2 Discussion Paper, from p 46.

[25] *Google Inc v Duffy* [2017] SASCFC 130.

remote from the publication of the third-party defamatory matter.

Recommendation 1 is intended to provide clarity and certainty in relation to the internet intermediary functions covered. This is because they are generally not the subject of defamation claims and (in the case of ISPs in particular) are unlikely to be considered publishers under the common law test. Recommendation 2 does involve an important change to the law by providing that in performing standard search functions, search engines should not be liable in defamation law. This proposed reform would apply narrowly, and be subject to specific conditions.

As a counterbalance to Recommendations 1 and 2, an important safeguard is provided through Recommendation 5. This would provide the courts with the power to order an internet intermediary to remove or disable access to defamatory material within the scope of an order or judgment for the complainant in an action for defamation, even when they are not a party to proceedings.

For both Recommendations 1 and 2, we consider that the determination of the exemption should be a matter for the judicial officer and wherever possible, it should be determined early. This is to support the policy intent behind these recommendations which is to recognise that any role of these internet intermediaries in the publication process and their relationship to the content is such that they should not be subject to defamation claims. If a complainant does seek to commence proceedings against one of these internet intermediaries, it is in the interests of both parties that the exemption be determined early. This will minimise costs and ensure that redress can be sought against more appropriate defendants. As a safeguard though, the judicial officer should have discretion to postpone the determination to a later stage where appropriate.

Recommendation 1: Conditional, statutory exemption from defamation liability for mere conduits, caching and storage services

See draft Part A MDAPs Sch 1 [2], draft section 9A

Introduce a new statutory, conditional exemption from liability in defamation law for:

a) Mere conduits, including Internet Service Providers (**ISPs**) that supply internet carriage services to the public

b) Caching services

c) Services that enable the storage of data

The statutory exemption would apply irrespective of whether the internet intermediary is made aware of the allegedly defamatory content. This is a very broad protection so the exemption would apply on the condition that:

- The internet intermediary did not initiate the process of publication or select the intended recipient(s), and
- The internet intermediary did not encourage, edit or promote the matter*

*The draft Part A MDAPs make clear that if a mere conduit, caching or storage service takes action in compliance with a Commonwealth, state or territory law, this does not preclude access to the exemption.

In any defamation proceedings, the statutory exemption is to be determined by a judicial officer. It should be determined as soon as practicable before the trial commences unless the judicial officer is satisfied there are good reasons to postpone the determination to a later stage.

Stakeholder views on an exemption for mere conduits, caching and storage services

A large number of stakeholders agreed that passivity is an appropriate principle on which an immunity for certain intermediary functions should be based. It was suggested though that caution should be exercised using neutrality towards the content as a principle on which to base immunity.

This is due to circumstances where an ISP that is otherwise neutral would need to prioritise certain internet traffic (for example in an emergency).

Several stakeholders took a different view on passivity – arguing that it does not address the underlying issue – which is the need to focus the dispute between the complainant and the originator. Nor does it account for other considerations such as the social and economic benefits of the services provided by internet intermediaries.

Some stakeholders argued that no blanket immunity should be given to any internet intermediary as it may become outdated and there is a risk that a defamed person would be denied a remedy for harm to their reputation. Other stakeholders submitted that this is not a practical risk if the immunity only applies to basic internet intermediary functions that do not actively participate in the publication.

A number of stakeholders agreed that immunity from defamation claims for third-party content should be granted on a fairly restrictive basis (e.g. to ISPs), provided the service is purely passive in the publication.

Several stakeholders submitted that if an immunity were introduced, a potential safeguard would be for ISPs or protected internet intermediaries to be subjected to blocking orders where appropriate – without carrying liability as publishers. This may be useful in circumstances where a repeat offender is offshore and continues to post unlawful content.

Key features of a conditional exemption for mere conduits, caching and storage services

The types of functions that Recommendation 1 is intended to cover include ISPs, cloud services, email and direct messaging services. The common feature of these functions is that their role in the process of publishing matter is of a solely technical and automatic nature.

Given the breadth of this protection, clear limiting principles are required. The exemption would apply on the condition that:

- The internet intermediary does not initiate the process of publication or select the intended recipient(s), and
- The internet intermediary does not encourage, edit or promote the matter

These limiting concepts are drawn in part from the underpinning concepts in the EU's E-Commerce Directive and its incoming new EU DSA.

In relation to the second limiting principle, the draft MDAPs make clear that the exemption is still available if the internet intermediary takes action in compliance with a Commonwealth, state or territory law. This recognises that there may be circumstances where an internet intermediary such as an ISP is required by law to prioritise certain internet traffic (for example if there is a major emergency) or to remove prohibited material.

The purpose of this statutory exemption is:

- To recognise that where internet intermediaries play an entirely passive role in the facilitation of a publication (similar to a telephone line or postal service in the analogue world), they should not be liable as publishers for the purposes of defamation law
- To provide certainty to these internet intermediaries that they are not at risk of being subject to a defamation claim
- To provide certainty to complainants regarding which internet intermediaries should not be approached for a remedy for damage to reputation from defamatory matter

The definitions of caching, conduit and storage service will do most of the work in restricting eligibility for the exemption in accordance with the policy intent. However, the limiting principles should operate as a safeguard to ensure that none of the services are able to access the exemption if they are acting beyond their standard functions.

Mere conduits, including ISPs

Based on the 'mere conduit' analogy with telephone lines and postal services and on case law elsewhere, it is generally presumed that an ISP which does no more than carry content, is not a publisher.

The relevant Commonwealth definition is now in the *Online Safety Act 2021* (OSA): 'if a person supplies, or proposes to supply, an internet carriage service to the public, the person is an *internet service provider*'.[26]

There is broad support from stakeholders for a statutory exemption applying to ISPs. Generally it is already assumed they would not be considered publishers for the purposes of defamation law, so there would appear to be minimal risk in affording them an exemption.

ISPs fall within the definition of a 'mere conduit'[27]. This is a 'service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network'.

In the EU, a mere conduit is not liable for the information transmitted, provided it does not a) initiate the transmission, b) select the receiver of the transmission, and c) select or modify the information contained in the transmission. This is so long as the acts of transmission and provision of access include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided it is not stored for any period longer than is reasonably necessary for the transmission.

Other examples of functions that fall within the EU DSA Article 3 definition of mere conduit are email services and providers of Wi-Fi.[28]

It is proposed that the statutory exemption be accorded to mere conduits as understood by EU DSA Article 3, in order to capture these and any other like internet intermediary functions.

Storage services

There are other internet intermediary functions that, like ISPs, are remote from the publication of defamatory content online. These are services that provide storage facilities but do not engage with the content. They are generally not the subject of defamation claims. Examples of these kinds of functions are web and cloud hosting service providers. They would include services that provide email storage and access, and document storage and access.

These services aim to store material and make it available online, but are remote from the content and the publication of that content to a wide audience. It is proposed that these functions should also be covered by the statutory exemption.

Caching services

Caching services store online data or files in a temporary location – so they can be accessed quickly. The EU's E-Commerce Directive/proposed new EU DSA[29] defines caching as a service that 'consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request'.

Under Article 4, caching services are not liable for the storage of this information, subject to a number of conditions – including that they do not modify the information and that they act expeditiously to remove or disable access to it upon obtaining actual knowledge that the information at the initial source of the transmission has been removed from the network, or access

[26] Section 19(1) *Online Safety Act 2021*.

[27] Article 3 proposed EU DSA/Article 12 E-Commerce Directive.

[28] Tomlinson & Vassall-Adams (eds) (2017) *Online Publication Claims: A Practical Guide*), Chapter 7 para 7.20.

[29] Article 4 proposed EU DSA/Article 13 E-Commerce Directive.

to it has been disabled, or a court has ordered as such.

The proposed statutory exemption from liability in defamation law would not include a condition that the caching service remove or disable access to content when notified it has been removed at the initial source of transmission. The reason for the difference is that the EU provisions regulate the conduct of internet intermediaries in relation to all types of content. Imposing this kind of obligation on caching services is appropriate in relation to other types of material such as hate speech, terrorist content or child sexual abuse material. It should be noted though that Recommendation 5 would ensure that the courts have the power to order that all internet intermediaries remove or disable access to defamatory matter – even when not a party or otherwise liable.

There are some indications that search engines may fall within the EU DSA Article 4 definition of caching services.[30] In *Mosley v Google Inc* [2015] EWHC 59 (QB) Justice Mitting held that Article 13 of the E-Commerce Directive (to be reflected in Article 4 of the proposed new EU DSA) 'affords legal protection to internet service providers such as Google who 'cache' information and images'.[31]

Although this may result in some overlap, in the interests of certainty, a separate statutory exemption for search engines is proposed in Recommendation 2.

Services that store content

In addition to caching, there are other services that enable the 'back end' storage of data, for example for a website, social media or email service or file storage (including limited distribution sharing facilities). Unlike the 'front end' services though, they do not disseminate information. These are the kind of services that are covered by:

- the Commonwealth OSA definition of hosting service (section 17) (see Appendix C), and
- the definition of 'hosting' in the EU's E-Commerce Directive (Article 14) /proposed new EU DSA (Article 5)

It is proposed that for the purposes of the statutory exemption, the phrase 'storage services' be used. This is because concerns have been raised by stakeholders about the unclear application of the term 'internet content host' that was previously in the *Broadcasting Services Act 1992* (Cth).[32]

Also, the EU's definition of 'hosting' also includes a broader range of functions such as social media platforms – that should certainly not be captured by the proposed exemption.

It is important to make clear that while functions such as web and cloud service providers would be covered by the exemption, other internet intermediaries sometimes referred to as 'hosts', such as individuals or organisations administering discussion forums, would not be covered.

Benefits and risks

Benefits

- Certainty for protected internet intermediaries that they are not at risk of being sued for defamation in relation to third-party content
- Certainty for complainants regarding which internet intermediaries they can and cannot approach for a remedy
- It should prevent protected internet intermediaries simply removing content in order to avoid liability

[30] Tomlinson & Vassall-Adams (eds) (2017) *Online Publication Claims: A Practical Guide*, Chapter 7 para 7.23, 'The most important kind of Information Society Service provider covered by the caching exemption is a search engine' citing *Mosley v Google Inc*.

[31] *Mosley v Google Inc* [2015] EWHC 59 (QB) para 32.

[32] 'A person who hosts content in Australia, or who proposes to host internet content in Australia'. This has been replaced by 'Australian hosting service provider' which means 'a person who provides a hosting service that involves hosting material in Australia' in section 5 of the OSA.

Risks

- It could be argued this is not necessary, as these internet intermediary functions are unlikely to be considered publishers (although this also means there is limited risk of curtailing complainants' access to a remedy)
- Where an internet intermediary function is covered by the exemption, this will mean it has no incentive to respond to a complaint or request in relation to defamatory content. The only way a complainant would be able to seek its assistance is through a court order. Recommendation 5 would provide courts with the power to issue orders in these circumstances

Recommendation 2: Conditional, statutory exemption from defamation liability for standard search engine functions

See draft Part A MDAPs Sch 1 [2], draft section 9A

Introduce a new statutory exemption from liability in defamation law for:

- the use of automated tools to search the internet to return search results, identifying and linking to third-party websites, based on the search terms input by users

The statutory exemption would apply irrespective of whether the search engine is made aware of the allegedly defamatory content. This is a very broad protection so the immunity would apply on the basis that:

- the search engine's role in the process of publishing the matter is of a solely technical and automatic nature
- in performing its function, the search engine has no monetary or other particular interest in promoting the content outside of the search engine's normal functioning

In any defamation proceedings, the statutory exemption is to be determined by a judicial officer. It should be determined as soon as practicable before the trial commences unless the judicial officer is satisfied there are good reasons to postpone the determination to a later stage.

Stakeholder views on an exemption for search engine functions

The Stage 2 Discussion Paper asked a number of questions about search engines, including if they should be considered as a separate category to other internet intermediaries.

It used the Australian Competition and Consumer Commission's definition of search engines as 'software systems designed to search for information on the World Wide Web, generally returning a curated, ranked set of links to content websites'. It also referred to the point made by Riordan in his taxonomy of internet intermediaries that 'while these services employ various means to locate and rank relevant material, they are united by their reliance upon automated tools and algorithms to parse, store and query large volumes of data authored by others'.[33]

The Stage 2 Discussion Paper also noted that search engines, unlike many social media platforms where users directly post content, often do not have a relationship with the originator of the content. However, they can allow third parties to pay to promote their content and have it featured higher in the list of search results.

A number of stakeholders submitted that search engines should be accorded immunity because they simply use algorithms to return search results based on a user's search query. One stakeholder noted they have no control over the search query or the content on indexed websites – they only

[33] Riordan, J. 2016, *Liability of Internet Intermediaries*, Oxford University Press at 43.

have control over the search algorithm. Other factors put forward to support the argument that search engines should be accorded immunity are:

- The inability of search engines to remove content from the internet (they can only block access to identified URLs from their search engine)
- The massive scale of search engine functions
- The significant social and economic value that search engines contribute to society
- Unlike a social media platform, a search engine does not have any relationship with the originator so is not able to connect them with the complainant.

Other stakeholders submitted that search engines should not be given special treatment because they provide functionality beyond the neutral provision of search results. Some argued they do have control over content, and that they play an active role through the design of their algorithms which rank and display results. It was also suggested that the role they play in disseminating and amplifying material impacts the extent of reputational damage.

Finally, the Stage 2 Discussion Paper asked whether search engines have different functions, some of which should give rise to liability, and some of which should not. Examples of these functions include indexing of content, ranking results, auto populating search terms, and providing snippets and highlights.

Search engine providers submitted that it is not appropriate to split the functions of a search engine as they are part of a single process to provide search results in response to user queries. Other stakeholders submitted that the liability of internet intermediaries should be determined by reference to the functions they perform in relation to the publication in question.

Key features of a conditional exemption for standard search engine functions

Search engines have been the subject of a number of defamation claims in Australia. The High Court has confirmed that a search engine may be a publisher of search results.[34] This means that providing a statutory exemption to search engines would represent a significant change.

However, the treatment of search engines in Australia diverges from other comparable jurisdictions, in particular the UK. In *Metropolitan International School Ltd v Designtechnica Corp*[35] the Court found that Google, as operator of its search engine, was not a publisher of snippets in search results. Based on the facts, Google had not authorised or caused the snippet to appear on the user's screen in any meaningful sense; it was only a facilitator and there had been no human input.

In the Canadian case of *Crookes v Newton*, the Court held that a mere hyperlink can never be a publication of its contents, as this would have a chilling effect on the internet.[36]

The E-Commerce Directive has been interpreted variously in each EU state's courts and legislatures, and consequently there is a lack of consistency in the EU in relation to search engine liability. It appears that domestic state courts have to date variously found that Google is either not liable for, or liable only on actual notice of, defamatory material indexed in search results, or snippets containing defamatory material in those search results.[37] Some EU domestic legislatures have introduced varying forms of defences or complete immunities for search engines.[38] The lack of recent case law may be due to complainants now preferring to frame their complaints under privacy

[34] *Trkulja v Google LLC* [2018] HCA 25.

[35] *Metropolitan International School Ltd v Designtechnica Corp* [2009] EMLR 27 (QB).

[36] *Crookes v Newton* [2011] 3 SCR 269 per Abella J at 285 [27] (with whom Binnie, LeBel, Charron, Rothstein and Cromwell JJ agreed).

[37] In *Metropolitan International Schools Ltd v Designtechnica Corp and Google* [2009] EWHC 1765 (QB) at [100] and [110] respectively, Eady J refers to a lower Spanish court decision, *Palomo v Google Inc* (2009), which appeared to hold that Google was not responsible for publishing hyperlinks to defamatory content, or at least not without 'actual knowledge', and to a French Court of Appeal decision in 2009 where the court held that Google was not under a duty to monitor the lawfulness of websites it indexes.

[38] A summary of these immunities is outlined in *Metropolitan International Schools Ltd v Designtechnica Corp and Google* [2009] EWHC 1765 (QB) at [97]-[114].

and data protection laws, in particular, the 'right to be forgotten',[39] in seeking the de-indexing of search engine results.

Google's liability for autocomplete suggestions in EU states is also disparate. In states where there is no legislative immunity for search engines, some EU courts have found Google liable, subject to the notice and take down requirements, either under the caching defence in Article 13 or the hosting defence in Article 14.[40] However, other EU courts have found that Google is not liable as a publisher of autocomplete suggestions.[41] The EU DSA will facilitate a more harmonised approach in the EU by incorporating the existing E-Commerce Directive defences as mandatory EU level text in new Articles 3-5.

It is proposed that a new statutory exemption from liability in defamation law be introduced for:

- the use of automated tools to search the internet to return search results, identifying and linking to third-party websites, based on the search terms input by users

The search result might include the title of the webpage and a hyperlink to it, a short extract and an image.

The rationale is that in performing these functions, search engines have no interest in the specific content. The publication of the search results is prompted in the first instance not by the search engine but by the user typing in a search query for which the user is also the recipient. The search results simply provide access to third-party content generated by an automated process.

However, search engines are highly sophisticated and constantly evolving. There are some existing functions that go beyond the description above and most likely there will be others in the future. One example is autocomplete suggestions which involve more interested engagement and responsibility on the part of the search engine. This involves a search engine predicting the user's search with reference to other users' common searches, which may create a suggestion that is itself defamatory. While this is done by algorithm, it is not a search engine function that simply connects the user to the webpage of a third party. The use of algorithms in this case generates suggested word associations that may be highly defamatory – and importantly, that the search engine has the ability to remove. This would not fall within the parameters of standard search functions that are able to access the exemption.

The risk of the exemption applying too broadly to functions that are not content neutral would be mitigated largely by the specific description of the search engine function used. However, it is also important to have limiting principles, making clear that the exemption would apply on the basis that:

- the search engine's role in the process of publishing the matter is of a solely technical and automatic nature
- in performing its function, the search engine is content neutral – it has no monetary or other particular interest in promoting the content outside of the search engine's normal functioning

These limiting principles delineate the purpose and scope of the exemption in the context of complex and interactive search engine functions. It is also to highlight that if the relevant function performed by a search engine did not fall within the exemption – it would still be able to rely on one of the proposed new defences (Recommendations 3A and 3B).

[39] Article 12 of the *Data Protection Directive* (Directive 95/46/EC), as applied in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) [ECLI:EU:C:2014:317].

[40] See the German, French and Italian court decisions referenced in Karapapa, S and Borghi, M, 'Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm' (2015) 23(3) *Int J Law Info Tech* 261-289, para 6.1, footnotes 70-87.

[41] See A Christie, 'Swiss Court finds Google not liable for suggested search terms', 25 August 2012, available at http://achristie.com/swiss-court-finds-google-not-liable-for-suggested-search-terms/; Karapapa, S and Borghi, M, 'Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm' (2015) 23(3) *Int J Law Info Tech* 261-289, para 6.2, footnotes 101, 102, 104.

Benefits and risks

Benefits:

- The exemption would recognise that in performing standard functions, search engines should not be liable as publishers for the purposes of defamation law
- It would provide certainty for search engines that, in performing their standard functions, they are not at risk of being sued for defamation in relation to third-party content
- It would avert the risk of search engines de-listing results that link to legitimate material in order to avoid liability (especially where this is requested for ulterior reasons)

Risks:

- Search engines would have no incentive to respond to a complaint or request in relation to search results. This could be a problem where the matter in question has gone viral – or the originator or other internet intermediaries will not remediate despite having been found liable. The only way a complainant would be able to seek assistance from the search engine is through a court order. Recommendation 5 would provide courts with the power to issue orders in these circumstances.

Recommendations 3A and 3B: Two alternative options for a new defence for internet intermediaries

Overview of Recommendations 3A and 3B – new defence for internet intermediaries

One of the impetuses for the Stage 2 Review is that the current state of defamation law in relation to internet intermediary liability for third-party content is unclear and inconsistent.

Defamation law, and the MDPs, were developed in the context of traditional publishers. 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.[42]

The Stage 2 Discussion Paper noted that within the existing architecture of the MDPs, the statutory defences are there to limit or preclude liability where there is a public policy reason for doing so. The ultimate aim is to strike the right balance between the objects of the MDPs.

The options for reform set out in the Discussion Paper to clarify or modify the liability of internet intermediaries in respect of third-party content include:

- Option 2: Clarify the innocent dissemination defence in relation to digital platforms and forum administrators
- Option 3: Safe harbour – subject to a complaints notice process

For the most part, stakeholder submissions supported the introduction of a new defence, although there was a range of views regarding Options 2 and 3, as well as a number of alternative suggestions. Based on the analysis below, the DWP recommends a new defence, responding to the issue of internet intermediary liability for third-party content.

Two **alternative** models are considered the most viable and are proposed for consideration:

- Model A: A safe harbour defence for internet intermediaries focused on connecting the complainant with the originator

or

- Model B: A new innocent dissemination defence recognising that internet intermediaries should have a defence in defamation in relation to third-party content until the point where they are given a written complaints notice and after that, if they remove the content within 14 days.

[42] See *Fairfax Media Publications Pty Ltd & Ors v Voller* [2021] HCA 27; *Fairfax Media Publications Pty Ltd & Ors v Voller* [2020] NSWCA 102; *Voller v Fairfax Media Publications Pty Ltd & Ors* [2019] NSWSC 766; *Defteros v Google LLC* [2021] VSCA 167 (the High Court has granted special leave to appeal the Victorian Court of Appeal decision); *Google LLC v Duffy* [2017] SASCFC 130.

The purposes of Models A and B are different. The primary purpose of Model A is to focus the dispute between the complainant and the originator. The purpose of Model B is to provide a clearer and more certain innocent dissemination defence for the benefit of both complainants and internet intermediaries.

In line with the different purposes, under Model 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. This is not the case for Model B.

This is illustrated by the following hypothetical scenario. Under their own name, a competitor posts defamatory reviews about a sole trader on a review website. Under Model A, because the originator was easily identifiable, the review website (the internet intermediary) would have a complete defence and would not be liable in defamation. The complainant could only pursue the originator for a remedy. In other words, the internet intermediary would be protected by the safe harbour of the defence, because the originator was identifiable to the complainant. Under Model B, the complainant could seek a remedy from the originator, the internet intermediary or both.

Another point of difference is that under Model A, the internet intermediary has two options for obtaining the benefit of the defence. The first option is to provide to the complainant, with the poster's consent, sufficient information to enable a concerns notice to be given to the poster or proceedings to be commenced against the poster. The second option is to take reasonable access prevention steps in relation to the publication (if there are any). By contrast, the only way the internet intermediary can obtain the benefit of the defence under Model B is to take reasonable access prevention steps (if there are any).

Under Model A, if the internet intermediary provides to the complainant, with the poster's consent, sufficient information to enable a concerns notice to be given to the poster or proceedings to be commenced against the poster, then the internet intermediary can keep the content online and obtain the benefit of the defence. Under Model B, the internet intermediary must always take reasonable access prevention steps in relation to the publication (if there are any).

Both models have significant advantages and disadvantages and these are explored below. Draft MDAPs have been prepared for each option for public consultation.

Recommendation 3A: Model A – safe harbour defence for digital intermediaries, subject to a simple complaints notice process (Alternative to Recommendation 3B)

See draft Part A MDAPs Sch 1 [6], draft section 31A

Introduce a defence for publications involving digital intermediaries (Model A). The purpose of Model A is to focus the dispute between the complainant and the originator.

Elements of the defence

It would be a defence to the publication of defamatory digital matter if the defendant proves:

- it was a digital intermediary in relation to the publication (that is a person, other than the author, originator or poster, who provided an online service in connection with the publication of the matter),
- at the time of the publication, it had a mechanism that was easily accessible by members of the public for submitting complaints notices, and
- if the complainant duly gave the digital intermediary a complaints notice — within 14 days the digital intermediary either:
  a) with the poster's consent, provided the complainant with sufficient information to enable a concerns notice to be given to the poster or proceedings commenced against the poster, or

b) took the access prevention steps in relation to the publication, if any, that were reasonable in the circumstances.

In order to obtain the poster's consent, the internet intermediary would need to provide the poster with a copy of the complaints notice. This is so the poster has sufficient information based on which they can choose to defend the publication.

Safeguard for good behaviour

A digital intermediary would not be ineligible for the defence solely because it took steps to detect, identify or prevent access to defamatory content, unlawful content or content incompatible with its terms of service.

Malice exclusion

The defence would be defeated if the complainant establishes that the defendant was actuated by malice in providing the online service used to publish the digital matter.

Complete defence where complainant can identify the poster

A complaints notice may only be given if, after taking reasonable steps, the complainant was not able to obtain sufficient information to enable a concerns notice to be given to the poster or proceedings to be commenced. A complainant would not be expected to hire a private investigator or seek an order for substituted service or preliminary discovery to meet the reasonable steps requirement.

The complaints notice

The prescribed information for a complaints notice would be:

- the name of the complainant
- the location where the matter can be accessed (for example, a webpage address)
- an explanation of why the complainant considers the matter to be defamatory and if the complainant considers the matter to be factually inaccurate, a statement to that effect
- the serious harm to reputation caused, or likely to be caused by the publication of the matter
- the steps taken to identify the poster

Stakeholder views on a safe harbour defence for internet intermediaries

The Stage 2 Discussion Paper identified the UK safe harbour subject to a complaints notice process as a potential model for Australia. It explained that the purpose of this defence is to focus the dispute between the complainant and the originator. A complaints notice process can provide complainants with a means of being connected with the originator of a defamatory post (where their identity is not apparent) or where the originator cannot be identified, then for the offending content to be removed. At the same time, by requiring the internet intermediary to play a role in facilitating access to a remedy, the defence recognises that internet intermediaries have some responsibility for content posted on their platforms.

The UK safe harbour is established by section 5 of the *Defamation Act 2013* (UK). Section 5 provides:

5 Operators of websites

1) This section applies where an action for defamation is brought against the operator of a website in respect of a statement posted on the website.
2) It is a defence for the operator to show that it was not the operator who posted the statement on the website.
3) The defence is defeated if the claimant shows that—
   a) it was not possible for the claimant to identify the person who posted the statement,
   b) the claimant gave the operator a notice of complaint in relation to the statement, and
   c) the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.
4) For the purposes of subsection (3)(a), it is possible for a claimant to 'identify' a person only if the claimant has sufficient information to bring proceedings against the person.

The regulations prescribe a number of steps with specific timeframes. They include the complainant submitting a complaints notice to the internet intermediary, the internet intermediary contacting the poster and the internet intermediary removing or keeping online the content depending on the poster's response.

New Zealand also has a safe harbour subject to a complaints notice process with similarities to the UK model.[43]

Many stakeholders supported the introduction of a safe harbour subject to a complaints notice process but there were very different views regarding the details.

There was general agreement that an internet intermediary cannot form a view on the merits of a complaint because it lacks the contextual information to determine whether the matter is indefensibly defamatory.

A number of legal stakeholders supported the adoption of a defence similar to the UK model or with some material changes. Technology sector stakeholders generally opposed the adoption of the UK model. Some submitted that acting as a 'go-between' between complainants and originators was inappropriate. A number stated that internet intermediaries rarely used the UK defence because it is cumbersome and they either remove the material or rely on other defences.

There were also different views among stakeholders regarding the purpose of a safe harbour subject to a complaints notice process. Legal stakeholders generally agreed that the purpose of a complaints notice process should be to connect the complainant and originator. Some legal stakeholders went further and noted that another objective of a complaints notice process should be to provide a remedy for complainants even where the complainant already has sufficient information to bring proceedings against the originator. A number of technology sector stakeholders were of the view that a complaints notice process should be a last resort process once others have been exhausted.

[43] See sections 24 and 25 of the *Harmful Digital Communications Act 2015* (NZ).

Another issue is which types of internet intermediaries are capable of complying with a complaints notice process. A number of stakeholder submissions identified the internet intermediaries' capacity to contact the originator as a critical issue and on this basis argued that a complaints notice process should not apply to search engines. Some stakeholders submitted that the different capacities of different forum administrators to manage a complaints notice process was also a relevant consideration.

A number of technology sector stakeholders submitted that the protection of anonymous speech is important and that a complaints notice process should not involve the internet intermediary removing the content when the originator does not consent to their contact details being provided to the complainant.

Key features of Model A – safe harbour defence for digital intermediaries, subject to a simple complaints notice process

The primary purpose of Model A is to focus the dispute between the complainant and the originator. Two aspects of the defence are important in this regard:

1) It provides that an internet intermediary has a complete defence if the complainant has sufficient information to give a concerns notice to the poster or commence proceedings against the poster.
2) Where this is not the case, the intermediary has a defence if they provide to the complainant (with the poster's consent) sufficient information to enable a concerns notice to be given to the poster or proceedings to be commenced against the poster. This will require the intermediary to contact the poster and seek sufficient details to provide to the complainant.

If neither 1 nor 2 apply, the intermediary has a defence if it takes steps to prevent access to the publication, if any, that are reasonable in the circumstances within a set time period.

Model A reflects some aspects of the UK section 5 defence but is given effect by adapting a model proposed by the NSW Bar Association (see **Appendix B**).

Unlike the UK section 5 regime, the Model A complaints notice process would not be prescribed. The rationale is to provide the internet intermediary with flexibility as to whether they choose to seek the consent of the poster to pass on their details to the complaint, and how they do this.

An important adjunct to this defence is that it would be subject to a new court power providing that, where a court grants an interim or final order or judgment against the poster or originator, the court may order an internet intermediary to remove or disable access to defamatory material within the scope of such order or judgment. This is covered by Recommendation 5.

Application

The defence would be available to a digital intermediary. It includes a person, **other than an author, originator or poster of the matter**, who provides an online service in connection with the publication of the matter. Online service is defined very widely to encompass all of the internet intermediary functions in the scope of the Stage 2 Review. So this includes social media platforms, review websites and forum administrators (to name a few).

The purpose of excluding the 'poster', 'author' or 'originator' of the content is to ensure the defence only applies where the person providing the service is acting as an intermediary – and therefore, is a secondary publisher. So for example, if a social media platform or a forum administrator published an article or a statement online – they would not meet the definition of 'digital intermediary'.

The term 'poster' is connected to the term 'post' which is defined to mean 'the use of an online service to communicate the matter to 1 or more persons'.

The terms 'author' and 'originator' are used in the existing innocent dissemination defence at section 32 of the MDPs. The concept of 'author' is intended to cover circumstances such as where the person who writes a defamatory statement is not the person who posts it. The word 'originator' is intended to include anyone who plays a role in creating the content. Often, they may also be the poster. But in some circumstances, they may not. For example, if a group of people create and edit a video together before it is posted online. Or if a person edits and endorses a statement that is drafted and posted by another person. Doing any of these things would mean that a person does not meet the definition of digital intermediary.

Safeguard for good behaviour

Importantly, a digital intermediary would not be ineligible for the defence solely because they practise good online moderation that is they take steps to detect, identify or prevent access to defamatory content, unlawful content or content incompatible with their terms of service.

The rationale for providing that this does not render a digital intermediary ineligible for the defence is to ensure that good behaviour is not disincentivised. Without such a provision, there is a risk that these activities could be considered to cause the digital intermediary to become an originator and ineligible for the defence. This could deter digital intermediaries from performing this beneficial function. The framing of this aspect of the defence draws on Article 6 of the EU DSA.

Exclusion where there is malice

The internet intermediary will be unable to rely on the defence if it was actuated by malice in providing the online service. This is to cover circumstances where the intermediary invited the publication of the defamatory matter with an improper motive or they created, provided or administered the forum / platform on which the matter was published with an improper motive. By way of example, this is intended to deny the following intermediaries access to the defence:

- A person who establishes a Facebook group entitled 'Principal X is a terrible school principal – list his faults here so we can get him fired' in which a user states that Principal X is unqualified when he in fact is qualified
- A social media platform launches in Australia with the promotional tagline 'Free speech, no take down, to the limit of the law'. Users are encouraged to use pseudonyms, and no contact details or identity are required. Thousands of users register and post egregious defamatory allegations about identifiable people. The platform's defamation moderation policy is as follows: Where a prescribed form defamation complaints notice is received, the platform does not respond to the complainant, contact the originator or review the merits of the complaint. There is no human moderation or legal assessment. Rather, the material is automatically deleted no earlier and no later than a minute before the expiry of the 'immunity' period [14 days].

However, this exception is not intended to deny, for example, the following intermediaries access to the defence:

- A person who establishes a Facebook group entitled 'Collins Street School Parents Group' in which a user states that Teacher Y is a paedophile when she in fact is not
- A news media company that maintains a public Facebook page on which it posts a news story about a sportsperson's performance in a recent sporting competition and a Facebook user posts that the sportsperson uses illegal performance enhancing drugs when in fact they do not

'Malice' is considered an appropriate concept for articulating this exception. Malice is a well-established concept within defamation law as a circumstance which may defeat certain defences.

Courts have to date been able to adapt the concept of malice to capture a variety of situations. This flexibility may assist in capturing new types of digital intermediaries, forums and platforms which

cannot at this time be identified but which should not have the benefit of the defence.

It is also worth noting that the UK safe harbour subject to a complaints notice process uses the concept of malice – the UK defence is defeated if the complainant shows that the operator of the website has acted with malice in relation to the posting of the statement concerned[44]. However, there is no case law as yet on the provision.

When it is possible for the complainant to identify the poster

Model A provides an automatic defence where it was possible for the complainant to identify the poster. This means where the complainant had sufficient information to issue a concerns notice to the poster or commence proceedings against the poster or could, by taking reasonable steps other than seeking an order for substituted service or preliminary discovery, get that information. The steps intended to be covered include using a simple internet search and using publicly available information, such as a business register. The steps are not intended to include more onerous tasks, such as obtaining preliminary discovery orders, substituted service orders or using a private investigator.

Section 44 provides for means of giving a concerns notice. For each means, the complainant requires certain contact details. For example, to give a concerns notice to a natural person by post, the complainant must have the person's name and the address specified by the person for the giving or service of documents or, if no such address is specified, the residential or business address of the person last known to the complainant.

To enable the internet intermediary to determine whether it can rely on the defence on the basis that it was possible for the complainant to identify the poster, it is recommended that the complaints notice must set out the steps taken by the complainant to identify the poster.

Complaints notice

The complaints notice is intended to give the internet intermediary actual notice of the complaint. The recommended information for the complaints notice seeks to balance providing the internet intermediary and poster with sufficient information to understand the core components of the complaint and enabling a complainant to prepare a complaints notice quickly and without legal advice.

Online publications generally involve the participation of multiple internet intermediaries. This means the complainant would have the option of giving a complaints notice to any (or all) of the internet intermediaries involved (unless they qualify for one of the proposed exemptions under Recommendations 1 and 2).

The general requirement that the internet intermediary provide an easily accessible complaints mechanism is intended to be broad and to ensure that the complainant has a means of giving the notice to the intermediary. It is intended to include, for example, an email address and an appropriately designed online form. For a forum administrator, it could simply include a means of messaging the person (or organisation) on the platform. The purpose of the requirement is to prevent an internet intermediary from deliberately making it difficult for a complainant to provide the notice, so that the intermediary can have the benefit of the defence. A similar requirement exists in the New Zealand legislation.[45]

The complainant would be considered to have given the internet intermediary the complaints notice if they had submitted it through the dedicated easily accessible mechanism or in accordance with section 44 of the MDPs, which addresses the giving of notices and other documents for the purposes of the MDPs generally. The reason for allowing the complaints notice to be submitted also pursuant to section 44 is to avoid digital intermediaries denying that they have been given a complaints notice for the purposes of the defence provision and therefore that they have the benefit

[44] Section 5(11), *Defamation Act 2013* (UK).

[45] See section 25(2) of the *Harmful Digital Communications Act 2015* (NZ).

of the defence even when the complainant has given the internet intermediary a complaints notice through another means.

Obtaining consent of the poster

The rationale for Model A is that a poster should have the opportunity to defend their publication, and to focus the dispute between the complainant and the poster.

A crucial step in Model A is that the internet intermediary notify the poster of the substance of the complaints notice, and seek the poster's consent to provide their contact details to the complainant. It is intended that the internet intermediary would contact the poster and seek their consent in relation to each individual complaints notice, rather than through use of a more generalised agreement (for example via their terms and conditions). It is not intended that the digital intermediaries would collect or hold any additional personal information of its users in order to comply with this obligation. The internet intermediary can choose how they contact the poster, including via the intermediary's existing communication channels. For example, a forum administrator could use the message facility on a platform to provide the complaints notice to the poster and seek their consent to provide contact details to the complainant. Seeking the poster's specific consent before disclosing their contact details to the complainant will assist in protecting the poster's privacy and anonymity.

Time period

The purpose of the 14 day time period is to balance the complainant's need for a prompt outcome and sufficient time for the intermediary and poster to assess the complaint and take the necessary steps. In describing a similar model, the NSW Bar Association (see Appendix B) and the Law Council suggested a 28 day period.

14 days is similar to the 9 business days to complete the UK complaints notice process, noting this has attracted criticism for being too short for a complex process. Given that Model A does not prescribe the complaints notice process in the way the UK legislation does, 14 days is recommended.

Removing the matter where the poster does not consent to their details being provided

If the poster does not respond to the internet intermediary regarding the complaints notice, or does not agree to their details being shared with the complainant, the internet intermediary must either:

- take the access prevention steps in relation to the publication, if any, that are reasonable in the circumstances (in order to rely on the Model A defence); or
- leave the matter online and rely on other defences available in defamation law to defend the matter.

This would also apply if the internet intermediary has no means of contacting the poster.

Model A requires the internet intermediary to take the access prevention steps, if any, that are reasonable in the circumstances. This means steps to remove, block, disable or otherwise prevent access by some or all persons to the matter. It is intended that these steps will be reasonable in the circumstances, taking into account the internet intermediary's capacity to do this in relation to the specific publication. The onus of proving that the reasonable access prevention steps have been taken will lie with the intermediary.

Anonymous/pseudonymous speech and removal of matter

In some circumstances a person may be publishing material online pseudonymously for good reason. This might include whistleblowing or a political activist from another country highlighting human rights violations in their home country. However, anonymity/pseudonymity can also be exploited to defame with perceived impunity. Consistent with the objects of the MDPs, these reforms aim to balance the need to provide effective and fair remedies for harm to reputation without unreasonably limiting freedom of expression – particularly on matters of public interest.

One risk with Model A is that to some degree, legitimate anonymous and pseudonymous speech may be stifled. If a poster does not consent to disclose their identity to the complainant, the internet intermediary may defend the material itself – perhaps using a qualified privilege or public interest defence. Some digital intermediaries, such as review websites, may have policies and processes in place to assess the material, whether it is defensible and when the internet intermediary will remove it or keep it online. Or it may be incentivised to remove the content in order to have the benefit of the defence. This could be problematic for an anonymous poster who holds a genuine belief that their assertions are in the public interest but does not wish to disclose their identity due to a legitimate fear for their own safety or wellbeing.

While this may be a valid concern, it is noted that there may be other avenues for a poster to communicate such information that is in the public interest. For example, in relation to criminal conduct, the poster can report the matter to police. Discriminatory conduct may be reported to a human rights commission. A poster might convey the matter to a journalist who then publishes the matter without revealing the source. Also, whistleblowing often involves making allegations about an organisation, rather than an individual; generally corporations do not have a cause of action for defamation.

It should be noted that Part B of the Stage 2 Review aims to address the potential chilling effect that defamation (or the threat of it) has on reporting of alleged unlawful conduct such as sexual assault and sexual harassment to police and other statutory investigative bodies.

Benefits and risks

Benefits

- Where the poster consents to their details being provided, the complainant may avoid the time and cost of a obtaining a preliminary discovery order
- Ensures the poster has an opportunity to defend the matter
- Recognises the role of many digital intermediaries in providing a platform for publication of third-party content. Their services often enable content to reach large audiences. It appropriate that they play a part in resolving the dispute to obtain protection
- Actual notice of the matter in question is required in order for the internet intermediary to be (potentially) liable
- The internet intermediary would have a clear timeframe and sufficient information based on which they may choose to defend the material

Risks

- Stakeholders have submitted that often, the poster will not consent to provide their contact details – or may not respond at all
- If the complainant can identify the poster, but the poster is impecunious, they will have no recourse to the internet intermediary for damages
- There is some community expectation that digital intermediaries take responsibility for defamatory content posted by users. The opportunities to defame on a large scale would be far fewer without them. They derive profits from users posting comments. Providing a complete defence where the complainant can identify the poster may not be consistent with this expectation
- There is a risk of lawful material being removed if the poster is unresponsive or not willing to share their contact details

Recommendation 3B: Model B – innocent dissemination defence for digital intermediaries, subject to a simple complaints notice process (Alternative to Recommendation 3A)

See draft Part A MDAPs Sch 1 [7], draft section 31A

Introduce a new defence for publications involving digital intermediaries (Model B). The purpose of Model B is to recognise that internet intermediaries should not be liable for the publication of third-party defamatory content where they are merely subordinate distributors and are not aware of it.

Elements of the defence

It would be a defence to the publication of defamatory digital matter if the defendant proves:

- it was a digital intermediary in relation to the publication (that is a person, other than the author, originator or poster, who provided an online service in connection with the publication of the matter),
- at the time of the publication, it had a mechanism that was easily accessible by members of the public for submitting complaints notices, and
- if the complainant duly gave the digital intermediary a complaints notice — within 14 days the digital intermediary:
    - took the access prevention steps in relation to the publication, if any, that were reasonable in the circumstances.

Safeguard for good behaviour

A digital intermediary would not be ineligible for the defence solely because it took steps to detect, identify or prevent access to defamatory content, unlawful content or content incompatible with its terms of service.

Malice exclusion

The defence would be defeated if the complainant establishes that the defendant was actuated by malice in providing the online service used to publish the digital matter.

The complaints notice

The prescribed information for a complaints notice would be:

- the name of the complainant
- the location where the matter can be accessed (for example, a webpage address)
- an explanation of why the complainant considers the matter to be defamatory and if the complainant considers the matter to be factually inaccurate, a statement to that effect
- the serious harm to reputation caused, or likely to be caused by the publication of the matter

Stakeholder views on the innocent dissemination defence for internet intermediaries

The Stage 2 Discussion Paper explained that clause 32 of the MDPs provides a defence of innocent dissemination, which protects a 'subordinate distributor' from liability.

Sub-clause 32(2) provides that a publisher (using the broad common law sense of the term) is a 'subordinate distributor' if it:

a) was not the first or primary distributor of the matter,

b) was not the author or originator of the matter, and

c) did not have any capacity to exercise editorial control over the content of the matter before it was first published.

Without limiting this definition, sub-clause 32(3) includes a specific list of persons that are not the first or primary distributors of matter. This includes (for example) a bookseller, librarian, newsagent, and postal service.

In order to rely on the innocent dissemination defence, the defendant must also prove that they did not know, nor ought reasonably to have known that the matter was defamatory (sub-clause 32(1)(b)) and this lack of knowledge was not due to any negligence on the part of the defendant (sub-clause 32(1)(c)). This means that once a subordinate distributor is on notice of the defamatory matter, it risks losing the benefit of the innocent dissemination defence.

The Stage 2 Discussion Paper noted two key issues had been raised in relation to the current innocent dissemination defence:

- It is unclear which types of internet intermediaries would be considered 'subordinate distributors', particularly given that some may be considered to have the technical capacity to exercise editorial control
- It is not clear if knowledge that the matter was defamatory means that the subordinate distributor must have assessed the content to be defamatory or simply to have been notified that it is the subject of complaint (strict liability). Given this uncertainty, when content is the subject of a complaint, there is a strong incentive for an intermediary to simply remove the matter to avoid losing access to the defence.

Many stakeholders noted that the operation of the innocent dissemination defence is unclear. Some stakeholders submitted that the current defence is not fit for purpose and does not provide sufficient protection for internet intermediaries.

A common concern was that the innocent dissemination defence in practice incentivises internet intermediaries to remove speech, which can result in over-censorship.

While some suggestions were put forward for reforming the innocent dissemination defence, a number of stakeholders 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.

Other stakeholders opposed any change being made to the innocent dissemination defence. Reasons included that that the common law has already developed principles in respect of actual and constructive knowledge, and the courts are currently resolving live questions as to who may be considered a subordinate publisher. Such questions should be continued to be determined on a case-by-case basis by the courts.

Key features of Model B – innocent dissemination defence for digital intermediaries, subject to a simple complaints notice process

Model B would introduce a new actual notice based innocent dissemination defence for internet intermediaries in relation to third-party content. While Model B has a similar structure to Model A it differs significantly in that no automatic defence (or safe harbour) is granted to an internet intermediary where a complainant can identify the poster.

The defence would provide internet intermediaries with access to a complete defence while ensuring complainants are not denied a remedy for damage to their reputation by:

- Providing a complainant with a clear process for bringing the defamatory matter to the internet intermediary's attention and requesting it be addressed,
- Clarifying what constitutes notice (in the form of a complaints notice), and

- Providing the internet intermediary with a reasonable and clear period of time within which it must decide whether to remove the content or defend it.

Like the traditional innocent dissemination defence, Model B recognises the test for publication is broad, and there should be a distinction drawn between a primary and subordinate distributor.

However, the downside to the defence is intermediaries are usually unable to determine whether or not a claim is defensible, and so would be incentivised to remove material as the only sure way of defending claims.

Application

As with Model A (see above), the defence would be available to a digital intermediary. This includes a person, **other than an author, originator or poster of the matter**, who provides an online service in connection with the publication of the matter.

Model B also shares a number of other components with Model A:

- Requirement to have an easily accessible complaints mechanism
- Exclusion where there is malice
- Safeguard for good behaviour

Please see the commentary above in relation to Model A.

Knowledge

The test currently provided by section 32(1) of the MDPs is that a subordinate distributor 'neither knew, nor ought reasonably to have known' that a matter was defamatory, and that this lack of knowledge is not due to negligence.

Model B clarifies what constitutes knowledge of a defamatory matter for an internet intermediary: it is actual knowledge following the receipt of a complaints notice.

Also, by requiring a complaints notice to be served on an internet intermediary, good behaviour (for example volunteer 'moderating' of content) is not disincentivised. An intermediary is free to monitor content online without fear of being considered to have 'constructive knowledge', for example if an employee or an agent reads the content but does not recognise it as possibly defamatory. By requiring actual knowledge of defamatory content in the form of a complaints notice, the time clock for liability does not start ticking for these intermediaries until a complaints notice is given.

Complaints notice

Model B adopts the same requirements for the complaints notice as Model A except for one important difference. In Model B, the complainant does not have to include the steps taken to identify the poster. This is because the focus of Model B is not connecting the complainant with the poster and there is no safe harbour for digital intermediaries if the poster can be identified.

Timeframes

As above for Model A, the rationale for the 14 day period is to balance providing the internet intermediary with sufficient time to respond and providing the complainant with a fairly fast outcome.

If the internet intermediary decides not to take reasonable access prevention steps

If, after the receipt of a valid complaints notice, the internet intermediary decides not to take reasonable access prevention steps (and leaves the matter online), they have the option of defending the matter using any other defences available to them in defamation law.

Benefits and risks

Benefits

- Model B provides greater certainty and clarity than the current legal framework by treating digital intermediaries who are not posters, authors or originators of the content as 'secondary distributors'.
- Model B gives the complainant the option of seeking a remedy from the poster, internet intermediary or both. This would be particularly beneficial to complainants where the poster is recalcitrant or fixated, refuses to engage or fails to respond.
- The prescribed information in a complaints notice would assist digital intermediaries in their assessment of whether or not a matter is prima facie defamatory.
- Through the complaints notice, Model B provides complainants with a relatively fast and simple method to seek a remedy in relation to online defamatory content.
- By providing a stand-alone defence tailored specifically to digital intermediaries, Model B does not disturb the operation of the current clause 32 defence as it applies to offline subordinate distributors.

Risks

- Unlike Model A, Model B does not focus the dispute between the complainant and the poster.
- Model B also does not provide the poster with the opportunity to defend the content.
- In circumstances where a complainant cannot identify a poster, Model B requires the complainant to obtain a court order identifying the poster for purposes of negotiation or litigation.
- Digital intermediaries are often not well placed to determine whether matter indefensibly defamatory.
- Model B may create an incentive for a complainant to approach an internet intermediary to have legitimate content removed, rather than approach the poster who may refuse or defend the content. This could result in over-censorship and the removal of legitimate content.

Recommendation 4: Clarify interaction with the *Online Safety Act 2021* immunity

Recommendation 4: Commonwealth Government to consider an exemption for defamation law from the *Online Safety Act 2021* immunity

The Commonwealth Government should give close consideration to whether an exemption from section 235(1) of the *Online Safety Act 2021* for defamation law is desirable, in the interests of clarity of the law.

Introduction

Clause 91(1) of Schedule 5 to the BSA, inserted in 1999, provided an immunity for 'internet service providers' and 'internet content hosts' in certain circumstances in relation to third-party material (**BSA Immunity**).[46] It provided that a law of a state or territory, or a rule of common law or equity, had no effect to the extent that it:

- subjects an internet content host or internet service provider to liability for hosting or carrying 'internet content' where they are not aware of the nature of the internet content, or
- requires the internet content host or internet service provider to monitor, make inquiries about, or keep records of, internet content that is hosted or carried.

The Stage 2 Discussion Paper noted that there has been only limited judicial consideration of the BSA Immunity, focussing on the definition of 'internet content host'. 'Internet content host' was defined in the BSA as 'a person who hosts interest content in Australia, or who proposes to host internet content in Australia'.[47] 'Hosting' was not defined. Basten JA, in a 2012 decision considered that 'internet content host' might include 'any party in control of a website to which material has been uploaded'.[48] In the *Voller* proceedings His Honour expressed the view that 'the operator of a website or page on a platform which is able to control the content it makes available to internet users is properly described as hosting that content'.[49]

Since the release of the Stage 2 Discussion Paper, the Commonwealth Parliament has passed the OSA, which commenced on 23 January 2022. Clause 235(1) of the OSA (**OSA Immunity**) substantially replicates and replaces the BSA Immunity, with the substitution of the term 'Australian hosting service provider' for 'internet content host'. 'Australian hosting service provider' is defined in the OSA as 'a person who provides a hosting service that involves hosting material in Australia'.[50] Again, 'hosting' is not defined. There has been no judicial consideration of the OSA Immunity as it has only recently commenced.

Relevant extracts of the BSA and OSA are set out at **Appendix C**.

[46] Cl 91(1), Schedule 5, *Broadcasting Services Act 1991* (Cth).

[47] Cl 3, Schedule 5 BSA.

[48] *Fairfax Digital Australia & New Zealand Pty Ltd v Ibrahim* [2012] NSWCCA 12 at [90], per Basten JA, Bathurst CJ and Whealy J agreeing (a case concerning suppression orders).

[49] *Fairfax Media Publications & Ors v Voller* [2020] NSWCA 102 per Basten JA (obiter) at [21].

[50] Section 5 of the OSA.

Stakeholder views on the *Online Safety Act 2021* immunity

Responding to the Stage 2 Discussion Paper, a significant number of stakeholders identified that the interaction of the BSA/OSA Immunity with defamation law was uncertain.

The key areas of uncertainty highlighted by stakeholders were as follows:

- Which internet intermediaries are covered. In particular, it is unclear what functions are covered by the definition of 'internet content host' in the BSA or 'Australian hosting service provider' in the OSA
- Whether the term 'Australian hosting service provider' applies only to entities domiciled in Australia, or whether there can otherwise be a qualifying Australian nexus such as having servers located in Australia, or otherwise
- What constitutes 'awareness of the nature of' the online content defeating the OSA immunity (OSA, s 235(1)(a) and (c)), and how this corresponds with the concept of 'constructive' knowledge defeating the innocent dissemination defence (MDPs, cl 32(1)(b), and
- Whether the MDPs, or any order made by a court to enforce the MDPs, could infringe the prohibition against an obligation to actively monitor, make inquiries about, or keep records of third-party online content (OSA, s 235(1)(b) and (d)).

Some suggested that any amendment to the MDPs should be aligned with the knowledge test in the BSA Immunity. It was also suggested that an exemption for defamation law be sought under section 235(1) of the OSA.

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

Mere conduits and storage providers

Recommendation 1 is to introduce a new statutory exemption from liability in defamation law for mere conduits including ISPs, and to caching and storage service providers.

The definition of ISPs appears to be stable and well understood. Whether or not an exemption is introduced, it appears that the presence of the OSA Immunity is unlikely to impact on their liability under the MDPs.

In 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.

The Explanatory Memorandum for the Online Safety Bill 2021 identifies an example as 'where a person hosts stored material or content for a website, or an email service'. [51] Based on this description, 'mere' storage providers would be covered.

If Recommendation 1 is introduced, this would make the application of the OSA immunity to these internet intermediary functions irrelevant in the context of defamation law.

[51] Explanatory Memorandum to the Online Safety Bill 2021, p 77.

Other Australian hosting service providers

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)[52] – there would be some overlap between the OSA Immunity and the new safe harbour or innocent dissemination defence. Article 14 of the E-Commerce Directive, which is titled 'hosting', has been interpreted to include a wide range of intermediaries including social media and ecommerce services.[53]

In this context, alignment of the knowledge requirement is important. Under the OSA Immunity, a qualifying internet intermediary is not liable under a state law for third-party content carried or hosted by it unless and until it is 'aware of the nature of' the content. Under both models for the proposed new complaints notice for the safe harbour defence (Recommendation 3A) and innocent dissemination defence (Recommendation 3B) the internet intermediary would not be liable until after the prescribed period following receipt of a valid complaints notice. During the prescribed period, the intermediary can assess and if it wishes, make its own enquiries to evaluate the nature of the content. Under this analysis the complaints notice would meet the requisite threshold of awareness under the OSA immunity.

If the recommendations in this report are adopted, we consider that defamation law would provide defences to internet intermediaries that would not offend the OSA. To this extent, the law and policy of the reforms and the OSA are consistent.

Prohibition against obligation to monitor

One final consideration is that the OSA provides 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 (s 235(1)(b) and (d)). To the extent that a court orders that an intermediary must monitor to ensure that the same or similar content is not reposted or is removed where it has been shared by other users on the platform, it is unclear whether that prohibition would be enlivened. This issue is relevant to the proposed court power to make orders against intermediary non-parties (Recommendation 5).

While there have been no relevant decisions on this issue in Australia, a recent European Court of Justice decision[54] considered the validity of a court order requiring Facebook to remove from its platform content ruled to be defamatory of the complainant, including variations of such content with 'equivalent' meaning, regardless of which user uploaded that content. The Court held that such an order did not infringe the similarly worded prohibition under the E-Commerce Directive[55] against imposing an obligation on an 'information society service' to actively monitor third-party content hosted on its service for defamatory or other unlawful material. This suggests that Recommendation 5 should not be in conflict with the OSA immunity.

On the basis of this analysis, an exemption from the OSA provisions is not strictly necessary, but nevertheless, it may be desirable to provide clarity to litigants. Such an exemption would make it very clear that defamation law does not require reference to the OSA, and potentially avoid complex disputes in litigation which test the issue.

[52] As was the argument presented in relation to the BSA term 'internet content host' by the amicus intervenors in *Fairfax Media Publications & Ors v Voller* [2020] NSWCA 102.

[53] See e.g. *Google France SARL v Louis Vuitton Malletier SA* [ECLI: EU: C:2010: 159]; *L'Oreal SA v ebay International AG* [ECLI:EU:C; 2011:474]; *SABAM v Netlog NV* [ECLI:EU:C:2012:85]. See now proposed Article 5 of the EU DSA.

[54] *Glawischnig-Piesczek v Facebook Ireland* [2019] EUECJ C-18/18 (03 October 2019).

[55] E Commerce Directive, Article 15(1): see now proposed Article 7, EU DSA.

Recommendation 5: New court powers for non-party orders to remove online content

Recommendation 5: Empower courts to make non-party orders to prevent access to defamatory matter online

See draft Part A MDAPs Sch 1 [8], draft section 39A

Amend the MDPs to provide that where a court grants an interim or final order or judgment for the complainant in an action for defamation, the court may order a person who is not a party to remove, block or disable access to the online matter within the scope of such order or judgment.

The power should require notice to be given to the person who is not a party before the order is made.

Introduction

The Stage 2 Discussion Paper[56] asked stakeholders several questions in relation to the powers of courts to order non-parties to remove, block or de-list material that has been found defamatory.

Where a complainant has obtained judgment against an originator, the court has awarded a remedy but in some circumstances, enforcement of the remedy can be elusive. Where an originator is unable to remove the content (for example because it has been copied and shared by others using new hyperlinks or on other platforms and has therefore 'gone viral') or refuses to do so, there may be a role for non-parties (often comprising internet intermediaries which host or otherwise provide access to the content) to play.

Courts in defamation proceedings, as in other civil proceedings, will generally only grant orders against defendants joined to the proceedings. The complainant is generally put in the position of serving the judgment it has obtained against the originator on the internet intermediary and asking it to remove the material on a voluntary basis. If it does not do so, respond promptly or at all, or if it does not remove the material to the claimant's satisfaction, the claimant may be unsatisfied.

The Discussion Paper asked whether non-party orders similar to those available under section 13 of the United Kingdom *Defamation Act 2013* (UKDA) should be available in relation to internet intermediaries hosting such content, and whether such orders should be able to be obtained on a worldwide basis.

[56] Stage 2 Discussion Paper, from p 73.

Section 13 of the UKDA provides as follows:

> 'Where a court gives judgment for the complainant in an action for defamation the court may order-
>
> a) The operator of a website on which the defamatory material is posted to remove the statement, or
>
> b) Any person who is not the author, editor or publisher of the defamatory statement to stop distributing, selling or exhibiting material containing the statement.'

The Stage 2 Discussion Paper also noted that the online environment contains a great deal of unedited and potentially defamatory speech, and asked whether the current high threshold for interim injunctions against publication (or take down orders) under defamation law should be varied in this context, including in the context of non-party orders. It is a well-established principle at common law that 'prior restraint' of a publication (an interim injunction) will rarely be granted in defamation proceedings pending a trial. This is in recognition of the principle that freedom of speech should not be curtailed by an injunction where damages would be an adequate remedy for the complainant if successful at trial.

Stakeholder views on court orders to prevent access to defamatory matter

Non-party orders

In respect of non-party orders, legal stakeholders noted that there are some existing powers by which courts, or at least those of superior jurisdiction, can potentially order a non-party to take down or disable access to material found to be defamatory. One stakeholder noted that no court had to date issued a take down order against a non-party internet intermediary in Australian defamation proceedings.

Internet intermediaries did not support new court powers as part of these reforms. Several indicated that they voluntarily geo-block material (restrict viewing of the material by Australian based users) which has been the subject of an Australian defamation judgment. However, another stakeholder submitted that this may not be a 'universal, or necessarily consistent, practice'.

One intermediary, while opposing the introduction of a non-party power similar to section 13 of the UKDA, suggested that if one is introduced, it should be subject to a high threshold and safeguards to protect freedom of expression.

Threshold for interim orders

Some stakeholders argued that there is merit in introducing a lower, 'prima facie defamatory' test for an interim injunction where the defendant is an internet intermediary, particularly for 'backyard' social media disputes. This included advocating for a lower threshold along the lines of the Law Commission of Ontario's (LCO) suggested test.[57] The LCO recommended that reforms be introduced to provide that, on motion by a complainant, the court in a defamation action may issue an interlocutory take down or de-indexing order against any person having control over a publication requiring its removal or otherwise restricting its accessibility pending judgment in the action, where:

- there is strong prima facie evidence that defamation has occurred, and there are no valid defences, and
- the harm likely to be or have been suffered by the complainant as a result of the publication is sufficiently serious that the public interest in taking down the publication outweighs the public interest in the defendant's right to free expression.

[57] The Ontario Law Commission's test is discussed at [3.225-3.226] of the Discussion Paper. See Recommendation 22(a), Law Commission of Ontario, *Defamation Law in the Internet Age - Final Report 2020*, available at https://www.lco-cdo.org/wp-content/uploads/2020/03/Defamation-Final-Report-Eng-FINAL-1.pdf

However, a majority of stakeholders opposed any lowering of the current threshold. One stakeholder noted that interlocutory injunctions have been obtained in social media cases even under the existing threshold.

Jurisdiction and enforcement issues

Some stakeholders raised concerns that any power to make orders to non-party intermediaries, particularly where such orders are framed as applying worldwide, may face difficulties of jurisdiction and enforcement in relation to foreign based intermediaries. Other stakeholders pointed out that to the extent that a court already has power, it is not the power that is in issue, but its enforcement, particularly in relation to worldwide orders. Stakeholders generally did not support any attempt to 'fix' the inherent jurisdiction and enforcement issues that arise in the context of the global online environment via the MDPs. Some considered that there may need to be international agreement to resolve this issue.

The courts should be empowered to make non-party orders to prevent access to defamatory matter online

In relation to non-party orders, while some courts may have an existing discretionary power to make such orders, it is unclear whether and when courts would be in a position, or would exercise discretion to, make such an order where the internet intermediary that stores or indexes the defamatory material is not joined to the proceedings.

Since the issue of the Stage 2 Discussion Paper, two decisions on section 13 of the UKDA have been published. They provide guidance as to the utility of such a power.

Summerfield Browne Limited v Waymouth[58] concerned an identified originator, resident outside the United Kingdom, who had refused to remove a defamatory online review of the complainant's law firm or respond to defamation proceedings. The High Court granted an order requiring the operators of the website to remove the defamatory review *'on the basis that the Defendant's conduct to date makes it doubtful that he will comply with the injunctive relief the Complainant has been granted.'*[59]

Blackledge v Persons Unknown (being the authors, editors and publishers of the website https://metooucu.blogspot.com)[60] concerned an unknown originator who had circulated allegations about the complainant by email and on a Google blog site. Saini J permitted the commencement of proceedings against a 'person unknown' ('D') via substituted service to the email address from which the defamatory emails had emanated. His Honour made a section 13 order as part of the suite of relief granted to the complainant: [61]

> *'In the circumstances, an order requiring Google to remove the Website is justified and wholly appropriate. It is highly unlikely that D will comply with the injunction I have made due to their failure to engage with proceedings. Where an injunction may not be effective, as in the instant case, an order under section 13 is an appropriate and proportionate remedy. On the facts of this case, where D has hidden their identity, a section 13 order is likely to be the only remedy that is capable of providing effective and meaningful protection to C's civil rights.'*

[58] [2021] EWHC 85 (QB). The hearing date was 18 January 2021; however, the judgment does not appear to have been published until some months later.

[59] Id at [39].

[60] [2021] EWHC 1994 (QB).

[61] Id at [61].

In cases where originators refuse to comply with orders, and in particular, if reforms are adopted which would create a safe harbour for internet intermediaries where the originator is identifiable (Recommendation 3A), then if the intermediary does not voluntarily remove the material, the complainant's judgment may be ineffective in removing the content from the internet. In some cases, the material may be cached and not effectively removed by the originator.

An order could be issued to any non-party with a role to play in limiting access to digital defamatory material, including an 'immune' non-party such as an ISP, where the court considers that this is necessary to ensure that the complainant's remedy is effective. This was suggested by the NSW Bar Association drawing on the model provided by copyright law.[62] The intention is to separate the enforcement of the complainant's remedy from the need to establish liability against those who can play a part in delivering that remedy.

Notice should be given to the non-party, and a chance to join the argument if desired.

The power would largely follow the section 13 UKDA model, with two amendments or clarifications:

- The power would also be available as an adjunct not only to a defamation final judgment against an originator, but to an interim injunction when one is granted against an originator. This would ensure that where there is an urgent need to take material down pending a trial, the court may make a non-party order to ensure this promptly occurs, in a form satisfactory to the claimant.
- The power is designed to address the particular problems affecting remedies for complainants in relation to defamatory material published via internet intermediaries considered in these Stage 2 reforms. It is considered likely that most such orders will be made in relation to internet intermediaries. However, to avoid complexity in relation to whether a non-party falls within the definition of 'digital intermediary' in the Part A MDAPs, it is proposed that the order can be made in relation to any non-party, provided that the order relates to digital defamatory material (**a digital matter**).

There is no change to the existing threshold for the granting of interim orders, and an order cannot be made against a non-party except as an adjunct to orders made against an originator respondent.

Benefits and Risks

Benefits

- Given the similarity of facts in the UK proceedings to many of those that now come before Australian defamation courts,[63] it would be beneficial to provide courts with a clear and uniform option to craft a fit remedy for complainants in such situations.
- The court could tailor the order to ensure the complainant has an effective remedy. For example, in *Summerfield*, the order required the intermediary to remove a defamatory review.
- The availability of such orders would offer a possible alternative to the issue of criminal contempt proceedings against a recalcitrant originator.[64]

Risks

- Courts could make such orders to non-parties which are overbroad or difficult to implement is addressed by requiring notice is given to the non-party that an order is proposed to be made. The non-party could then seek to be heard, or informally negotiate with the complainant on the form of order.

[62] *Copyright Act 1968* (Cth), s 115A.

[63] See for example, *Webster v Brewer (No 3)* [2020] FCA 1343; and the subsequent contempt proceedings in New Zealand: [2020] NZHC 3419; (No 2) [2021] NZHC 298; *Nettle v Cruse* [2021] FCA 935; *Seven Network (Operations) Ltd v Dowling (No 2)* [2021] NSWSC 1106; *Brennock v Norman* [2021] NSWSC 1182; *Fergusson v Dallow (No 5)* [2021] FCA 698.

[64] See cases cited at previous footnote.

- Internet intermediaries may not fully implement an order which purports to apply worldwide. Rather, they may geo-block the content from Australian users of its service. This may satisfy some complainants, but not others, However, this raises more general jurisdictional and enforcement issues concerning Australian courts and their jurisdiction over foreign entities which cannot be addressed through reform to the MDPs.
- Damages cannot be awarded via the non-party order. The use of non-party orders therefore does not compensate a complainant who is unable to sue an internet intermediary for damages because it has established a defence introduced by these reforms.

Recommendation 6: Considerations when making preliminary discovery orders about originators

Recommendation 6: Courts to consider balancing factors when making preliminary discovery orders

See draft Part A MDAPs Sch 1 [5], draft section 23A

Amend the MDPs to provide that, where court rules allow a complainant to seek a preliminary discovery order from an internet intermediary in order to obtain information about an originator for the purposes of commencing defamation proceedings against them, the court should take into account:

- the objects of the MDPs
- any privacy, safety or public interest considerations which may arise should the order be made

Introduction

Many originators who post defamatory material online do so pseudonymously. In order to commence defamation proceedings, the complainant must identify and locate the originator. The Stage 2 Discussion Paper noted that so called 'Kabbabe orders',[65] or preliminary discovery orders, are regularly being obtained against intermediaries hosting review site platforms to require them to reveal any identifying information they hold about an originator. Since the Stage 2 Discussion Paper, many more 'Kabbabe orders' have been obtained in the Federal Court of Australia.[66]

These orders have generally been obtained in relation to information held by the review website or platform on which the allegedly defamatory material is posted. However, such orders have also been obtained from a local ISP which connected the alleged originator to the review website.[67]

In the United Kingdom, orders to 'innocent' third parties to disclose the identity of alleged anonymous 'wrongdoers' are known as 'Norwich Pharmacal' orders. Such orders are an exercise of the court's equitable jurisdiction. The courts require a complainant to prove that:

- a wrong must have been carried out, or arguably carried out, by an ultimate wrongdoer,
- there must be the need for an order to enable action to be brought against the ultimate wrongdoer, and

[65] *Kabbabe v Google LLC* [2020] FCA 126.

[66] See e.g. *Allison v Google LLC* [2021] FCA 186; *Seven Consulting Pty Ltd v Google LLC* [2021] FCA 203; *Sydney Criminal Lawyers v Google LLC* [2021] FCA 297; *Heath v LawTap Pty Ltd* [2021] FCA 485; *Lin v Google LLC* [2021] FCA 1113; *Kandola v Google LLC* [2021] FCA 1261; *Berry Family Law v Google LLC* [2021] FCA 1589; and orders made in unreported Federal Court decisions in *Seeto v Google LLC* (VID394/2020); *Cahill v Google LLC* (VID543/2020); *Jarrett v Google LLC* (VID151/2021); *Hyman v Google LLC* (VID 152/2021); and *Korana v Google LLC* (VID 480/2021).

[67] *Colagrande v Telstra Corporation Limited* [2020] FCA 1595 (application to obtain identity information from a local ISP in relation to an allegedly defamatory review posted on an overseas website).

- the person against whom the order is sought must:
  a) be mixed up in so as to have facilitated the wrongdoing, and
  b) be able or likely to be able to provide the information necessary to enable the ultimate wrongdoer to be sued'.

Norwich Pharmacal orders are becoming more common in the context of online defamation claims, due to the ubiquity of pseudonymous online speech.[68] In most instances the intermediary does not oppose such orders. However, there are exceptions. In one case,[69] Facebook successfully opposed the making of a Norwich Pharmacal order to reveal the identity and location of an originator on the basis that it could expose the originator to arrest by Ugandan authorities. In another, an anonymous originator who had sent pseudonymous emails to customers of the complainant wrote directly to the court seeking to prevent (unsuccessfully) a Norwich Pharmacal order being issued to reveal their identity.[70]

Rule 7.22 of the Federal Court Rules provides that a preliminary discovery order to identify a prospective respondent may be granted where 'there may be a right' for the prospective applicant to obtain relief against a prospective respondent and the applicant 'reasonably believes' that they have this right and another person' 'knows or is likely to know' or 'has, or is likely to have' a document that would help identify the prospective respondent.[71] The prospective applicant must show that they are 'unable, notwithstanding having made reasonable inquiries and taken other steps reasonably required in the circumstances, to ascertain the description of the prospective respondent'.

Rules permitting preliminary discovery orders made to third parties to identify potential respondents exist in all state civil procedure rules.[72] Civil procedure rules also deal with methods of service out of the jurisdiction, as is required where an intermediary is domiciled offshore. The Federal Court of Australia and superior courts in all Australian states and territories[73] may grant leave to serve these orders internationally under the streamlined processes available under the Hague Service Convention.[74]

In *Kabbabe*, the applicant was not required to show an 'arguable' case of defamation against the prospective respondent, who had left a review of the applicant on Google Review using a pseudonym. Rather, he was required only to show that he wished to commence proceedings against this unknown originator, and that Google 'may' have information which could identify them.

The Court permitted service by international registered post in accordance with service rules for the United States under the Hague Convention. The Court ordered that Google produce subscriber information for the prospective respondent, including the name of the user of the account, any phone numbers, internet IP addresses, location metadata, and other Google accounts used from the same internet IP address.

The Stage 2 Discussion Paper asked stakeholders whether specific provisions should be introduced governing when a court may order that an internet intermediary disclose the identity of a user who has posted defamatory material online, whether countervailing considerations such as the privacy and safety of originators should be taken into account, and in relation to procedural issues including whether the orders should be provided for in the MDPs, or left to jurisdictions' procedural rules.

---

68 See e.g. *Gyh v Persons Unknown* [2017] EWHC 3360 (QB); *Muwema v Facebook Ireland Ltd* [2018] IECA 104; *Parcel Connect Limited t/as Fastway Couriers v Twitter International Company* [2020] IEHC 279; *Board of Management of Salesian Secondary College (Limerick) v Facebook Ireland Ltd* [2021] IEHC 287.

69 *Muwema v Facebook Ireland Ltd* [2018] IECA 104.

70 *Portakabin Limited v Google Ireland Limited* [2021] IEHC 446: per Allen J at [20]: 'there is no right to write anonymous letters'.

71 Federal Court Rules, r 7.21, 7.22 subclauses 1(a) and (c). Cf UCPR rule 5.2.

72 See e.g. NSW UCPR 2005, rule 5.2.

73 See Federal Court Rules 2011 (Cth), Div 10.6; NSW, see Uniform Civil Procedure Rules 2005 (NSW), R 11.1 and Part 11A; Supreme Court (General Civil Procedure) Rules 2015 (Vic), O 80; Uniform Civil Procedure Rules 1999 (Qld), Div 3; (matters commenced in the Qld District Court can also be filed for service in the Supreme Court registry: see *Pilling v Shajahan Karim LLB* [2020] QDC 306); Rules of Supreme Court 1971 (WA), O 11A; Supreme Court Civil Rules 2006 (SA), Div 3(3); Supreme Court Rules 2000 (Tas), Part 38A; Court Procedure Rules 2006 (ACT), Div 6.8.12; Supreme Court Rules 1987 (NT), r 7A.

74 *Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters done at The Hague on 15 November 1965* (**Hague Service Convention**). The Hague Convention allows service by international registered post where a member state, such as the US, permits this.

Stakeholder views on preliminary discovery orders to provide information about originators

A substantial number of stakeholders submitted that no change to these preliminary discovery order powers should be made. It appears that such orders have become an important tool for complainants in seeking to commence proceedings against unidentified originators of online defamatory comments. Some stakeholders also suggested that if an originator wants to make public defamatory statements anonymously, they should go to a journalist, for whom safeguards to protect anonymous sources are already in place.

However, some raised concerns about the low threshold for such orders, or more generally, supported the right of users to post pseudonymously online, citing factors such as privacy of users, the risk of harassment or legal silencing of #MeToo and other whistle blowers, and safety concerns such as where the location information of a dissident or domestic violence victim may be disclosed.

Internet intermediaries submitted that they will generally not provide private information provided by or held by them about users of their platform, such as contact details, location information or real names, to third parties without a court order, citing privacy and freedom of expression concerns. Where a court order is received, they will generally comply with it. Some noted that they may consult the user or notify them that the order has been received.

The courts should consider balancing factors when ordering an internet intermediary to disclose information about an originator

Pseudonymous online speech is a feature on some digital platforms and many internet intermediaries' privacy policies preclude voluntary disclosure of identifying information.

However, there is no general right to defame anonymously, or more specifically, to resist preliminary discovery orders to disclose one's identity in defamation proceedings.

Australian courts can, and do, take into account considerations of proportionality, privacy and the risk of abuse of process in exercising the discretion to make preliminary discovery orders to reveal the identity of a prospective respondent.

Courts have acknowledged that the granting of preliminary discovery orders to identify prospective respondents involves a balancing exercise between the complainant and the prospective respondent's rights.[75] In other contexts such as copyright, courts have framed orders to balance the privacy of the prospective respondent and to limit their exposure to legal proceedings for relatively trivial infringements.[76]

This discretionary balancing exercise also arises in the context of journalist's source protection. Under the common law 'newspaper rule' evolved to protect freedom of expression in defamation proceedings, courts will generally not make a preliminary discovery order to identify an originator who is a journalist's confidential source.[77] However, this principle is not absolute, and preliminary discovery orders may be granted where the complainant may otherwise be left without a remedy.[78]

As the use of 'Kabbabe orders' against internet intermediaries continues, it may be expected that the courts will develop similar discretionary principles if required. A recent decision handed down after the issue of the Discussion Paper concerned a complainant's attempt to unmask the originator of YouTube videos criticising the conduct of an international martial arts organisation,[79] The court granted 'Kabbabe orders', stating in the orders that '[t]he applicant acknowledges that the respondent may inform the YouTube Account Holder of this request, in accordance with Google's

[75] *Dallas Buyers Club v iiNet Limited* [2015] FCA 317 per Perram J at [86].

[76] See e.g. *Dallas Buyers Club v iiNet Limited* [2015] FCA 317; *Siemens Industry Software Inc v Telstra Corporation Limited* [2020] FCA 901.

[77] *John Fairfax & Sons Ltd v Cojuanco* (1988) 82 ALR 1.

[78] See *Liu v The Age Company Ltd* [2012] NSWSC 12, where McCallum J granted discovery of a journalist's confidential source under rule 5.2 of the UCPR 2005 (NSW).

[79] *International Wushu Federation v Google LLC* [2021] FCA 904.

usual policies' and that 'Google may apply to the court at any time to vary or discharge this Order'.

There is also a general principle of discovery which prevents collateral use or misuse of information for purposes other than in the proceedings for which discovery was ordered.[80]

Despite the developments described above, there may still be a risk that such orders are abused or have a chilling effect on whistleblowing disclosures. They are potentially open to abuse in whistle blower cases where revealing the identity of the originator may put them at risk.

Requiring that the objects of the MDPs, and any privacy, safety or relevant public interest considerations be taken into account by courts making 'Kabbabe orders' in defamation matters would provide uniform guidance to courts exercising preliminary discovery powers to make orders to an intermediary to disclose identifying information about an originator in defamation cases.

The requirement would be set out in the MDPs so as to provide a clear framework for exercise of the court's general discretion in making preliminary discovery orders to identify a prospective respondent where defamation proceedings are concerned.

Benefits and risks

Benefits

- Ensure that courts considering the making of 'Kabbabe orders' in defamation proceedings do not grant such orders without consideration of countervailing factors specific to the digital defamation context.
- Reduce the risk of complainants 'forum shopping' in Australian courts to unmask an originator for ulterior motives such as the suppression of whistle blower allegations if this amounted to an abuse of process.

Risks

- Specifying factors to be taken into account in the court's discretion to grant preliminary discovery orders to identify a prospective respondent in defamation cases concerning digital matter may be perceived to be unnecessary as courts already consider a range of factors when making such orders, whether or not the matter is a 'digital matter'.
- There may be perceived inconsistency between the MDPs and the test for application of a court's civil procedure rules dealing with preliminary discovery orders.

[80] *Home Office v Harman* [1983] 1 AC 280.

Recommendation 7: Offers to make amends to be updated for online publications

Recommendation 7: Mandatory requirements for an offer to make amends to be updated for online publications

See draft Part A MDAPs Sch 1 [3], draft section 15(1A)(b) and Sch 1 [4], draft section 15(1B)

Amend the mandatory requirements for the content of an offer to make amends in clause 15 to:

- provide an alternative to clause 15(1)(d) by allowing the publisher to offer to remove, block or disable access to the matter in question. This would be instead of the requirement for an offer to publish, or join in publishing, a reasonable correction of, or a clarification or additional information about, the matter in question.
- make clear that if the alternative is used by the publisher, clause 15(1)(e) would not be mandatory either

Introduction

Part 3 of the MDPs establishes a procedure to enable parties to settle disputes without the need for litigation, by requiring the complainant (the 'aggrieved person') to put the publisher on notice of the alleged defamatory matter, and allowing sufficient time for the publisher to make a reasonable 'offer to make amends'. If the complainant does not accept an offer to make amends that is reasonable in all the circumstances, the publisher has a defence in any subsequent defamation action.

Clause 15 of the MDPs sets out a number of requirements for what a reasonable offer to amends *must* and *may* include. Two of the mandatory requirements are:

- an offer to publish, or join in publishing, a reasonable correction of, or a clarification of or additional information about, the matter in question (cl 15(1)(d))
- if material containing the matter has been given to someone else by the publisher or with the publisher's knowledge — an offer to take, or join in taking, reasonable steps to tell the other person that the matter is or may be defamatory of the complainant (cl 15(1)(e))

Clause 15 also includes a list of further remedial actions a publisher *may* offer to the complainant (such as an apology). The Stage 1 amendments to the MDPs added an option for the offer to make amends to include an offer to remove the matter from a website or electronically accessible location. This would be available to a primary publisher of content online (so the poster, author or originator) and any internet intermediary considered a publisher under the common law.

While this was intended to address the nature of online publications, the Stage 2 Discussion Paper recognised that the Part 3 process is not designed with internet intermediaries in mind. In particular, an internet intermediary may not be able to comply with the mandatory requirements for a reasonable offer to make amends. The Stage 2 Discussion Paper asked stakeholders a number of questions about how the concerns notice and offer to make amends process could be better adapted to respond to internet intermediary liability for the publication of third-party content.

Stakeholder views on offers to make amends and online publications

A number of stakeholders pointed out that, in the context of third-party content published online, the remedy most sought after by complainants is to have the matter removed or de-indexed. It was noted that apologies and compensation are not usually the desired outcome.

Stakeholders also noted that internet intermediaries may not be able to comply with the mandatory requirements in the offer to make amends provisions. For example, a search engine would not be able to 'offer to publish, or join in publishing, a reasonable correction of, or a clarification of or additional information about, the matter in question' for a search result.

Several suggestions were put forward for adapting the concerns notice and offer to amend process for internet intermediaries:

- Remove or revise some of the mandatory requirements for the offer to make amends
- The concerns notice/offer to make amends process could be integrated with a new complaints notice process. Or an offer to remove process could be included as part of a new complaints notice process

Other stakeholders submitted there should be no change the concerns notice and offer to make amends provisions but a separate complaints notice process should be developed – that precedes any concerns notice process.

The mandatory requirements for an offer to make amends should be updated for online publications

If adopted, Recommendations 3A (safe harbour, subject to complaints notice) or 3B (innocent dissemination defence for internet intermediaries) would provide a mechanism for the complainant to issue a complaints notice to the defendant. This could result in the internet intermediary providing the complainant with the originator's contact details (if they do not have them already) (Recommendation 3A), removing the content (Recommendations 3A and 3B) or choosing to leave the content online (and therefore losing the benefit of the defence – Recommendations 3A and 3B). It is in the third scenario where it would become necessary for the complainant to issue a concerns notice to the internet intermediary.

In addition to this scenario, there may be other circumstances where an online publisher may wish to make a reasonable offer to make amends to the complainant. This includes:

- Where a social media platform or a forum administrator (for example) has authored or posted content online themselves
- Where an originator has published content online (for example by making a post on a social media platform).

The Part 3 process has an important role to play supporting two objects of the MDPs:

a) To provide effective and fair remedies for persons whose reputations are harmed by the publication of defamatory matter, and

b) To promote speedy and non-litigious methods of resolving disputes.

It is important to ensure that Part 3 that it is relevant to both online and offline publications.

The contents of an offer to make amends set out in clause 15 articulate what is a fair and effective remedy for harm to a person's reputation. We consider that some changes are justified to reflect the nature of online publications. The requirements in clauses 15(1)(d) and (e) of the MDPs make sense for traditional publications such as hard copy newspapers. Traditional publications of this kind were relatively ephemeral in the sense that once published, they did not remain readily accessible at the click of a button. If the publisher received a concerns notice about a defamatory statement in a particular edition, they could then offer to publish a correction in a subsequent edition, presumably

reaching largely the same audience.

In contrast, when defamatory matter is published online it is often there to stay. There is also the ease and speed at which it can be further disseminated to a wide audience. It is understandable then that for many complainants, their central concern is simply to have the matter removed.

Recommendation 7 is to amend the mandatory requirements for the content of an offer to make amends to provide an alternative to clause 15(1)(d) by allowing the publisher to offer to remove or de-list the matter in question. This would be instead of the mandatory requirement for an offer to publish, or join in publishing, a reasonable correction of, or a clarification or additional information about, the matter in question. The amendments would make clear that the alternative is used by the publisher, clause 15 (1)(e) would not be mandatory either.

Recommendation 7 would ensure there is an appropriate avenue for making amends in circumstances where it is not possible or meaningful for online publishers, including internet intermediaries to publish a correction or clarification. It also reflects the kind of remedy that many complainants are seeking in relation to online publications.

It is important to make clear that this would provide an alternative rather than precluding the publisher from fulfilling clauses 15(1)(d) and (e). Ultimately, under clause 18 of the MDPs, in order for the publisher to be able to rely on the defence, the court must be satisfied that in all the circumstances the offer was reasonable (clause 18(1)(c)). This means that if the circumstances were such that it would have been appropriate for the online publisher to offer to publish a correction or clarification and to inform the audience that the matter is or may be defamatory, the court would be able to take this into account when determining if the defence is established.

Benefits and risks

Benefits

- These changes would ensure Part 3 of the MDPs is better adapted to the nature of online publications and what internet intermediaries are and are not capable of doing
- These changes would recognise that in the era of online communications, often the remedy complainants are seeking first and foremost is to have the matter removed

Risks

- Online publishers, including internet intermediaries may simply remove defamatory matter, including in circumstances where it would be appropriate to publish a correction
- Initially at least, there may be some confusion about in what circumstances it is appropriate to use the alternative option or when it would be expected that the publisher fulfil clauses 15(1)(d) and (e)

Savings and transitional provisions for Part A

The draft Part A MDAPs include savings and transitional provisions that are tailored to specific amendments.

Digital intermediary amendments

The 'digital intermediary amendments' are defined to include:

- The statutory exemptions for certain internet intermediary functions (Sch 1 [2] draft section 9A)
- The alternative options for new defences for internet intermediaries (Sch 1 [6] draft section 31A and Sch 1 [7] draft section 31A)

Generally speaking, the new laws would apply to the publication of defamatory matter after the commencement date.

There is one exception to this for multiple publications of the same or substantially the same matter that occur within a year of each other. In these circumstances, if one or more of the publications occurs prior to the commencement date and another occurs after the commencement date, the old laws will apply to both publications.

By way of example, if a post or multiple posts are made on a social media platform after the digital intermediary amendments have commenced – the new laws will apply to the cause of action(s). But if a post is made on a social media platform prior to commencement and then is re-posted after commencement (and within 12 months of the first post), the old laws will apply to both the post and the re-post.

This was the approach taken when the MDPs were originally agreed and introduced. It is in recognition that pre and post-commencement actions regarding the same or substantially the same matter are part of the same dispute. The intention is to minimise confusion and promote consistent application of the law.

Concerns notice amendments

The 'concerns notice amendments' are the updates to the mandatory requirements for concerns notices, to better accommodate online publications.

The new laws would apply to a concerns notice in relation to matter published after the commencement date. The new laws would also apply to a concerns notice about matter published before the commencement date, so long as it is the first notice, or a notice replacing a previous notice, and it is provided after the commencement date.

Discovery or prevention order amendments

The 'discovery or prevention order amendments' include:

- The new court powers to order non-parties to prevent access to defamatory matter in certain circumstances

- The requirement for courts to take into account certain matters (such as privacy and safety) when ordering the disclosure of information about an originator

The new laws would apply to the making of such an order after commencement date regardless of when the publication was made and the proceedings were commenced. However, the old laws would apply to an order made before the commencement date and the amendment or revocation of an order made before the commencement date.

Appendix A: Categorising internet intermediaries

Introduction

The Stage 2 Discussion Paper used the umbrella term **internet intermediaries** based on the Organisation for Economic Cooperation and Development (**OECD**) description of entities that that 'bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties'.[81] Internet intermediaries range from internet access and service providers, to content hosts, social media platforms and forum administrators.

In order to have a conceptual framework, the Stage 2 Discussion Paper grouped the functions of internet intermediaries into three categories:

1) **Basic internet services**: internet intermediaries that act as mere conduits, passively facilitating internet use.
2) **Digital platforms**: as described by the Australian Competition and Consumer Commission (**ACCC**) in its Digital Platforms Inquiry Final Report[82], digital platforms are applications that serve multiple groups of users at once, providing value to each group based on the presence of other users.
3) **Forum administrators**: individuals and organisations that host online discussion forums – including as administrators and moderators – and have some level of control over the content posted in these forums (either by moderating or blocking content).

Stakeholder views

A number of stakeholders expressed support for the proposed approach to categorising internet intermediaries, but noted the need for flexibility. The majority of stakeholders noted the great variety of internet intermediary functions and the fact that they continue to develop and evolve over time. One stakeholder indicated a preference for the terms 'Digital Infrastructure' (e.g. ISPs), 'Digital Caching' (e.g. search engines) and 'Hosting' (e.g. platforms hosting user generated content).

Some stakeholders, particularly from the technology sector, submitted that the categories fail to recognise the complexity and diversity of internet intermediaries. Several stakeholders suggested that further delineation between the categories is required. It was also suggested that, rather than focusing on existing services, a better approach would be to consider the role of internet intermediaries and the extent of their editorial control.

[81] OECD, 2010, 'The Economic and Social Role of Internet Intermediaries', see: http://www.oecd.org/digital/ieconomy/44949023.pdf

[82] Australian Competition and Consumer Commission, Digital Platforms Inquiry: Final Report 2019, see: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

One technology sector stakeholder submitted that because the functions of internet intermediaries are so varied and there is a risk of any categorisation becoming outdated, the only distinction that should be drawn is that between primary and secondary publishers. Several stakeholders proposed that, in order to avoid trying to classify different internet intermediary functions, the focus should simply be on what they are not – which is the originator of the publication in question.

Basic internet services

A number of stakeholders expressed support for the proposal in the Stage 2 Discussion Paper that the defining feature of basic internet services is passivity. There appears to be no dispute that ISPs should be considered basic internet services. Several legal stakeholders submitted that is where the line should be drawn. Some stakeholders, particularly from the technology sector, submitted that other functions such as cloud service providers and email service providers, should also fall into this category. A smaller number went further – submitting that the use of algorithms does not prevent an internet intermediary from being content neutral and that search engines should be considered basic internet services.

Digital platforms

In their submissions, some stakeholders supported using the ACCC's classification of digital platforms. However, several technology sector stakeholders submitted that the classifications are problematic as they do not take into account the variety of digital platforms, the different ways they operate and are used and the degree of control they have over different types of content. In particular, it was submitted that the ACCC classifications ascribe too much functional control to services that only use algorithms.

Forum administrators

Several stakeholders submitted that it is not appropriate or necessary to treat forum administrators as a separate category. One stakeholder argued they should be treated in the same way as other digital platforms – and as secondary publishers. A legal stakeholder submitted that, as a general proposition, forum administrators have more control over third-party content than other originators.

Several stakeholders argued strongly that forum administrators should be treated differently to other digital platforms. One stakeholder submitted that where forum administrators do not own or control a website or platform, they should not be liable for third-party comments published on it – even where they may have invited such comments.

Stakeholders also submitted that a one-size-fits-all approach is problematic because forum administrators are diverse:

- They include individuals (many of whom are volunteers) and a range of organisations – both profit and not-for-profit
- This means there are significant differences in the resources available to them (for example, to check or moderate third-party content)

The circumstances in which forum administrators operate are also varied:

- The level of knowledge they have in relation to the content and the extent of their engagement with the content will differ
- Their ability to control third-party content will depend on the rules or tools available on the relevant website or platform

One stakeholder submitted that some forum administrators are not aware of what control they do have over third-party content – and the potential legal implications of their role. In contrast to this, it was also suggested that this is very different to circumstances where forum administrator posts content about a matter of public interest that may elicit controversial opinions. It is suggested this type of forum administrator plays a greater role in the publication than someone moderating a community group.

Principles for categorising internet intermediaries

Stakeholder submissions confirmed that the exercise of attempting to categorise internet intermediary functions is highly complex and at risk of quickly becoming out-of-date. Nevertheless, in responding to the section in the Stage 2 Discussion Paper about categorising internet intermediaries, stakeholders provided a number of important insights. This is the basis of the following key principles that have informed the development of the policy recommendations and the drafting of the Part A MDAPs:

- It is better to avoid using specific, technical definitions and where necessary – focus on describing the function rather than the service type.
- The underlying principles should be clearly conveyed – this will provide guidance for the courts in applying the reforms, particularly where technology has evolved.
- At the same time, it is important to provide clear rules where possible – for example by defining the boundaries of any proposed immunities or defences.

Appendix B: NSW Bar Association proposal

32A Defence of innocent dissemination in relation to Internet publication

1) This section relates to the publication of defamatory matter on the Internet.

2) It is a defence to the publication of defamatory matter if the defendant proves that the defendant was involved in the publication of the matter only in the capacity of an Internet intermediary.[83]

3) A defence under this section is defeated if, and only if, the plaintiff establishes that:

   a) it was not possible for the plaintiff to identify the originator of the defamatory matter, and

   b) the plaintiff gave the defendant a complaints notice[84] in respect of the matter concerned, and

   c) the defendant was capable of taking down the defamatory matter, and

   d) within 28 days after a complaints notice was given the defendant failed to either:

      i. provide the plaintiff with information to identify the originator of the defamatory matter; or

      ii. take down the defamatory matter.

4) For the purpose of subsections (3)(a) and (d)(i), it is not possible for a plaintiff to identify an originator unless the plaintiff had, or was given by the defendant, sufficient information to bring proceedings against the person.

[83] The Committee assumes that Internet intermediary will be defined in the MDPs
[84] The Committee assumes that complaints notice will be defined in the MDPs

Appendix C: *Broadcasting Services Act/Online Safety Act* provisions

Definition of 'internet service provider'

Clause 8, Schedule 5 of the *Broadcasting Services Act 1992* (Cth) (the **BSA**) provided that 'if a person supplies, or proposes to supply, an internet carriage service to the public, the person is an internet service provider'.

This has been transferred into section 19(1) of the *Online Safety Act 2021* (Cth) which provides that for the purposes of the Act, 'if a person supplies, or proposes to supply, an internet carriage service to the public, the person is an ***internet service provider***'. The *Online Safety Act 2021* commenced in January 2022.

Definition of 'internet content host'

The BSA defined 'internet content host' as 'a person who hosts internet content in Australia, or who proposes to host internet content in Australia'.

This has been replaced by provisions in the *Online Safety Act 2021* which provide that:

> '***Australian hosting service provider*** means a person who provides a hosting service that involves hosting material in Australia' (section 5)
>
> '***Hosting service provider*** means a person who provides a hosting service' (section 5)

Hosting service is defined in section 17 of the *Online Safety Act 2021* (see below). The Explanatory Memorandum for the Online Safety Bill 2021 identifies an example of this – where a person hosts stored material or content for a website, or an email service. The Explanatory Memorandum also notes that a search engine which merely indexes content and makes it searchable would not meet this definition of hosting service.

17 Hosting service

For the purposes of this Act, if:

a) a person (the first person) hosts stored material that has been provided on:

i. a social media service; or

ii. a relevant electronic service; or

iii. a designated internet service; and

b) the first person or another person provides:

i. a social media service; or

ii. a relevant electronic service; or

iii. a designated internet service;

on which the hosted material is provided;

the hosting of the stored material by the first person is taken to be the provision by the first person of a *hosting service*.

235 Liability of Australian hosting service providers and internet service providers under State and Territory laws etc.

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.

2) The Minister may, by legislative instrument, exempt a specified law of a State or Territory, or a specified rule of common law or equity, from the operation of subsection (1).

Note: For specification by class, see subsection 13(3) of the *Legislation Act 2003*.

3) An exemption under subsection (2) may be unconditional or subject to such conditions (if any) as are specified in the exemption.

Declaration by Minister

4) The Minister may, by legislative instrument, declare that a specified law of a State or Territory, or a specified rule of common law or equity, has no effect to the extent to which the law or rule has a specified effect in relation to an Australian hosting service provider.

Note: For specification by class, see subsection 13(3) of the *Legislation Act 2003*.

5) The Minister may, by legislative instrument, declare that a specified law of a State or Territory, or a specified rule of common law or equity, has no effect to the extent to which the law or rule has a specified effect in relation to an internet service provider.

Note: For specification by class, see subsection 13(3) of the *Legislation Act 2003*.

6) A declaration under subsection (4) or (5) has effect only to the extent that:

a) it is authorised by paragraph 51(v) of the Constitution (either alone or when read together with paragraph 51(xxxix) of the Constitution); or

b) both:

i. it is authorised by section 122 of the Constitution; and

ii. it would have been authorised by paragraph 51(v) of the Constitution (either alone or when read together with paragraph 51(xxxix) of the Constitution) if section 51 of the Constitution extended to the Territories.

Communities and Justice

Locked Bag 5000
Parramatta NSW 2124

Email: defamationreview@justice.nsw.gov.au

NSW GOVERNMENT