Discussion Paper

Attorneys-General

Review of Model Defamation Provisions – Stage 2

Contents

Glossary

ACCC	Australian Competition and Consumer Commission
Basic internet services	Internet intermediaries that function as mere conduits. These intermediaries are analogous to telephone lines and postal services in that they merely facilitate access to services on the internet, rather than actively participating and profiting from the generation and dissemination of user content.
BSA	*Broadcasting Services Act 1992* (Cth).
CAG	The former Council of Attorneys General (**CAG**) assisted the Council of Australian Governments (**COAG**) by leading national law reform. The CAG consisted of Attorneys General from the Australian Government and all states and territories.
Complainant	An individual or organisation that alleges that they have been defamed by matter published online.
DWP	All states and territories are signatory to the MDP Intergovernmental Agreement which establishes the Model Defamation Law Working Party (**DWP**), which reports to Attorneys General on proposals to amend the MDPs.
Digital platform	An internet intermediary that provides a platform for user generated content to be posted and shared including by allowing third-party comments as well as aggregating and curating user generated content from other sources. This can include search engines where search results are curated.
Forum administrator	An entity including an individual, company or community group hosting a social media page, administrator of an online forum or creator of a message thread. Forum administrators are granted control of a portion of a digital platform subject to the ultimate control of the digital platform.

ISP	An internet service provider (**ISP**) connects its subscribers to the internet by supplying telecommunications facilities and access equipment, such as modems and subscriber lines (as described by Jaani Riordan[1]). The BSA considers a person [who] supplies, or proposes to supply, an internet carriage service to the public to be an ISP.[2]
Originator	An individual or organisation that authors or creates content online (for example by writing a blog, making a comment on a discussion forum or posting content on a web page or digital platform).
Internet intermediary	Entities that bring together or facilitate transactions between third parties on the Internet (as defined by the Organisation for Economic Cooperation and Development (**OECD**)[3]). This is the umbrella term used in this Discussion Paper to cover the broad range of online services and platforms to which Part A relates.
LCO Final Report	The final report released by the Law Commission of Ontario (**LCO**) in March 2020 following its Defamation Law in the Internet Age review.
MDPs	The Model Defamation Provisions are uniform laws agreed in 2005 and enacted by each state and territory. In July 2020 Attorneys General agreed to Model Defamation Amendment Provisions (**MDAPs**). References to the MDPs are as if amended by the MDAPs unless otherwise noted.

1 Riordan, J. 2016, *Liability of Internet Intermediaries*, Oxford University Press.

2 Clause 8, Schedule 5 to the *Broadcasting Services Act 1992* (Cth).

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

1. Background

1.1 In November 2004, the former Standing Committee of Attorneys-General agreed there was a need for uniform state and territory legislation to reform the law of defamation in Australia. Attorneys-General agreed to support the enactment in their respective jurisdictions of Model Defamation Provisions (**MDPs**). The MDPs are available on the Australasian Parliamentary Counsel's Committee website at www.pcc.gov.au.

1.2 All states and territories are signatory to the MDP Intergovernmental Agreement (**IGA**). The IGA establishes the Model Defamation Law Working Party (**DWP**), which reports to Attorneys-General on proposals to amend the MDPs.

1.3 In February 2018, the former NSW Department of Justice completed a statutory review of that state's *Defamation Act 2005*. The review identified a number of areas in the Act – and by implication, the MDPs – which would benefit from amendment or modernisation.

1.4 In June 2018, the NSW Attorney General asked the former Council of Attorneys-General (**CAG**) to reconvene the DWP to consider whether the policy objectives of the MDPs remain valid and to make recommendations for reform. The CAG agreed.

1.5 Stage 1 of the review of the MDPs was undertaken over 18 months from early-2019 to mid-2020. This review involved two rounds of public consultation and saw submissions received from media companies, legal stakeholders, digital platforms, legal representatives for plaintiffs and defendants, academics and individuals with experience in bringing or defending defamation claims.

1.6 Based on stakeholder feedback, the DWP instructed the Australasian Parliamentary Counsel's Committee to prepare draft amendments to the MDPs (the Model Defamation Amendment Provisions (**MDAPs**)). In July 2020, the CAG approved the MDAPS and agreed that all jurisdictions will enact and commence them as soon as possible. These amendments resolved well-known and longstanding issues affecting the MDPs. This marked the conclusion of the first stage review of the MDPs.

1.7 The Discussion Paper released as part of the Stage 1 review raised a number of broad questions about the application of the MDPs to digital platforms. The issues raised by stakeholders in response to those questions were both technical and complex.

1.8 On 26 July 2019, the Australian Competition and Consumer Commission (**ACCC**) published its Digital Platforms Inquiry Final Report, making important findings about the functions of digital platforms and recommendations for reform in the areas of competition law, media regulation and privacy law. The Australian Government released its response to the ACCC report in December 2019.

1.9 In light of these developments, as well as the complexity of stakeholder responses, the CAG agreed to undertake a second stage MDP reform process, focusing on the responsibilities and liability of digital platforms for defamatory content published online, as well as any other issues relating to defamation law that Attorneys-General asked the DWP to consider.

1.10 This Discussion Paper is the first step in the second stage of the review of the MDPs. It comprises two parts:

- **Part A** addresses the question of internet intermediary liability in defamation for the publication of third-party content. It suggests options for reform that reflect the potential spectrum of liability for internet intermediaries.
- **Part B** considers whether defamation law is having a chilling effect on reports of alleged criminal conduct to police and statutory investigative bodies and on reports of unlawful conduct to disciplinary bodies and employers. It includes a series of questions for stakeholders about the potential benefits and risks of extending absolute privilege to these circumstances.

1.11 The purpose of this Discussion Paper is to canvas the issues relating to these two topics. Stakeholder responses to the questions asked throughout the Paper are intended to guide the DWP as it seeks to develop a better understanding of both the problems at hand and identify policy solutions for addressing them if required.

1.12 Although the Stage 1 defamation reforms have not commenced at the time of writing, this paper is drafted on the basis of the agreed amendments.

Stage 1 – MDP reforms agreed in July 2020, including:	**Stage 2 – This Discussion Paper asks:**
• Clarification of the cap on damages for non-economic loss • Introduction of a new public interest defence • Introduction of a serious harm threshold • Introduction of a single publication rule • Introduction of a mandatory concerns notice procedure	• **Part A:** What is the liability of internet intermediaries for defamatory material published online by third-party users? • **Part B:** Should absolute privilege be extended to reports of illegal and unlawful conduct made to police and statutory investigative bodies, and employers and disciplinary bodies?

Discussion Questions

PART A

Question 1: Categorising internet intermediaries

(a) Is the grouping of internet intermediary functions into the three categories of 'basic internet services', 'digital platforms' and 'forum hosts' a useful and meaningful way to categorise internet intermediary functions for the purpose of determining which functions should attract liability? Why?

Question 2: Categorising basic internet services

(a) What internet intermediary functions should be categorised as basic internet services? It is proposed that to be categorised as a basic internet service the internet intermediary must be a mere conduit (similar to telephone or postal services) in that they do not have an interest or involvement in the nature of the content they transmit or host.

(b) What are the key concepts that should determine if an internet intermediary function is a basic internet service? Is passivity and neutrality an appropriate basis on which to determine which internet intermediary functions attract liability?

(c) Are there any functions that could be categorised as 'basic internet services' but should give rise to liability, or are there circumstances in which basic internet services should be liable?

Question 3: Categorising digital platforms

(a) Is it appropriate to adopt the classification of digital platforms used in the ACCC's Digital Platforms Inquiry Final Report to understand their roles and functions for the purpose of considering liability in defamation for third-party content?

(b) Do the common features listed above accurately reflect the functions of digital platforms?

(c) Should search engines be treated as a single function for the purpose of categorising intermediaries for defamation liability? Or do search engines have different functions, some of which should or should not give rise to liability?

(d) Is it appropriate to consider search engines a subset of digital platforms, or should they be considered as a separate category that can have access to separate specific defences?

(e) Are there new and emerging digital platform functions that need to be considered?

(f) Are there any publishing functions of digital platforms that should not attract liability? Why?

(g) Is it appropriate to consider digital platforms as having comparable functions to online media companies, or should they be considered as separate categories with different responsibilities and defences? Why?

Question 4: Categorising forum administrators

(a) Is it appropriate to consider 'forum administrators' as a separate category of internet intermediaries? If so, how should this be defined?

(b) What are the different circumstances and scenarios involving forum administrators that need to be considered?

Question 5: Treatment of internet intermediaries as publishers of third-party content

(a) Should internet intermediaries be treated the same as any other publisher for third-party content under defamation law?

(b) If yes, is this possible under the current MDPs, or are amendments necessary, in order to ensure they are treated the same as traditional publishers for third-party content?

Question 6: Immunity for basic internet services

(a) Is it necessary and appropriate to provide immunity from liability in defamation to basic internet services?

(b) If such an immunity were to be introduced, should it be principles-based or should it specifically refer to the functions of basic internet services?

(c) Are there any internet intermediary functions that are likely to fall within the definition of basic internet services (as outlines in Issue 1) that should not have immunity?

(d) Is there a risk that providing a broad immunity to basic internet services would unfairly deny complainants a remedy for damage to their reputation? What risks exist and how could they be mitigated?

Question 7: Amend Part 3 of the MDPs to better accommodate complaints to internet intermediaries.

(a) How can the concerns notice and offer to make amends process be better adapted to respond to internet intermediary liability for the publication of third-party content?

(b) What are the barriers in the concerns notice and offer to make amends process contained in Part 3 of the MDPs (as amended) that prevent complainants from finding resolutions with internet intermediaries when they have been defamed by a third-party using their service?

(c) In the event the offer to make amends process is to be amended, what are the appropriate remedies internet intermediaries can offer to complainants when they have been defamed by third parties online?

Question 8: Clarifying the innocent dissemination defence

(a) Should the innocent dissemination defence in clause 32 of the MDPs be amended to provide that digital platforms and forum administrators are, by default, secondary distributors, for example by using a rebuttable presumption that they are?

(b) In what circumstances would it be appropriate to rebut this default position?

(c) Should a new standalone innocent dissemination defence specifically tailored to internet intermediaries be adopted the MDPs?

(d) If a standalone defence is created, should the question of what is knowledge or constructive knowledge of third-party defamatory content published by an internet intermediary be clarified? If so, how?

(e) Are there other ways in which the defence of innocent dissemination could be clarified?

Question 9: Safe harbour subject to a complaints notice process

(a) Should a defence similar to section 5 of the *Defamation Act 2013* (UK) be included in the MDPs?

(b) If so, should it be available at a preliminary stage in proceedings, where an internet intermediary can establish they have complied with the process?

(c) Should a complaints notice process be available when an originator can be identified? For example, to provide for content to be removed where the originator is recalcitrant?

(d) If such a defence were introduced, would there still be a need to strengthen the innocent dissemination defence?

(e) Should the defence be available to all internet intermediaries that have liability for publication in defamation? For example, could a separate complaints notice process be developed that could apply to search engines?

(f) How can the objects of freedom of expression and the protection of reputations be balanced if such a defence is to be introduced?

Question 10: Immunity for internet intermediaries unless they materially contribute to the unlawfulness of the publication

(a) Should a blanket immunity be provided to all digital platforms for third-party content – even if they are notified about it, unless they materially contribute to the publication?

(b) What threshold or definition could be used to indicate when an intermediary materially contributes to the publication of third-party content?

(c) If a blanket immunity is given as described above, are there any additional or novel ways to attract responsibility from internet intermediaries?

Question 11: Complaints notice process for Australia

(a) Should a complaints notice be distinct from the mandatory concerns notice under Part 3 of the MDPs, or should the same notice be able to be used for both purposes?

(b) Are there any issues regarding compatibility between the mandatory concerns notice and a potential complaints notice process? Are there parts of either that might overlap or be superfluous if a mandatory concerns notice is already required?

(c) What mechanisms could be used to streamline the interaction between the two notice processes?

Question 12: Steps required before engaging in the complaints notice process

(a) Should the complainant be required to take steps to identify and contact the originator before issuing a complaints notice? If so, what should the steps be and how should this be enforced?

(b) Where the complainant can identify the originator, should there be any circumstances where the complainant is not required to contact the originator directly and could instead use the complaints notice procedure?

Question 13: Complaints notice form and content

(a) What content should be required to be included in a complaints notice in order for it to be valid? Should this include an indication of the serious harm to reputation caused or likely to be caused by the publication, or should it be sufficient for the content to be prima facie defamatory?

(b) Should there be a requirement for the intermediary to notify the complainant, within a certain time period, that the complaints notice does not meet the requirements?

(c) Should a complaints notice require the complainant to make a 'good faith' declaration? Should there be any other mechanisms used to prevent false claims?

Question 14: Application and outcome of complaints notice

(a) Should the complaints notice process be available to all digital platforms who may have liability in defamation or only those that can connect the complainant with the originator?

(b) What should happen to the content complained of following receipt of a complaints notice by the digital platform?

(c) Should the focus of the complaints notice process be to connect the complainant with the originator? What other outcomes should achievable through this process?

(d) What steps from the UK process should be adopted in Australia?

(e) Are there circumstances where the digital platform should be able to remove the content complained of without the poster's agreement?

Question 15: Orders to have online content removed

(a) What should be the threshold for obtaining an order before a trial to require the defendant to take down allegedly defamatory material?

(b) Is there a need for specific powers regarding take down orders against internet intermediaries that are not parties to defamation proceedings, or are current powers sufficient?

(c) What circumstances would justify an interim or preliminary take down order to be made prior to trial in relation to content hosted by an internet intermediary? Should courts of all levels be given such powers? For example, in some jurisdictions lower courts have limited powers to make orders depending on the value of the claim.

(d) Should a court be given power to make an order which requires blocking of content worldwide in appropriate circumstances?

(e) If such powers are necessary, it is appropriate for them to be provided for in the MDPs or should it be left to individual jurisdictions' procedural rules?

(f) Are there any potential difficulties with jurisdiction or enforceability of such powers which could be addressed through reform to the MDPs?

Question 16: Orders to identify originators

(a) Is it necessary to introduce specific provisions governing when a court may order that an internet intermediary disclose the identity of a user who has posted defamatory material online?

(b) What countervailing considerations, such as privacy, journalists' source protection, freedom of expression, confidentiality, whistle-blower protections, or other public interest considerations might apply?

(c) What types of internet intermediaries should such provisions apply to?

(d) Is it necessary to provide for reforms to ensure that records are preserved by intermediaries where a complainant may wish to uncover the identity of an unknown originator?

(e) Do any enforcement issues arise in relation to foreign-based internet intermediaries who may not accept jurisdiction? How could this be overcome?

(f) Is it appropriate to provide for these types of orders in the MDPs, or should this be left to each jurisdiction's procedural rules?

Question 17: Other issues regarding liability of internet intermediaries

(a) Are there any other issues regarding liability of internet intermediaries for the publication of third-party content that need to be considered?

PART B

Question 18: Defamation and reports of criminal conduct

(a) Are there any indications that defamation law is deterring victims and witnesses of crimes from making reports to police and other statutory investigative agencies charged with investigating criminal allegations?

(b) Are victims and witnesses of crimes being sued for defamation for reports of alleged criminal conduct to authorities?

Question 19: Absolute privilege for reports to police and investigative agencies

(a) Should the defence of absolute privilege be extended to statements made to police related to alleged criminal conduct?

(b) Should the defence of absolute privilege be extended to statements made to statutory investigative agencies related to alleged criminal conduct? If yes, what types of agencies?

(c) What type of statutory investigative agencies should be covered and what additional safeguards, if any, may be needed to prevent deliberately false or misleading reports and to protect confidentiality?

(d) What is the best way of amending the MDPs to achieve this aim (for example, by amending clause 27 and/or by each jurisdiction amending its Schedule 1)?

Question 20: Defamation and reports of unlawful conduct in the workplace

(a) Is fear of being sued for defamation is a significant factor deterring individuals from reporting unlawful conduct such as sexual harassment or discrimination to employers or professional disciplinary bodies?

(b) Are victims and witnesses of sexual harassment or discrimination being sued for defamation for reports of alleged unlawful conduct to employers or professional disciplinary bodies?

Question 21: Absolute privilege for reports to employers and professional disciplinary bodies

(a) Should absolute privilege be extended to complaints of unlawful conduct such as sexual harassment or discrimination made to:

   i. employers, or to investigators engaged by employers to investigate the allegation?

   ii. professional disciplinary bodies?

(b) If so, to what types of unlawful conduct should be included providing this protection?

(c) If yes to a), what is the best way of amending the MDPs to achieve this aim (for example, by amending clause 27 and/or by each jurisdiction amending their Schedule 1)?

(d) Are there sufficient safeguards available to prevent deliberately false or misleading reports being made to employers or professional disciplinary bodies? If not, what additional safeguards are needed?

Consultation process

The DWP invites interested individuals and organisations to provide written submissions in response to any of the issues raised in this Discussion Paper.

Some of the questions are legal and technical in nature. It is not expected that all stakeholders will be in a position to respond to all discussion questions.

Submissions should be sent:

- By email to defamationreview@justice.nsw.gov.au, or
- By mail to Policy Reform & Legislation, Department of Communities and Justice, GPO Box 6, Sydney NSW 2001

by **19 May 2021**.

Submissions may be published on the NSW Department of Communities and Justice's website, unless you specifically ask us not to do so.

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.

To view an accessible text-version of the Discussion Paper images visit: http://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/review-of-model-defamation-provisions-stage-2-discussion-paper.aspx

If you need to speak to someone about issues raised in this Discussion Paper, please reach out:

1800 RESPECT- National Sexual Assault, Family & Domestic Violence Counselling Line: 1800 737 732 or 1800respect.org.au

Lifeline: 13 11 14 or lifeline.org.au

PART A – Liability of internet intermediaries

2. Introduction

2.1 Since the MDPs were enacted in state and territory legislation in 2005 and 2006, developments in the nature and scale of online communications have raised fundamental issues for defamation law.

2.2 Defamation law evolved in a pre-digital world, where publishing was predominately a professional activity subject to editorial standards and pre-moderation. However, in this era of digital communications, the role of the professional moderator has diminished. Now anyone with an internet connection has the ability to publish information or commentary to the world at large – unchecked.

2.3 The process of digital publication can involve a variety of different actors. This ranges from the individual or organisation that authors or creates the content, the host of the web page on which the content is published, the social media services where it is shared and the search engine that provides links and 'snippets' (extracts of materials) in search results. Any of these actors can be captured by the broad definition of publisher in defamation law. There is an endless array of different scenarios involving internet intermediaries and significant confusion as to what should be their respective responsibilities and liability.

2.4 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).

2.5 The purpose of Part A of this Discussion Paper 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.

2.6 There are a number of potential policy grounds for a range of internet intermediaries having some responsibility in defamation law for the publication of third-party content where they have created systems or online environments to enable and promote the publication and dissemination of user-generated content.

- These intermediaries have the ability – both at the point of design and in day-to-day operations – to either heighten or minimise the risk of harm.
- Often the intermediary has a business model that profits from the network effects. A common feature of many intermediaries' business models is to attract as many users as possible and to keep users on their platforms for as long as possible. This ability to increase the value to users through the presence of other users is the 'network effect'.[4] This business model is frequently designed to generate a profit from advertising.

[4] Australian Competition and Consumer Commission (**ACCC**), *Digital Platforms Inquiry: Final report 2019*, see: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report, p 63.

- Intermediaries are in a position to help the complainant seek redress, for example, by connecting them with the originator, taking content down or de-ranking content.

2.7 The DWP also considers that the responsibilities and liability of internet intermediaries should be related to their different roles and functions. Careful consideration needs to be given to the nature of what different internet intermediaries do and are capable of doing. In the offline world, defamation law has addressed this issue through the concept of a secondary publisher. Traditionally, the primary publisher – for example, a newspaper, was the most obvious and attractive defendant. Secondary publishers, such as newsagents, booksellers and librarians, have been shielded by this fact – as well as the protection offered by the innocent dissemination defence.

2.8 However, when it comes to online communications, which are made available or accessible via internet intermediaries, often (but not always) the internet intermediary is in the best position to address the harm (for example, by removing content). Internet intermediaries are also often an easily identifiable party. It is understandable then that they would be a potential defendant in defamation proceedings, as has increasingly occurred in recent cases. However, this does not necessarily mean that they should automatically be held responsible for content that is authored or created by a third-party. Part A addresses these issues and is structured as follows:

- 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

2.9 It is also important to highlight that defamation law is private law.[5] Potential liability, and private suit by an aggrieved party, is the only policy lever available for seeking to strike a balance between protecting reputations and not unduly limiting freedom of expression.

2.10 The focus of the Stage 2 review is on the MDPs that do not fully codify the common law. In particular, the question of who is and is not a publisher is determined by the common law. It is not proposed that a definition of publisher should be incorporated into the MDPs to address the question of internet intermediary liability for third-party content.

5 While criminal defamation (or criminal libel) exists on the statute books of all States and Territories, the MDPs only deal with the tort of defamation as a civil law matter.

2.11 This is for a number of reasons. The common law test applies to online and offline publishers. It also has a significant body of jurisprudence behind it. Defining who is a publisher in the MDPs could have unintended consequences. Arguably, the common law is better able to respond to new technological developments as they happen, including developments related to the internet itself.[6] Retaining a common law definition allows for some flexibility to consider respective roles and responsibilities in the contemporary, online context of publications. There is a risk that if a statutory definition of 'publisher' were introduced to address today's internet intermediaries, it would quickly become outdated by rapid technological innovations. Accordingly, it is considered preferable to leave the broad principles of publication to evolve at common law as they have done to date.[7]

2.12 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. This is where the DWP considers there may be opportunities for reform, to clarify and potentially limit the exposure of internet intermediaries from liability in defamation for third-party content – if appropriate. The effect of providing new defences and immunities can be to exclude some internet intermediaries from liability as publishers, while retaining sufficient flexibility for the courts to look at the nature of each publication in determining if a defence or immunity is available. This Discussion Paper also asks whether a blanket immunity for all internet intermediaries is appropriate, and whether additional powers should be given to the courts to order removal of content or to identify originators.

What stakeholders have told the DWP so far

2.13 In February 2019, the CAG released a Discussion Paper as part of the Stage 1 review of the MDPs.[8] Question 15 of that Discussion Paper asked a number of questions about the adequacy of existing protections for digital publishers, including the innocent dissemination defence, whether a 'safe harbour' provision would be beneficial, and if clear 'take down' procedures for digital publishers are necessary.

2.14 When responding to these questions, stakeholders representing internet intermediaries' interests argued that there is insufficient protection from liability for content that they have not authored. Other stakeholders, including academics and peak legal bodies, noted that the MDPs should be updated to reflect the nature of digital publications while balancing this with the need to ensure that complainants have access to a remedy.

---

6 See e.g. Gleeson CJ, McHugh, Gummow and Hayne JJ, *Dow Jones and Company Inc v Gutnick* [2002] HCA 56; 210 CLR 575 at [38].

7 Rolph, David, *'Publication, Innocent Dissemination and the Internet after Dow Jones v Gutnick'* [2010] 33(2) UNSWLawJl 24, p 580.

8 Defamation Working Party MDP Review Discussion Paper 2019, see: https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/Final-CAG-Defamation-Discussion-Paper-Feb-2019.pdf.

2.15 Some stakeholders called for the innocent dissemination defence to be better adapted to digital publications and considered in tandem with the immunity in clause 91 of Schedule 5 to the *Broadcasting Services Act 1992* (Cth) (**BSA**). Stakeholders told the DWP it is unclear when an internet intermediary will be considered a 'subordinate distributor' as they may have the technical capability to edit or remove content. Stakeholders also raised the question of whether the BSA provision incentivises internet content hosts to leave their services unmonitored so as to avail themselves of the BSA immunity.

2.16 Internet intermediaries told the DWP that they are not, and cannot, be aware of all content posted by third parties that appears on their webpages or in search results. Some submissions argued that internet intermediaries should not be required to remove content without a court order, because they are not in a position to assess whether content is defamatory. The concern is that they may be inclined simply to remove content to avoid potential liability, which would have a chilling effect on freedom of expression.

2.17 The countervailing view is that, given the risk for substantial reputational damage, there should be quick, easily accessible and low cost avenues for complainants to have content modified or removed, including where the originator's identity is unknown, or if the originator refuses to comply with a request or court order. The need to engage in court processes may preclude a complainant from seeking a remedy, particularly where there is an imbalance of bargaining power between the complainant and a financially powerful intermediary. It is not a reasonable first step in the process. There is also mismatch between the speed at which online publications can spread and the time it takes to seek relief through a court process.

Context - approaches in foreign jurisdictions

United Kingdom

2.18 The United Kingdom (**UK**) is the birthplace of the tort of defamation, developed over centuries through common law and supplemented by the UK *Defamation Acts* of 1952, 1996 and 2013.[9] The developing doctrine of online intermediary liability in the UK has not yet provided a conclusive position, but this is an evolving area of jurisprudence as more cases subject to the 2013 Act make their way through the higher courts. The UK has an enshrined right to freedom of expression under article 10 of the *Human Rights Act 1998* (UK), but this right is subject to limits imposed by other laws that prohibit offensive or dangerous speech, as well as by civil obligations such as defamation.

[9] These statutes apply to England and Wales, some but not all provisions also apply in Scotland. For the purposes of this discussion we should be taken as referring to the law of England and Wales.

Legislative protections for intermediaries

2.19 The *Defamation Act 2013* (UK) introduced a new 'safe harbour' defence for operators of websites hosting user-generated content (section 5). The term 'website operator' is not defined in the *Defamation Act 2013* (UK), but UK Ministry of Justice guidance[10] notes that it covers websites hosting user-generated content, and does not affect other internet services such as search engines, services that simply transmit information, or services that provide access to a communications network.

2.20 Section 5 provides that, where an action for defamation is brought against the operator of a website in respect of a statement posted on the website, it is a defence for the operator to show that it was not the operator who posted the statement on the website. The defence is defeated if the claimant shows that:

- It was not possible for the claimant to identify the person who posted the statement
- The claimant gave the operator a notice of complaint in relation to the statement, and
- The operator failed to respond to the notice of complaint in accordance with any provision contained in the regulations.

2.21 The *Defamation (Operators of Websites) Regulations 2013* (UK) sets out the required complaints notice procedure by the operator in response to a notice of complaint in order to maintain the defence. This process includes the requirement that, where the person who posted the statement cannot be identified or is unwilling to engage in the process, material will be removed.

2.22 To date, there have been no cases decided in relation to section 5, so it is unclear how the defence will work. The lack of case law could point to the success of the safe harbor provision in providing an alternative dispute resolution, or it could be that the defence is rarely relied upon by intermediaries, as it is more straightforward to rely on other defences. There is still limited case law available on the *Defamation Act 2013* (UK), and it is likely to take some time for cases decided under this Act to make their way through the higher courts.

2.23 Section 1 of the *Defamation Act 1996* (UK) is broadly similar to the defence of innocent dissemination in the MDPs. It provides that a person has a defence in defamation proceedings if they show that: a) they were not the author, editor or publisher of the statement complained of; b) they took reasonable care in relation to its publication; and c) they did not know, and had no reason to believe, that what they did caused or contributed to the publication of a defamatory statement.

---

10 UK Ministry of Justice, see: https://www.gov.uk/government/publications/defamation-act-2013-guidance-and-faqs-on-section-5-regulations.

2.24 Unlike the clause 32 innocent dissemination defence in the MDPs, the UK defence provides additional guidance for determining whether a person took reasonable care, or had reason to believe that what they did caused or contributed to the publication of a defamatory statement. It provides that regard shall be had to: a) the extent of their responsibility for the content of the statement or the decision to publish it; b) the nature or circumstances of the publication; and c) the previous conduct or character of the author, editor or publisher.

2.25 The *Defamation Act 2013* (UK) introduced a new provision that offers additional protection to secondary publishers. Section 10 removes the court's jurisdiction to hear and determine an action against a secondary publisher unless it is satisfied that it is not reasonably practicable for an action to be brought against the author, editor or publisher.

2.26 The *Electronic Commerce (EC Directive) Regulations 2002* (UK) implement the European Parliament and Council *Directive 2000/31/EC*, which includes limitations of liability of intermediary service providers where they act as mere conduits, cache material or host material, provided that they do not have actual knowledge of unlawful content; and once notified of unlawful content, act expeditiously to remove access to the content.

Liability at common law

2.27 The leading authority on liability for third-party defamation is the English case of *Byrne v Deane* (***Byrne***).[11] Although decided in 1937, this has laid the foundation for jurisprudence on online intermediary defamation liability across common law jurisdictions. It established that liability for publication can arise not just from positive action, but also from failure to remove defamatory content once made aware of it.

2.28 *Godfrey v Demon Internet Ltd*[12] (***Godfrey***) applied the *Byrne* approach to an online bulletin board operator. The Court held that the defendant was not just a conduit in this case, because it hosted and transmitted the offending statement and could delete it if it wished. The defence of innocent dissemination was not available to the defendant, as it was determined that they had become a primary publisher by virtue of not acting once on notice of the defamatory statement.

2.29 *Bunt v Tilley*[13] later settled the position that merely providing a customer with an internet access service does not incur liability for an Internet Service Provider (**ISP**) for defamatory material sent by that customer. For the purposes of defamation liability, an ISP that performs only a 'passive' role in facilitating posting on the internet should not be deemed to be a publisher at common law. Eady J did emphasise that this only applied to cases where the ISP's involvement was merely providing the internet connection as a conduit, and did not displace the precedent set in *Godfrey* where the ISP was an active participant due to having agency over which chatrooms it hosted.

---

11 *Byrne v Deane* [1937] 1 KB 818.

12 *Godfrey v Demon Internet Ltd* [2001] QB 201, [1999] 4 All ER 342 (QB).

13 *Bunt v Tilley* [2006] EWHC 407 (QB).

2.30 *Tamiz v Google Inc*[14] endorsed the *Byrne* doctrine. The Court considered that Google (as the owner of Blogger) had the ability once notified, to remove the defamatory content. The Court did not think that Google was a publisher prior to notification of the defamatory material, since it cannot be said that Google either knew or ought to have known of the defamatory comments.

2.31 *Metropolitan International School Ltd v Designtechnica Corp*[15] then found Google, as operator of its search engine, was not a publisher of snippets in search results. The Court found that intermediaries that only play a role of passive facilitator are not publishers for the purposes of defamation law. 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 this case it was not possible to draw a complete analogy with a website host, because the search engine operator cannot press a button to ensure the offending words will never reappear on a snippet, and any blocking process could be evaded by the author simply moving the material elsewhere. Even after notification, Google still was not a publisher due to its lack of control. This view differs from the position the Australian courts adopted in *Trkulja v Google LLC*[16] (***Trkulja***), and means search engines do not currently have liability in defamation in the UK.

United States

2.32 Defamation law in the United States of America (**US**) is regulated at a state level, similar to Australia, however, the states do not have a uniform scheme, meaning outcomes vary significantly state-to-state. Some federal laws place limits on the ability to sue in defamation, most notably the First Amendment to the US Constitution, which protects freedom of speech.

2.33 Since the 1964 case of *New York Times Co. v. Sullivan*,[17] it has been made clear that the First Amendment has a limiting effect on defamation law across the US. The result is that US jurisprudence tends to be more defendant-friendly, with higher protections on free speech. The *Securing the Protection of our Enduring and Established Constitutional Heritage Act (2010*) (**SPEECH**) also makes foreign defamation judgments unenforceable by US courts if they are not consistent with the First Amendment right to free speech or if the defendant would have not been found liable if the case had been heard under US law.

14 *Tamiz v Google Inc* [2013] 1 WLR 2151 (CA).

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

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

17 *New York Times Co. v Sullivan* (1964) 376 U.S. 254.

Internet intermediary immunity

2.34 Section 230 of the *Communications Decency Act 1996* (US) (**CDA**) is widely lauded as being the law that 'created the Internet'.[18] Section 230 is currently under review by the US Department of Justice.[19]

2.35 The CDA states that 'no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'.[20] Subject to some limitations,[21] it effectively provides internet intermediaries with immunity for the publication of third-party content.

2.36 There have been just a small number of cases where courts have found that a 'provider or user of an interactive computer service' loses the benefit of section 230 if it 'materially contribut[ed] to its alleged unlawfulness'.[22] The US courts have not provided clear guidance on where the line is to be drawn between acceptable editing and where intervention is sufficient to make an intermediary an 'information content provider'. Where an intermediary edits or makes comment that can change the meaning of the information, and the new meaning is defamatory, they may lose the protection of section 230.[23]

Canada

2.37 Canada has a federal system, with all provinces apart from Quebec deriving their defamation law from English common law, and Quebec from the French civil law. Defamation law varies from province to province, and the Supreme Court of Canada, which is the highest court of law in Canada, makes decisions by applying the relevant province's laws.

2.38 The constitutional entrenchment of the right to free expression in section 2(b) of the *Canadian Charter of Rights and Freedoms* (1982) has led the Supreme Court of Canada to strengthen the defence of fair comment and create a new defence of responsible communication.[24] In the seminal case of *Hill v Church of Scientology*,[25] the Supreme Court of Canada, while declining to adopt the broad protections of freedom of expression in the

---

18 Kosseff, J. 2019, *Twenty-three words that created the internet*, Cornell University Press.

19 US Department of Justice, see: https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996.

20 Section 230(c)(1) of the *Communications Decency Act 1996* (US) (Protection for private blocking and screening of offensive material).

21 Section 230 does not affect federal criminal law, intellectual property law, State law that is consistent with the section or communications privacy law.

22 Laidlaw, E and Young, H, 2018, 'Internet Intermediary Liability in Defamation', *Osgoode Hall Law Journal*, 56 (1), p132

23 Electronic Frontiers Foundation, see: https://www.eff.org/issues/bloggers/legal/liability/230

24 Downard, P. 2010, *The Defence of Responsible Communication*, 51 Supreme Court Review (2d).

25 *Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130.

American approach in *New York Times Co. v Sullivan*, adopted a more restrained protection for responsible publications.

Intermediary liability at common law

2.39 The first major Canadian case dealing with internet intermediaries was *Weaver v Corcoran*,[26] where the Supreme Court of British Columbia found that the intermediary was a passive instrument in publication, but noted that, once on notice, had the intermediary failed to act, then it would be a publisher by omission.

2.40 Since then, Canadian courts have developed piecemeal precedent that makes it clear that the question of publication liability will be dependent on specific facts of each case.[27]

Law Commission of Ontario review of defamation in the digital age

2.41 In March 2020, the Law Commission of Ontario (**LCO**) released its Final Report – *Defamation Law in the Internet Age*.[28] It makes 39 recommendations for fundamental reforms to defamation law. Key proposals in relation to internet intermediaries are that:

- Intermediary platforms that host third-party content should be required to pass a notice of a defamation complaint onto the publisher, and take down content if the publisher does not respond to the notice. Failure to do so should result in regulatory fines being issued.
- Internet intermediary platforms would not be responsible for assessing the merits of a notice of complaint.
- Intermediary platforms would not have residual liability in defamation law as 'publishers' of third-party content.[29]

2.42 The LCO suggest that ISPs and search engines would not be subject to its proposed notice and takedown regime, since they are not directly connected with online publishers, but both ISPs and search engines may be subject to a court injunction to take down illegal content.[30]

---

26 *Weaver v Corcoran* (2015) BCSC 165.

27 Laidlaw & Young, *Internet Intermediary Liability in Defamation: Proposals for Statutory Reform 2017*, see: http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw-and-Young.pdf.

28 Law Commission of Ontario, *Defamation Law in the Internet Age- Final Report 2020*, see: https://www.lco-cdo.org/wp-content/uploads/2020/03/Defamation-Final-Report-Eng-FINAL-1.pdf (LCO Final Report).

29 LCO Final Report (n 28). Recommendation 19: a new notice regime for defamation complaints in respect of all publications. This includes specific requirements for intermediary platforms to forward the notice to the publisher of the allegedly defamatory content. Recommendation 35: a defamation action may only be brought against a publisher of the expression complained of. 'Publisher' should be defined to require an intentional act of communicating a specific expression. Recommendation 36: a publisher of a defamatory expression should not be liable for republication of the expression by a third-party unless the publisher intended the republication. Recommendation 38: there should be a takedown obligation on intermediary platforms hosting third-party content available to users in Ontario. This would operate in conjunction with the new notice regime.

30 LCO Final Report (n 28).

Context – Regulatory changes underway in Australia

2.43 The Australian Government is responsible for laws and regulations relating to internet governance and online safety. This involves a range of matters relating to online services and infrastructure, including internet governance, cyber security issues, competition and online harms.

2.44 There are two areas of particular relevance to this Discussion Paper. The first is the online safety framework overseen by the eSafety Commissioner – which is currently the subject of a legislative reform process. The second is the ACCC *Digital Platforms Inquiry Final Report* and the Australian Government's roadmap for implementing its recommendations. These are relevant because they set the broader context in which internet intermediaries operate in Australia – now and in the future.

Online Safety

2.45 The *Enhancing Online Safety Act 2015* (Cth) establishes and sets out the functions of the eSafety Commissioner, which include:

- Administering a complaints system for cyber-bullying material targeted at an Australian child.
- Administering a complaints and objections system for non-consensual sharing of intimate images.
- Administering the online content scheme under the BSA.

2.46 The *Enhancing Online Safety Act 2015* (Cth) includes a number of definitions for different online services. The Act sets out which powers of the eSafety Commissioner apply to which services and when.

2.47 In 2018, the eSafety Commissioner developed a set of voluntary Safety by Design principles to place the safety and rights of users at the centre of the design, development and deployment of online products and services. These principles were developed in collaboration with online service providers.

2.48 On 11 December 2019, the Australian Government released an Online Safety Charter,[31] articulating the Government's expectations of the steps online service providers should take to protect their users from harmful online experiences. The Charter acknowledges that online providers have a responsibility to take meaningful action to address and prevent harms from being incurred by end-users. The Charter endorses the eSafety Commissioner's Safety by Design principles as best practice.

2.49 The Australian Government has also committed to the development of a new Online Safety Act. On 11 December 2019, the *Online Safety Legislative Reform Discussion Paper* was released, seeking comments on the key elements of a proposed new Online Safety Act.[32] The *Online Safety Legislative Reform Discussion Paper* described online harms as including

---

31 Australian Government Online Safety Charter, published 11th December 2019.

32 Australian Government Department of Infrastructure, Transport, Regional Development and Communications, 11 December 2019, *Online Safety Legislation Reform – Discussion Paper*, see: https://www.communications.gov.au/have-your-say/consultation-new-online-safety-act.

'cyberbullying, abusive commentary or 'trolling', the non-consensual sharing of intimate images (image-based abuse), grooming for the purpose of child sexual abuse, cyberflashing, doxing and cyberstalking'.[33] Some (but not all) of these harms may also involve the online publication of defamatory matter.

2.50 Some of the key elements of a proposed new Online Safety Act that are set out in the *Online Safety Legislative Reform Discussion Paper* are:

- The introduction of Basic Online Safety Expectations that would apply to all social media services as a starting point.
- The existing cyberbullying scheme, which applies to social media services would be extended to apply to 'relevant electronic services' and 'designated internet services'.
- The creation of a new cyber abuse scheme for adults. This would apply to material that is menacing, harassing or offensive and intended to have an effect of causing serious distress or harm.
- Inclusion of the current online content scheme in the BSA to address illegal and harmful content.
- The take-down time for all four online safety schemes (existing and proposed) would be 24 hours.
- A scheme to reduce the availability of harmful material on ancillary service providers, such as search engines and app stores. The eSafety Commissioner would have 'reserve powers' to ask search aggregator services to delist or de-rank websites that have been found by the eSafety Commissioner to be systematically and repeatedly facilitating the posting of cyberbullying or cyber abuse.

2.51 On 23 December 2020, the Australian Government Department of Infrastructure, Transport, Regional Development and Communications issued an exposure draft of the Online Safety Bill 2020 (Cth) (**Online Safety Bill**). Some key features in addition to those outlined in the *Online Safety Legislative Reform Discussion Paper* include:

- The BSA immunity provision has been moved into the Online Safety Bill 2020 under clause 235.
- Clauses 88 and 90 of the Bill provide that, where required by the eSafety Commissioner, social media services, relevant electronic services, designated internet services and hosting service providers must take down cyber-abuse material within 24 hours.
- Part 13 of the Bill also provides the eSafety Commissioner with the power to obtain end-user identity information and contact details from online service providers, including social media service providers.

2.52 On 24 February 2021, the Australian Government introduced the Online Safety Bill 2021 in Parliament.

---

[33] *Online Safety Legislation Reform – Discussion Paper* (n 32) 14.

Australian Consumer and Competition Commission (ACCC) *Digital Platforms Inquiry Report* and Australian Government Response

2.53 In December 2017, the ACCC was directed to consider the impact of digital platforms on competition in the media and advertising services markets. The Terms of Reference for the Inquiry stipulated that the three categories of digital platforms to be considered were: online search engines, social media platforms and other digital content aggregation platforms.

2.54 On 26 July 2019, the ACCC's *Digital Platforms Inquiry Final Report*[34] was released. The ACCC made a number of findings regarding the functions of digital platforms, their business models and market power. The report includes 23 recommendations that cover competition law, consumer protection, media regulation and privacy law.

2.55 On 12 December 2019, the Australian Government released a response and implementation roadmap for the *Digital Platforms Inquiry Final Report*.[35]

2.56 While the focus of the ACCC *Digital Platforms Inquiry Final Report* was largely on matters relating to competition, there are several aspects of the report and the Australian Government's implementation roadmap that are relevant for the purposes of this Discussion Paper:

- The ACCC Report includes detailed analysis and a number of findings in relation to the activities and functions of digital platforms. This includes actively selecting, evaluating, ranking and arranging content – as well as being the gateways to online news for many consumers.
- The implementation of the ACCC's recommendations will affect the regulatory environment for digital platforms and, in turn, the experience of users of those platforms.

2.57 The following ACCC recommendations are particularly relevant:

- **Recommendation 6:** that a platform-neutral regulatory framework be developed to ensure effective and consistent regulatory oversight of all entities involved in content production or delivery in Australia, including media businesses, publishers, broadcasters and digital platforms.

  In response, the Australian Government is undertaking a staged process to reform media regulation towards an end state of a platform-neutral regulatory framework covering both online and offline delivery of media content to Australian consumers.

- **Recommendation 7:** that designated digital platforms provide codes of conduct governing relationships between digital platforms and media businesses to the Australian Communications and Media Authority **(ACMA)**. In response to this recommendation, on 20 April 2020 the Australian Government announced that it had directed the ACCC to develop a mandatory code of conduct to address bargaining power

---

34 Australian Competition and Consumer Commission **(ACCC)**, *Digital Platforms Inquiry: Final report 2019*, see: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

35 Australian Government, *Regulating in the digital age, Government Response and Implementation Roadmap for the Digital Platforms Inquiry*, December 2019, see: https://treasury.gov.au/publication/p2019-41708.

imbalances between Australian news media businesses and digital platforms.

The code would initially apply only to Facebook and Google. The ACCC and Australian Treasury released a draft code for public consultation on 31 July 2020. It would allow news media businesses to bargain individually or collectively with Google and Facebook over payment for the inclusion of news on their services. Following consultation, the ACCC made recommendations to the Government based on the views put forward by stakeholders. The Government considered these recommendations and developed legislation. The Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020 (Cth) was introduced to the Australian Parliament on 9 December 2020.

- **Recommendation 15:** that digital platforms with more than one million monthly active users in Australia implement an industry code of conduct to counter disinformation. In response to Recommendations 14 and 15, the Government asked digital platforms to develop a voluntary code on disinformation and news quality. The ACMA is required to report to the Australian Government by 30 June 2021 on the code process, the adequacy of digital platform's measures and the broader impacts of disinformation in Australia.

  On 26 June 2020, the ACMA released a position paper on misinformation and news quality. On 22 February 2021 the Digital Industry Group Inc. **(DIGI)** launched a new code of practice to reduce the risk of online misinformation causing harm to Australians. According to DIGI, the Australian Code of Practice on Disinformation and Misinformation has been adopted by Twitter, Google, Facebook, Microsoft, Redbubble, and TikTok.

- **Recommendation 18:** that the Office of the Australian Information Commissioner develop a privacy code for online platforms.

  In March 2019, the Australian Government announced it would consult on draft legislation to amend the *Privacy Act 1988* (Cth), including to introduce a binding privacy code that would apply to social media platforms and other online platforms that trade in personal information.

- **Recommendations 22 and 23:** that digital platforms comply with internal dispute resolution requirements (recommendation 22) and establishment of an ombudsman scheme to resolve complaints and disputes with digital platform providers (recommendation 23).

  The Australian Government's response indicated that it will develop a pilot external dispute resolution scheme in consultation with major digital platforms, consumer groups and relevant agencies. The outcomes of the pilot scheme will inform consideration of whether to establish a Digital Platforms Ombudsman to resolve complaints and disputes between digital platforms and the individual consumers and small businesses using their services.

3. Key Issues

3.1 In this section, the DWP outlines five key issues for consideration and puts forward questions for stakeholder feedback. The issues are:

- 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

3.2 The DWP also asks if there are any other issues that need to be considered in relation to liability of internet intermediaries for the publication of third-party content.

Assessing the reform options

3.3 The objects of the MDPs provide guidance for the reform process and criteria against which the DWP can assess options for reforms. 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.

3.4 For the purposes of assessing the options presented in this Discussion Paper, there is an additional criterion that the DWP considers relevant:

- 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.[36]

Freedom of expression

3.5 The volume and variety of user-generated content published online creates a real challenge for defamation law. Internet intermediaries argue that it is not appropriate for them to be the arbiters of what content is defamatory. This is traditionally a matter for the courts. Defamation law is a strict liability tort, so there is a risk that intermediaries will simply remove content to avoid being sued. This could result in content published online being unnecessarily removed or blocked, which would have a chilling effect on freedom of speech.

---

[36] See further commentary on the role of technological innovation in Pappalardo, K and Suzor, N 2018 *The Liability of Australian Online Intermediaries Sydney* Law Review 40 (4) p 472-473, and submission by DIGI to the DWP on the importance of certainty in legal liability for digital business, see: https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/defamation-submission-digital-industry-group.pdf. Also, OECD (n 3).

Effective and fair remedies for harm to reputation

3.6 One of the primary objectives of defamation law is providing effective recourse to people or certain organisations who may have had their reputation harmed by the publication of defamatory matter. Part 3 of the MDPs provides for a mandatory concerns notice process, and also provides the option for a publisher to make an offer to make amends. This includes articulating what must and may be included in a reasonable offer to make amends. For example, a publisher must include an offer to publish a correction, and it may include an offer to remove material from a website. Part 3 of the MDPs is a key reference point when considering what an effective and fair remedy is in the online context.

Promoting speedy and non-litigious methods of resolving disputes

3.7 A person who claims that they have been defamed may not be able to access a timely resolution if the only path to a remedy is seeking a court order. In the age of digital communications, the ease and speed with which defamatory matter can be published and disseminated to a wide audience means that a quick response may be of the utmost importance.

3.8 Under Part 3 of the MDPs, the concerns notice (which will be mandatory) and offer to make amends process are designed to encourage parties to resolve disputes without the need to resort to litigation, but these processes do not directly address the publication of defamatory third-party content.

Technological innovation and the emergence of new online services and activities

3.9 In its 2010 report on the economic and social role of internet intermediaries, the Organisation for Economic Co-operation and Development (OECD) acknowledged that, 'Internet intermediaries enable creativity and collaboration to flourish among individuals and enterprises and generate innovation.'37

3.10 The DWP recognises the significant and ongoing role that internet intermediaries have to play, both socially and economically, in Australia and around the world. To ensure the longevity of the reforms, the reforms will focus on functions rather than types of internet intermediaries, to ensure defamation laws can adapt as technological advances are made.

37 OECD (n 3) 8.

ISSUE 1: Categorising internet intermediary functions

Who is a publisher in defamation law?

3.11 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 in defamation law. This includes anyone who repeats, endorses or adopts the matter in question. In certain circumstances, failing to remove defamatory material from a publication controlled by the defendant can also constitute publication of that material. This is known as 'publication by omission'.

3.12 The question of whether the defendant is a publisher is a matter for evidence in each case, concerning the level of 'participation' and 'control' attributable to the defendant in the publication process.[38]

Who is a publisher in the context of online communications?

3.13 In the context of online communications, this broad definition of publisher potentially captures a whole range of actors that have different motivations, capabilities and relationships to the allegedly defamatory content.

3.14 In the first instance, the content is created and then posted or uploaded online by the **originator**. Originators may produce content such as a tweet, or write comments on blogs or fora. They may write articles for newspapers or websites. They could be podcasters producing audio content, or releasing apps for mobile devices. The variety of different kinds of content is endless.

3.15 The intentions of originators in publishing content online also vary. At one end of the spectrum, the originator may be a 'troll' who is intentionally, and repeatedly posting content that is offensive or inflammatory. At the other end of the spectrum, the originator may be a whistle blower bringing to light information of public importance. In between these two ends, the originator may be publishing content that they consider legitimate, such as a news article or report, a comment, a link, or expression of support for the views of another. The originator may be anonymous, publishing under a pseudonym, or clearly identifiable. They may be uncontactable or recalcitrant. They may be well resourced or impecunious. In some cases, the originator may have lost control of the content – for example if it has gone 'viral'.

3.16 For content to be communicated online, **internet intermediaries** must be involved. These range from ISPs, to internet content hosts, search engines and social media platforms (to name a few). It could also include an individual or an organisation hosting an online discussion forum that permits or invites third-party content. Some internet intermediaries, by virtue of their particular function, have minimal connection with the content posted by the originator. Others may play a more active role – for example, by selecting, moderating or curating it. Some intermediaries may create new content out of algorithms that automatically generate content, such as auto-complete search suggestions or snippets in search results. Depending

---

38 *Thompson v Australian Capital Television Pty Ltd* [1996] HCA 38; (1996) 186 CLR 574; *Google LLC v Duffy* [2017] SASCFC 130 per Kourakis CJ, at [92].

on their function, each internet intermediary will have a different relationship with both the content and the originator. In many cases, a range of internet intermediaries will be involved in the publication of the content.

The Broadcasting Services Act 1992 (Cth)

3.17 Clause 91(1) of Schedule 5 to the BSA, inserted in 1999, provides an immunity for 'internet service providers' and 'internet content hosts' in certain circumstances in relation to third-party material.

3.18 It provides that a law of a state or territory, or a rule of common law or equity, has 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.

3.19 The application of clause 91(1) in the current online environment is unclear. First, it is unclear what 'aware of the nature of' the internet content means. While it appears that 'aware' means actual awareness (as opposed to constructive awareness), it is not clear whether, for the purposes of clause 91(1) as applied to state defamation laws, a general complaint to an internet intermediary is sufficient to make it aware of the 'nature of the internet content', or whether a complaint specifying the defamatory nature of the content, or even a court judgment that the material is defamatory, is required before the internet intermediary loses the clause 91(1) immunity.

3.20 The terms 'internet service provider' and 'internet content host' are also unclear. Stakeholders have submitted that these terms may not cover search engines. It is also possible that an internet intermediary may fall within more than one of these defined terms.

- 'Internet service provider' is defined as 'a person [who] supplies, or proposes to supply, an internet carriage service to the public'.
- 'Internet content host' is defined as 'a person who hosts internet content in Australia, or who proposes to host internet content in Australia'. A 2012 New South Wales Court of Criminal Appeal decision held that the definition of 'internet content host' could include 'any party in control of a website to which material has been uploaded'.[39] This understanding of 'internet content host' was reiterated in *Fairfax Media Publications; Nationwide News Pty Ltd; Australian News Channel Pty Ltd v Voller* [2020] NSWCA 102 (***Voller***), where Basten JA considered 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'.

[39] *Fairfax Digital Australia & New Zealand Pty Ltd v Ibrahim* [2012] NSWCCA 125.

3.21 There is uncertainty as to the territorial reach of clause 91(1). In *Voller*, Basten JA in obiter, considered that the better view of clause 91(1) is that it applies only to those internet content hosts which host content on servers located in Australia.

3.22 These questions of scope have important implications for defamation law in the online environment. Clause 90 of Schedule 5 to the BSA states that, 'It is the intention of the Parliament that this Schedule is not to apply to the exclusion of a law of a State or Territory to the extent to which that law is capable of operating concurrently with this Schedule.' However, the mandatory nature of clause 91 leaves little room for clause 90 to operate to provide for other legislation to work alongside clause 91. Also, as provided by section 109 of the *Commonwealth of Australia Constitution Act 1900* (**Australian Constitution**), any provision of the MDPs which is inconsistent with clause 91(1) is invalid. This means that an internet intermediary that is considered an 'internet service provider' or an 'internet content host' may have immunity under clause 91(1) to a defamation claim, prior to it becoming 'aware' of the nature of that content.

Categorising internet intermediaries

3.23 It is difficult to define the different roles and functions of internet intermediaries – particularly because they are always evolving, and one internet intermediary may perform multiple roles simultaneously.[40] There is always a risk that such classifications can become outdated by technological changes.

3.24 Nevertheless, the task of this Discussion Paper is to consider what liability internet intermediaries should have in defamation – based on the extent to which they contribute to the risk of harm to reputation resulting from the publication of user-generated content. This requires an understanding of what internet intermediaries do and are capable of doing.

3.25 In this Discussion Paper, the umbrella term **internet intermediaries** is used. This is based on the description of 'internet intermediaries' by the OECD as entities 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'.[41]

3.26 Internet intermediaries range from internet access and service providers to search engines, to social media platforms. For the purposes of considering liability in defamation, based on recent developments in Australian case law, we use the term internet intermediaries in this paper to also include individuals or organisations that host online forums that allow or invite third-party comments.

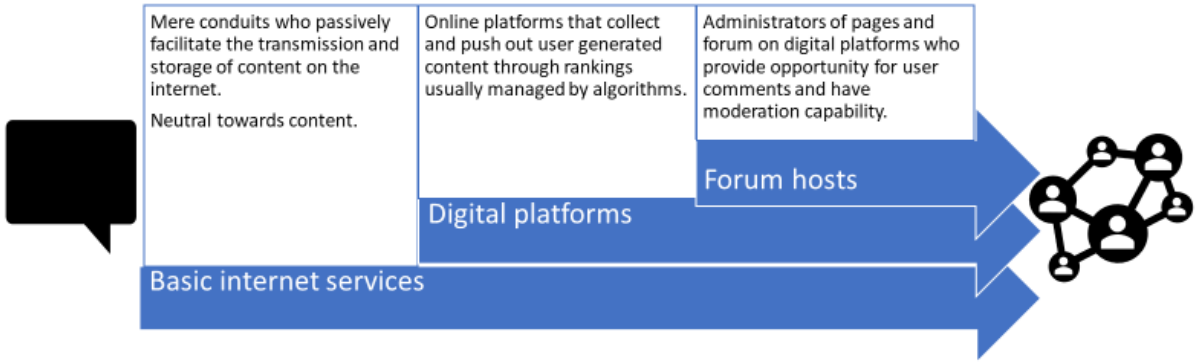
---

40 OECD (n 3) 10; ACCC (n 34) 42.

41 OECD (n 3) 9.

3.27 For the purposes of this paper, the DWP proposes to group the functions of internet intermediaries into three categories:

1. **Basic internet services:** internet intermediaries that act as mere conduits, passively facilitating internet use. They are content neutral, which means that they neither have an interest in, nor the capacity to promote, particular types of content being generated or accessed by users.
2. **Digital platforms:** as described by the ACCC, 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).



Question 1: Categorising internet intermediaries

(a) Is the grouping of internet intermediary functions into the three categories of 'basic internet services', 'digital platforms' and 'forum hosts' a useful and meaningful way to categorise internet intermediary functions for the purpose of determining which functions should attract liability? Why?

Basic internet services

3.28 With the **basic internet services** category, the DWP is seeking to identify which internet intermediary functions can be understood as mere conduits – similar to telephone or postal services in the analogue world. The key feature the DWP expects these functions to share is passivity. This includes being content neutral. Basic internet services would neither have an interest in, nor the capacity to promote, particular types of content being generated or accessed by users. The DWP proposes to use passivity and neutrality towards content as a basis for which to determine what functions should not attract liability.

3.29 In his 2016 book *The Liability of Internet Intermediaries*, Jaani Riordan proposes a taxonomy of internet intermediaries which distinguishes between internet intermediaries based on their functions. The first layer of this taxonomy is **Physical layer services**, which 'rarely exercise control over content'. Their function is to provide 'the basic connectivity necessary for communication'.[42] Examples include modems, optic fibres and wireless access points. Riordan notes that these services are 'very rarely involved in disputes over liability for *content* because they are simply too remote from the nexus of wrongdoing'.[43]

3.30 The next layer is the **Network layer services**, which 'interpret and route data for higher-level applications' but 'do not inspect or modify data'.[44] Riordan lists a number of sub-classes of network layer services, including ISPs, cloud service providers and 'hosts'.

3.31 Unlike the physical layer services, these types of network layer services functions have been, or have the potential to be, the subject of disputes over liability in defamation law. It is important therefore to understand what they do – and the extent to which their position in relation to content is passive and neutral.

Internet Service Providers (ISPs)

3.32 The BSA provides that 'if a person supplies, or proposes to supply, an internet carriage service to the public, the person is an internet service provider'.[45]

3.33 Riordan describes ISPs as connecting 'subscribers to the internet by supplying telecommunications facilities and access equipment, such as subscriber lines'. This includes mobile network operators.[46]

3.34 In simple terms, ISPs provide services for connecting to the internet. Their characteristics include: they act as a utility – providing access to their infrastructure (which they either own or lease); payment by users for their services – usually by way of a contractual subscription; and usually charging based on volume of use (measured in traffic – both upload and download) rather than the nature of use.[47] ISPs cannot control the content posted using their services beyond blocking access to content on a URL [uniform resource locator] basis.

---

42 Riordan (n 1) 37.

43 Riordan (n 1) 38.

44 Riordan (n 1) 34.

45 Clause 8, Schedule 5, BSA.

46 Riordan (n 1) 38.

47 Cisco, ISP Services and Characteristics, see: http://borg.uu3.net/cisco/inter_arch/page05.html#:~:text=from%20different%20ISPs.-,ISP%20Backbone%20Selection%20Criteria,networks%E2%80%94and%20traffic%20exchange%20agreements.

3.35 In a UK case that considered whether an ISP, in providing a connection to the internet, was a publisher for the purposes of defamation law, the Judge described the ISP in the same vein as a telephone company or 'other passive medium of communication'.[48]

Hosts and cloud service providers

3.36 Riordan describes hosts as supplying 'storage and transmission facilities that allow hosted services to be accessed by other internet users'.[49] Riordan notes that the relationship between hosts and customers is primarily contractual, and that 'almost all conditions of service prohibit the publication of defamatory, copyright-infringing and other tortious content'.[50] This would presumably give hosting services the grounds to remove content if found to be defamatory; generally, where there is evidence of a violation of terms of service, these providers terminate a user's account, rather than disabling specific content.[51]

3.37 While the BSA also includes a definition of 'internet content host', it very broad and there is some uncertainty as to its scope.

3.38 Riordan describes cloud services as offering 'remote computational and storage services for on-demand access at network edges' – noting that services such as webmail and databases are increasingly delivered via cloud infrastructure.[52]

3.39 Since the publication of Riordan's book, the use of cloud services has proliferated, with many commonly used digital applications being hosted in the cloud. In the context of this Discussion Paper, the characteristics of cloud and server hosting are similar. Both provide mechanism for content to be stored and accessed online.

<u>Can ISPs, hosts and cloud service providers be classified as basic internet services?</u>

3.40 ISPs are commonly considered to be the internet equivalents of telephone and postal services. This is on the basis that they are mere passive facilitators and are not concerned with the nature of the content they transmit. It is arguable, although less clear, that the functions of hosts and cloud service providers can be categorised in the same way. The challenge is that these services are increasingly diverse.

<u>Other functions that could be considered basic internet services</u>

3.41 Based on the concepts of passivity and content neutrality, other functions that may fall into the definition of basic internet services could include: online document creators (such as Microsoft Office 365 and the Google Docs suite) and email services (such as Outlook and Gmail).

---

48 *Bunt v Tilley and others* [2006] EWHC 407 (QB) 345 per Eady J.

49 Riordan (n 1) 38.

50 Ibid.

51 Ibid.

52 Ibid.

Question 2: Categorising basic internet services

(a) What internet intermediary functions should be categorised as **basic internet services**? It is proposed that to be categorised as a basic internet service the internet intermediary must be a mere conduit (similar to telephone or postal services) in that they do not have an interest or involvement in the nature of the content they transmit or host.

(b) What are the key concepts that should determine if an internet intermediary function is a **basic internet service**? Is passivity and neutrality an appropriate basis on which to determine which internet intermediary functions attract liability?

(c) Are there any functions that could be categorised as 'basic internet services' but should give rise to liability, or are there circumstances in which basic internet services should be liable?

Digital platforms

3.42 The third and final layer of Riordan's taxonomy is **Application layer services**, which he groups into three sub-classes:

- Platforms (such as social networks and publishing services);
- Gateways (such as search engines); and
- Marketplaces (such as Amazon).

3.43 Some of the key functions (for the purposes of this Discussion Paper) that fall under Riordan's application layer services were also considered by the ACCC in its Digital Platforms Inquiry Final Report. The ACCC used the term digital platforms to include online search engines, social media platforms and other digital content aggregation platforms.

Common features of digital platforms

3.44 Riordan describes application layer services as 'by far the most diverse', being where content is 'transacted' – noting that application layers operate 'closest to end-users and exercise the most direct control over application content'.[53]

3.45 A general description used by the ACCC is that 'digital platforms are applications that serve multiple groups of users at once, providing value to each group based on the presence of other users'.[54] This ability to increase the value to users through the presence of other users is the 'network effect', which is one of the factors that the ACCC considers has contributed to the growth of digital platforms.[55] The ACCC Report found that the two largest digital platforms, Facebook and Google, generate much of their value through their ubiquity, as the longer users stayed on these websites, the richer the data set on users would become, allowing for increasingly valuable information for targeted advertisers.[56]

---

53 Riordan (n 1) 40.

54 ACCC (n 34) 41.

55 ACCC (n 34) 63.

56 ACCC (n 34) 55 and 209 - 211.

3.46 The ACCC also made clear that some of the major digital platforms provide a range of services, and that these services are constantly changing.[57]

3.47 In considering the role of digital platforms in Australian media markets, the ACCC concluded that digital platforms are 'considerably more than mere distributors or pure intermediaries in the supply of news content in Australia'.[58] This is due to digital platforms increasingly performing functions that are comparable to online media companies – such as actively selecting, evaluating, ranking and arranging content.

3.48 Digital platforms also at times automatically generate content, such as auto-complete search suggestions and automatically generated images and snippets in search results produced by search engine algorithms. These algorithms can enhance public access to information available online. However, there are also potential harms to individual reputations when they generate defamatory results.

3.49 The DWP recognises that there are is a broad range of services and functions that fall under the **digital platforms** category – and that they have different purposes and capabilities.

Social media platforms

3.50 The ACCC defined 'social media platforms' as: online services that allow users to participate in social networking, communicate with other users, and share and consume content generated by other users (including professional publishers). Social media platforms generally display content for consumption as linear 'feeds', curated by algorithms or displayed chronologically. Examples include Facebook, Instagram and Snapchat. Platforms may also offer additional functions, including instant messaging services.[59]

3.51 Riordan notes that key attributes and practices for platforms are user-created content, content moderation (with techniques including pre-publication approval, post-publication removal and automated content filtering) and algorithmic and community moderation.

Digital content aggregators

3.52 The ACCC defined 'digital content aggregators' as online intermediaries that collect information from disparate sources and present them to consumers as a collated, curated product. Those specialising in journalism – 'news aggregators' – are the most relevant example for the purposes of the ACCC's Inquiry. Users may be able to customise, filter or search their aggregation results. Examples include Google News, Apple News, and Flipboard.[60]

---

57 ACCC (n 34) 42.

58 ACCC (n 34) 170.

59 ACCC (n 34) 41.

60 Ibid.

3.53 For the purposes of defamation, it is likely that, in the event that defamatory content was disseminated through aggregators, the complainant would, in the first instance, seek recourse from the journalist/media organisation that originally published the story. However, whether the aggregator could be liable for publication may depend on the extent to which they manipulate and spread the information they collate, including through algorithms that promote certain types of content.

Search engines

3.54 The ACCC defined '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. Search engines operate in an automated fashion using sophisticated algorithms to collect information (commonly known as 'crawling') and to provide search results. Examples include Google Search, Bing, and Yahoo!.[61]

3.55 In his taxonomy, Riordan describes the functions of gateways including search engines as being to 'collate, index and distribute hyperlinks to third parties' internet content'. Riordan notes 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'.[62]

3.56 The ACCC found that search engines rank results using algorithms, and that top ranked results were more likely to be viewed by users.[63] The ACCC found that the position at which content is displayed on digital platforms has a significant impact on the scope of the publication. Content that ranks high on a linear feed is more likely to be viewed by users, meaning whatever the algorithms rank as most relevant will in turn increase the readership of that content.[64]

3.57 Today, search engines vary in design and function, meaning it may not be possible to accurately categorise all search engines as digital platforms. It is important to consider the distinction between the different functions performed by search engines, such as indexing of content, ranking results, curating results, auto populating search terms, snippets and highlights and what role these may have in publication. It may be that these functions need to be categorised at a more granular level when determining liability.

3.58 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, search engines can allow users to pay to promote their content and have it featured higher in the list of search results.

61 Ibid.

62 Riordan (n 1) 43.

63 ACCC (n 34) 55 and 209 - 211.

64 ACCC (n 34) 172.

Other functions that could be considered digital platforms

3.59 The ACCC did not consider all digital platforms as part of its Inquiry, as the Terms of Reference focussed only on search, social media and content aggregation platforms. In its ongoing role monitoring 'digital platform services', the ACCC is now considering an expanded group of 'digital platform services' including messaging services and electronic marketplaces.[65]

3.60 There are some other platforms in particular that warrant attention in the context of potential liability in defamation.

Review websites

3.61 Online and offline retailers and services are increasingly becoming reliant on user reviews in order to build and maintain patronage. New digital platforms are emerging for the primary purpose of hosting reviews, with many also leveraging reviews to refer sales and earn commissions, such as TripAdvisor. Review websites vary in the extent to which they require verification of reviewers and moderation of reviews. For example, Google allows reviews from anyone signed into their Google account, but does not verify whether that user has actually used the product or service they review, while Product Review signposts where a review is verified, generally through requiring evidence to be uploaded confirming use of the product being reviewed. To access reviews, users either search for a specific brand, or company, rather than being pushed suggested content through algorithms, or can search for businesses by types or location and these results can be ranked and curated.

Podcast aggregators

3.62 Podcast aggregators, similar to other digital content aggregators pull podcasts and related media content from RSS [really simple syndication] or XML [extensible markup language] feeds and display them through front end systems that allow users to subscribe and browse podcasts. Users can search for specific podcasts, but many apps, such as Apple Podcast, also provide curated lists of podcasts based on user rankings and reviews and promoted content. Similar to digital content aggregators, usually the originator will be identifiable for the purposes of defamation disputes. However, where certain content is highlighted and pushed to users through curated lists, then the aggregator may play an active role in the publication.

---

65 In December 2019, the Government announced that the ACCC would have a role for five years to monitor digital platform services and their impacts on competition and consumers. As part of this role, the ACCC is to provide the Australian Government with six-monthly reports on digital platform services. The latest report is the ACCC Digital Platform Services Inquiry, Interim report September 2020, see: https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Service%20Inquiry%20-%20September%202020%20interim%20report.pdf.

Instant messaging services

3.63 In recent times, some messaging services have expanded their capability to allow messages to be sent and viewed by hundreds of users in the same message thread instantly. This presents new opportunity for defamatory content to be shared in a manner that increases the harm caused to others. Increasingly, these services are encrypted so that only those within the message chat thread or can view the content. In order for a message thread to exist, a singular host must create it. In many cases, but not all, that host may have additional administrative powers over the message, including the ability to add and remove members, as well as to delete content. Sometimes all members of the message can do this.

Question 3: Categorising digital platforms

(a) Is it appropriate to adopt the classification of digital platforms used in the ACCC's *Digital Platforms Inquiry Final Report* to understand their roles and functions for the purpose of considering liability in defamation for third-party content?

(b) Do the common features listed above accurately reflect the functions of digital platforms?

(c) Should search engines be treated as a single function for the purpose of categorising intermediaries for defamation liability? Or do search engines have different functions, some of which should or should not give rise to liability?

(d) Is it appropriate to consider search engines a subset of digital platforms, or should they be considered as a separate category that can have access to separate specific defences?

(e) Are there new and emerging digital platform functions that need to be considered?

(f) Are there any publishing functions of digital platforms that should not attract liability? Why?

(g) Is it appropriate to consider digital platforms as having comparable functions to online media companies, or should they be considered as separate categories with different responsibilities and defences? Why?

Forum administrators

3.64 Most of the analysis and writing about online intermediary liability focuses on the service providers. This is appropriate in the context of considering regulatory mechanisms and regimes. There is a final group of intermediaries to consider, which has been prominent in recent developments in Australian defamation case law.66 This is anyone who is the host or administrator of an online forum that permits third-party commentary.

66 *Voller v Nationwide News Pty Ltd* [2019] NSWSC 766; *Fairfax Media Publications Pty Ltd v Voller* [2020] NSWCA 102. The High Court has granted special leave to appeal: *Fairfax Media Publications Pty Ltd v Voller* [2020] HCATrans 214.

3.65 This might be a large company or a small community group hosting a Facebook page or an individual administrator of an online forum or instant messaging thread. Any of these forum administrators is potentially liable for defamatory comments made by third parties – particularly if they are aware of it and have the capacity to take it down. Forum administrators could include persons or entities that have created large instant messaging threads, if when doing so they provide a platform for others to post content but retain the ability to review and remove offending content.

Question 4: Categorising forum administrators

(a) Is it appropriate to consider 'forum administrators' as a separate category of internet intermediaries? If so, how should this be defined?

(b) What are the different circumstances and scenarios involving forum administrators that need to be considered?

ISSUE 2: Immunities and defences

3.66 In this section the DWP sets out options for reform to clarify or modify the liability of internet intermediaries in respect of third-party content. These options are drawn from existing principles of defamation law and approaches taken in other jurisdictions. It should be made clear from the outset that they are not mutually exclusive and a number of options could potentially operate together. The DWP is seeking stakeholder feedback on the viability and appropriateness of each of the options – particularly in so far as they might apply to different internet intermediary functions.

3.67 The options canvassed are presented on a spectrum of liability, from least change from the status quo, to broadest immunity from liability for internet intermediaries:

- Option 1: Retain status quo with some minor changes to the MDPs to clarify the role of internet intermediaries
- 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
- Option 4: Immunity for internet intermediaries for user-generated content unless the internet intermediary materially contributes to the unlawfulness of the publication

3.68 One of the key challenges of law reform in this area is to address the need for certainty at the same time as providing sufficient flexibility to accommodate the wide range of internet intermediary functions – both existing and emerging. Focusing on functions of internet intermediaries provides flexibility to address new and emerging technologies, while also outlining expectations on internet intermediaries if they want to gain the benefit of new defences and immunities. If designed well, the reforms may prompt reconsideration of business models to better protect users from the risk of harm to reputation, in order to reduce risk of liability of internet intermediaries.

Option 1: Retain status quo with some minor changes to the MDPs to clarify role of internet intermediaries

3.69 This option canvasses three ways in which the current position in defamation law can be retained, with some minor changes to better accommodate internet intermediaries. Three sub-options are presented for consideration and comment.

Option 1a: The status quo

3.70 The concept of publication under defamation law is very broad. As communications have moved online, they are enabled by internet intermediaries. In traditional publications, defamatory publications could be made without the use of intermediaries. But where they were done so with the use of intermediaries, for example, by using book publishers and book sellers, those intermediaries could be held liable for the defamatory publication, subject to a defence being available. The defence of innocent dissemination (discussed in detail in Option 2 below) was developed to protect these intermediaries where they were deemed to not have been aware of the defamatory publication they enabled.

3.71 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. Australia has diverged from the UK in the findings as to whether certain internet intermediaries are publishers of third-party content. The role of internet intermediaries in publication, and their ability to avail themselves of the innocent dissemination defence, is an evolving issue.[67] The current case law in Australia is not sufficiently settled to definitely say whether internet intermediaries are treated the same as other publishers for the purposes of liability of third-party content.

How the law has approached the question of internet intermediaries as publishers for third-party content

Mere conduits

3.72 Generally speaking, in defamation law a defendant who merely 'passively facilitates' the communication of the content is not considered a publisher. An example is a telephone company providing wires or a 'mere conduit' through which a conversation is transmitted.[68] Such defendants are considered not to be a position to control the content they disseminate, nor responsible for what their 'dumb pipes' contain. Arguably, this means that ISPs would not be considered publishers for defamation purposes. This is the position that has been adopted in the UK.[69] While this view has recently been expressed in obiter by a state appeal court,[70] there is no binding higher court authority on this point in Australia.

---

67 Rolph (n 7)

68 *Byrne v Deane* [1937] 1 KB 818, *Bunt v Tilley* [2007] 1 WLR 1243; *Google Inc v Duffy* [2017] SASCFC 130 per Kourakis CJ, at [139].

69 Cf *Bunt v Tilley* [2006] EWHC 407 (QB), in which proceedings against internet service providers were struck out on the basis that they were not publishers.

70 See obiter per Kourakis CJ, *Google Inc v Duffy* [2017] SASCFC 130, at [121]; [139]-[140] supporting the approach taken in *Bunt v Tilley*.

Search engines

3.73 A series of Australian cases, including the High Court case of *Trkulja*,[71] have confirmed that search engines can be liable as publishers. However, uncertainty still remains regarding the basis on which search engines might be liable for third-party content.72 The cases have established that a search engine can be a publisher of extracts of material ('snippets') reproduced from hyperlinked sites shown in the search results, and from auto-complete suggestions generated by the search engine algorithm in response to the partial input of search terms by users.[73] In some circumstances, the search engine may also be deemed to be liable for publication by displaying a hyperlinked site containing defamatory imputations in search results.[74]

Social media platforms

3.74 It is currently unclear whether a social media platform is considered a publisher under Australian defamation law.[75] There have not been any recent cases in Australia which directly address the liability of a social media platform for defamatory content hosted on its platform.

Forum administrators

3.75 Several cases have found forum administrators to be publishers of third-party content they administer.[76] For example, the NSW Court of Appeal in *Voller*[77] recently affirmed that media defendants operating Facebook pages were publishers of third-party comments in response to news stories they posted there.

---

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

72 Cf *Google LLC v Duffy* [2017] SASCFC 130; *Trkulja v Google LLC* (No 5) [2012] VSC 533; *Defteros v Google LLC* [2020] VSC 21; and *Bleyer v Google Inc* [2014] NSWDC 897 at [78], [83].

73 *Google LLC v Duffy* [2017] SASCFC 130; *Trkulja v Google LLC* [2018] HCA 25; *Defteros v Google LLC* [2020] VSC 219. Cf *Bleyer v Google Inc* [2014] NSWDC 897 at [83].

74 *Google LLC v Duffy* [2017] SASCFC 130; *Defteros v Google LLC* [2020] VSC 219.

75 For example, in *Kocwa v Twitter Inc* [2020] QDC 252, the court summarily dismissed proceedings commenced against Twitter. Twitter did not appear in the proceedings and claimed it was not liable for the cause of action. In *Voller v Nationwide News Pty Ltd* [2019] NSWSC 766, the defendants were hosts of Facebook pages, and Facebook itself was not a party to the proceedings so the courts only indirectly considered liability of digital platforms.

76 See e.g. *Voller v Nationwide News Pty Ltd* [2019] NSWSC 766; *Aldridge v Johnston* [2020] SAFC 31.

77 *Fairfax Media Publications Pty Ltd v Voller* [2020] NSWCA 102. The High Court has granted special leave to appeal this finding: *Fairfax Media Publications Pty Ltd v Voller* [2020] HCATrans 214.

Application

3.76 This option will apply as it currently does to all internet intermediaries, meaning, subject to any defences being available and the facts of an individual case, an internet intermediary can be found to be the publisher of third-party content published using their services.

3.77 As discussed above, some intermediaries are considered to be mere conduits in the publication, and therefore have not attracted liability for defamation made by third parties using their services in Australia. However, increasingly in recent cases, there have been circumstances where digital platforms have been found to be liable for publications made by third parties using their services.[78]

3.78 There may be issues with the current concerns notice/offer to make amends process and many of the statutory defences which are designed with traditional publishers in mind. This could mean that, if internet intermediaries are found liable for third-party content, they have diminished opportunity to resolve disputes before proceedings are commenced and limited defences available.

Assessment

3.79 The DWP recognises that one of the impetuses for the Stage 2 review is that the current state of defamation law in relation to internet intermediaries is unclear and inconsistent. The complexity of the issues at hand is the reason why this was separated out into a separate reform process. Common law precedents are developing across the various Australian jurisdictions, but are in a current state where each relies on the very specific facts of its own case in order to determine if an intermediary is or is not a publisher, providing little certainty to internet intermediaries and online users. Legislation has the benefit of being able to be drafted from a broader perspective and can take a more holistic approach to development of law than the courts, which are limited to rulings related to specific facts of each case.

3.80 The DWP also recognises that, in the 2019 Discussion Paper, stakeholders were asked if reforms were needed in relation to the treatment of internet intermediaries in the MDPs.[79] The views put forward to the DWP at this time continue to be relevant and will be considered as part of the Stage 2 review process.

3.81 The benefit of retaining the status quo is that it does not interfere with the evolving jurisprudence Australia courts are developing in relation to how internet intermediaries should be treated in relation to publication under defamation law. Reliance on common law also allows defamation law to remain flexible and adapt as technological changes affect the role internet intermediaries play in publication.

---

78 For example, in *Defteros v Google LLC* [2020] VSC 219 Google was found liable for displaying a Wikipedia article link that the complainant successfully argued was defamatory.

79 Refer to Question 15 of the 2019 Discussion Paper, see: https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/Final-CAG-Defamation-Discussion-Paper-Feb-2019.pdf.

Question 5: Treatment of internet intermediaries as publishers of third-party content

(a) Should internet intermediaries be treated the same as any other publisher for third-party content under defamation law?

(b) If yes, is this possible under the current MDPs, or are amendments necessary, in order to ensure they are treated the same as traditional publishers for third-party content?

Option 1b: Immunity for 'basic internet services' from defamation liability

3.82 In the development of defamation doctrine over the last century, it has been argued that certain traditional intermediaries are so passive in the facilitation of publication, that they do not themselves attract liability. For example, telephone lines and postal services have been considered too remote from publication to be considered liable.[80] They are described as 'mere conduits'.

3.83 Based on the 'mere conduit' analogy with analogue world telephone companies and postal services, and on case law elsewhere,[81] 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,[82] there is no binding higher court authority on this point in Australia, and the issue would, as always, turn on the evidence of how the ISP is operating, and the level of participation and control it exhibited over the matter in question.

3.84 This raises several questions. The first is whether any statutory protection for ISPs from liability in defamation for third-party content is required in Australia. It could be argued that this is simply not necessary, given that they are effectively immune from defamation liability as they are unlikely to be considered publishers. On the other hand, it may be appropriate to provide ISPs with statutory immunity for the publication of third-party content in order to provide more certainty. If statutory immunity were provided to ISPs, the second question is whether this should also be extended to other **basic internet services**.

3.85 The policy rationale for providing statutory immunity to ISPs and other **basic internet services** 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.

80 Eady J's analysis in *Bunt v Tilley* [2006] EWHC 407 (QB).

81 *Bunt v Tilley* [2006] EWHC 407 (QB).

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

Application

3.86 The purpose of Question 2 of this Discussion Paper is to understand what internet intermediary functions should be considered **basic internet services** on the basis that they are mere conduits that do not have an interest or involvement in the nature of the content they transmit or host.

3.87 Stakeholder feedback on Question 2 will assist the DWP to consider the scope of application for any potential statutory immunity.

3.88 An important consideration in terms of the framing of a potential immunity is whether a principles-based approach or a functions-based approach would be more appropriate. A principles-based approach might focus on the concepts of passivity and neutrality as suggested in Question 2. Alternatively, specific functions such as ISPs could be prescribed as attracting immunity. While a principles-based approach would provide more flexibility, this may place a burden on the courts to examine the functions of internet intermediaries to determine if they meet the test. This could result in different and unpredictable outcomes, thus not achieving the intended policy outcome of providing greater certainty of the extent of liability in publication for internet intermediaries. A function specific approach would offer more certainty, but it would be less capable of responding to new and emerging technologies.

Assessment

3.89 The benefit of providing a statutory immunity is that there would be certainty for **basic internet services** that they are not at risk of being sued for defamation in relation to third-party content. It would also provide certainty to complainants regarding which internet intermediaries they can and cannot approach for a remedy. This would do away with the need for defamation proceedings in order for a court to determine if a basic internet service is a publisher of the third-party content in question. If such proceedings were commenced, they would likely be summarily dismissed if the internet intermediary can demonstrate that it falls into the category of a **basic internet service**.

3.90 The counterargument to this is that statutory immunity would take **basic internet services** out of the picture altogether regarding liability in defamation for third-party content. The immunity would apply irrespective of whether the intermediary is made aware of the allegedly defamatory content. This is different to the approach in the BSA, which provides an immunity to ISPs and internet content hosts only up until the point they are aware of the nature of the content. The justification for this, based on existing principles of defamation law, would be that their participation in the publication is too passive to attract liability. However, given the breadth of the protection, there must be a high threshold for its application.

3.91 This immunity would assist in ensuring that freedom of expression is not unduly limited, as there would be no need for relevant intermediaries to remove content in order to avoid liability. However, it would narrow the field of defendants for a complainant, meaning it could undermine their ability to protect their reputation and achieve speedy and non-litigious outcomes. It would provide more legal certainty to internet intermediaries, promoting a healthy digital economy. Arguably it would not change the current legal position but instead provide more legal certainty for those internet intermediaries that are already unlikely to be considered publishers.

Question 6: Immunity for basic internet services

(a) Is it necessary and appropriate to provide immunity from liability in defamation to basic internet services?

(b) If such an immunity were to be introduced, should it be principles-based or should it specifically refer to the functions of basic internet services?

(c) Are there any internet intermediary functions that are likely to fall within the definition of basic internet services (as outlines in **Issue 1**) that should not have immunity?

(d) Is there a risk that providing a broad immunity to basic internet services would unfairly deny complainants a remedy for damage to their reputation? What risks exist and how could they be mitigated?

Option 1c: Amend Part 3 of the MDPs to better accommodate complaints to internet intermediaries.

3.92 One of the objects of the MDPs is to promote speedy and non-litigious methods of dispute resolution.

3.93 Part 3 of the MDPs establishes a procedure to enable parties to settle disputes without the need for expensive litigation, by encouraging publishers to make a reasonable 'offer to make amends' to the complainant (the 'aggrieved person'). If the complainant does not accept an offer that was reasonable in all the circumstances, the publisher may establish a defence in any subsequent defamation action. Recent amendments to the MDPs mean that proceedings generally cannot be commenced unless a valid concerns notice is issued.[83]

[83] Clause 12B, MDPs. Note that the courts can dispense of this requirement in exceptional circumstances (clause 12A(3)).

3.94 Under the MDPs, a valid concerns notice must: be in writing, specify the location where the matter in question can be accessed, inform the publisher of the defamatory imputations of concern and inform the publisher of the serious harm to their reputation they consider the matter to have caused or be likely to cause.[84] The publisher is then given a period of not less than 28 days during which it may make a reasonable offer to make amends which must be in writing and must include:[85]

- an offer to publish, or join in publishing, a reasonable correction of, or a clarification of or additional information about, the matter in question, and
- if the alleged defamatory material 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, and
- an offer to cover expenses reasonably incurred by the complainant before the offer was made and in considering the offer.

3.95 The offer to make amends *may* also include:[86]

- an offer to publish an apology, or
- if the matter has been published on a website or any other electronically accessible location, an offer to remove it, or
- an offer to pay compensation, or
- the particulars of any correction or apology made, or action taken, before the date of the offer.

3.96 Part 3 of the MDPs applies equally to online and offline publications. The amendments to the MDPs, including the requirement to issue a concerns notice, have not come into force at the time of writing, but, once commenced, will have an important role to play in relation to dispute resolution concerning digital publications. The amendments include specific changes to better apply the process to online publications, for example, the requirement to specify the location from which a matter can be accessed (for example, a webpage address)[87] and the option to include an offer to remove the matter from the website or location if it is published online.[88]

3.97 The mandatory concerns notice process in Part 3 of the MDPs is designed to incentivise parties to resolve a defamation dispute before the dispute ends up in court. The process requires the complainant to put the publisher on notice of the alleged defamatory matter, and the publisher is given time to make a reasonable offer to make amends.

---

84 Clause 12A, MDPs.

85 Clause 15(1), MDPs.

86 Clause 15(1A), MDPs.

87 Clause 12A(1)(a)(ii), MDPs.

88 Clause 15(1A)(b), MDPs.

3.98 The mandatory concerns notice and option to make an offer to make amends was designed with traditional publishers in mind, and thus the timeframes for remedies and filing for court may not be compatible with the pace at which information is distributed online, and the ease at which corrections can be made. If internet intermediaries continue to be treated the same as other publishers, there may be an opportunity to amend the current concerns notice and/or offer to make amends process to better suit complaints of online defamation made to internet intermediaries.

Application

3.99 This option could be implemented by amending the current concerns notice and/or offer to make amends process to better apply to internet intermediaries.

3.100 Currently, the process under Part 3 of the MDPs is not designed with a complaint about third-party defamatory content published using an internet intermediary in mind. An internet intermediary may not be able to resolve the complaint per the mandatory requirements of a reasonable offer to make amends. 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"[89] for a search result that was complained of as being defamatory. As offers to make amends are not mandatory, the consequence of not being able to acquit the requirements of an offer to make amends is that a search engine would not have the defence of a reasonable offer to make amends available to them in the event they were subject to defamation proceedings for third-party content.

3.101 Inserting alternative mechanisms into the offer to make amends process to better apply to internet intermediaries being complained to about third-party content could help address the potential shortfalls of the current process when it comes to complaints of third-party content.

3.102 Alternatively, a discrete concerns notice and offer to make amends process could be developed specifically for internet intermediaries.

Assessment

3.103 There is a possibility that this option could be progressed alongside the introduction of a dedicated complaints notice process as set out in **Issue 3**. Further discussion on how a complaints notice process might interact with the existing concerns notice/offer to make amends process is set out in **Issue 3**, but this is an important consideration.

3.104 In the event this option is progressed without a complaints notice process also being introduced then it could be an effective mechanism for allowing complainants to better resolve disputes in a speedy and non-litigious manner while making minimal changes to the status quo.

3.105 Consideration also needs to be given to what are the most appropriate remedies for complainants who have been defamed by third parties online. For example, complainants may be seeking to have content removed or de-indexed in the first instance.

---

89 A mandatory requirement of an offer to make amends under clause 15(1)(d), MDPs.

3.106 However, a separate dedicated process just for complaints to internet intermediaries could lead to complexities where the role of the internet intermediary is unclear and so careful consideration will need be given to when and how a separate process will apply.

Question 7: Amend Part 3 of the MDPs to better accommodate complaints to internet intermediaries.

(a) How can the concerns notice and offer to make amends process be better adapted to respond to internet intermediary liability for the publication of third-party content?

(b) What are the barriers in the concerns notice and offer to make amends process contained in Part 3 of the MDPs (as amended) that prevent complainants from finding resolutions with internet intermediaries when they have been defamed by a third-party using their service?

(c) In the event the offer to make amends process is to be amended, what are the appropriate remedies internet intermediaries can offer to complainants when they have been defamed by third parties online?

Option 2: Clarify the innocent dissemination defence in relation to digital platforms and forum administrators

3.107 Clause 32 of the MDPs provides a defence of innocent dissemination, which protects a 'subordinate distributor' from liability.

3.108 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.

3.109 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. It also includes 'an operator of, or a provider of access to, a communications system by means of which the matter is transmitted, or made available, by another person over whom the operator or provider has no effective control'.[90]

3.110 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)).

[90] Clause 32(3), MDPs.

3.111 This means that once a subordinate distributor is on notice of the defamatory matter, it risks losing the benefit of the innocent dissemination defence.

3.112 The application of the innocent dissemination defence to internet intermediaries that are found to be publishers is a developing area. Recent cases suggest that search engines and digital platforms found to have published defamatory material in search results are *prima facie* eligible for a clause 32 defence where they can establish that they are subordinate distributors. This is so long as they delist or take down the third-party defamatory material expeditiously, or within a 'reasonable time', after being fixed with knowledge of the defamatory content of such material (for example, after receiving a defamation complaint).[91] However, again, this is subject to the evidence in each case. The position of forum administrators in relation to this defence is uncertain given the recent and ongoing *Voller* litigation affirming that forum administrators can be deemed publishers of third-party comments posted in that forum.[92]

3.113 A further area of uncertainty in this context is the issue of what will constitute knowledge, or constructive knowledge, of the defamatory content. The defendant has the burden of proving that it did not know, nor ought reasonably to have known, that the content was defamatory and that its lack of knowledge was not due to negligence. The constructive knowledge element of this test introduces judicial considerations of negligence in the context of the intermediary's role in the publication.[93]

3.114 Some recent decisions on the liability of search engines have adopted a strict liability test in relation to the issue of constructive knowledge of third-party content published in search results, holding the defendant to be on notice of the defamatory nature of the content as soon as it is made aware of its presence by the plaintiff.[94] However, uncertainty remains as to what will constitute constructive knowledge of defamatory third-party content to an internet intermediary in different factual scenarios.[95]

---

91 See e.g. *Defteros v Google LLC* [2020] VSC 219.

92 Voller v Nationwide News [2019] NSWSC 766; *Fairfax Media Publications v Voller* [2020] NSWCA 102.

93 Cf *Google LLC v Duffy* [2017] SASCFC 130 per Kourakis CJ at [98].

94 *Google LLC v Duffy* [2017] SASCFC 130 per Kourakis CJ at [98], Peer and Hinton JJA agreeing; followed by Richards J in *Defteros v Google LLC* [2020] VSC 219.

95 Cf Basten JA, *Fairfax Media Publications Pty Ltd v Voller* [2020] NSWCA 102 at [41].

Current issues

3.115 Stakeholders have submitted that the clause 32 defence as currently drafted does not provide enough protection for internet intermediaries. The key issues raised are:

- It is unclear which types of internet intermediaries would be considered 'subordinate distributors' given that some may be considered to have the technical capacity to exercise editorial control (for example, those that host or cache content – and even ISPs).
- 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.

Potential changes

Alternative A

3.116 One option is to amend the innocent dissemination defence in clause 32 of the MDPs to create a default position that digital platforms and forum administrators are not primary distributors. This change would still require digital platforms and forum administrators to satisfy the other limbs of the innocent dissemination defence, but would clarify the position regarding their involvement in the publication.

3.117 Alternative A could be implemented by inserting an additional paragraph adding 'digital platforms' and 'forum administrators' (or appropriate definitions encompassing these entities as defined in this Discussion Paper) into sub-clause 32(3) of the MDPs.

Alternative B

3.118 Alternatively, a standalone subsection could be added to clause 32, or a separate new standalone innocent dissemination defence introduced, which applies a presumption that a digital platform or forum administrator is a subordinate distributor, without reference to the general test in subclause 32(1). The presumption could be rebuttable in certain circumstances. For example, the presumption could be rebuttable if the complainant shows that the digital platform or forum administrator acted so as to adopt, curate or promote content published by another. This standalone defence could also specify what constitutes notice in order to clarify when the defence applies.

Application

3.119 This option would give immunity from defamation claims to digital platforms such as social media platforms and search engines, and to forum administrators, in respect of third-party content they host or index, provided that they act expeditiously to remove material complained of, and have not engaged in conduct which rebuts the presumption of immunity.

3.120 The defence could detail what constitutes notice and engagement with the content for the purposes of liability of the digital platform or forum administrator.

Assessment

3.121 The advantage of this option is that it provides a default position that a digital platform or forum administrator will be entitled to an innocent dissemination defence. This would provide greater certainty for digital platforms and forum administrators that if they remove or delist defamatory content expeditiously after receiving a complaint, they will generally have the benefit of this defence. Arguably, this reflects the position of these intermediaries in the chain of publication, providing them with immunity where they have acted expeditiously once on notice, and have not engaged in conduct which would rebut the presumption of immunity. Another advantage is that it could clarify what notice requirements exist for internet intermediaries, therefore encouraging particular behaviours from internet intermediaries in order to benefit from the defence.

3.122 The disadvantage of this option is that if a complainant wishes to challenge the default immunity of a digital platform or forum administrator, it will have the evidentiary burden of proving that the presumption of immunity should be rebutted. Where a complainant does not have resources to bring such evidence to trial (and the matter was removed expeditiously so that the defence is otherwise made out), the complainant will not have a remedy in defamation against the digital platform or forum administrator. This will be so irrespective of whether or not the originator can be identified and sued. On the other hand, where a complainant does wish to challenge the application of the defence, this will still require the testing of evidence on the facts of the case.

3.123 Another disadvantage of this approach is that there would be a strong incentive for the digital platform or forum administrator to simply remove or delist content from the point of notification to avoid potential liability. Such removal may not be aligned with the wishes of the originator, or in the case of removal by the digital platform, the forum administrator.

3.124 If the digital platform or forum administrator is not the originator of the content, they may not be a position to judge the merits of the claim. This may lead to abuse by complainants who are seeking to censor public interest discussion about their activities. For example, any complainant who wished for a negative review on a review website to be removed could lodge a defamation claim against the intermediary, in the knowledge that the intermediary would be incentivised to remove the material to avoid liability (regardless of the accuracy of the review).

3.125 The wording of the amended defence as it applies to digital platforms and forum administrators would have to be carefully considered to determine what conduct or circumstances would rebut any presumption of immunity. If too vaguely framed, this may lead to uncertainty while the courts determine the scope of the immunity. If too specific, however, the immunity may quickly be superseded by new developments online.

3.126 This alternative also would not provide any greater clarity on how the defence would apply once a person is notified of the allegedly defamatory content, and in particular, what would constitute notice or a reasonable time for removal of defamatory matter.

Question 8: Clarifying the innocent dissemination defence

(a) Should the innocent dissemination defence in clause 32 of the MDPs be amended to provide that digital platforms and forum administrators are, by default, secondary distributors, for example by using a rebuttable presumption that they are?

(b) In what circumstances would it be appropriate to rebut this default position?

(c) Should a new standalone innocent dissemination defence specifically tailored to internet intermediaries be adopted the MDPs?

(d) If a standalone defence is created, should the question of what is knowledge or constructive knowledge of third-party defamatory content published by an internet intermediary be clarified? If so, how?

(e) Are there other ways in which the defence of innocent dissemination could be clarified?

Option 3: Safe harbour – subject to a complaints notice process

3.127 Section 5 of the *Defamation Act 2013* (UK), 'Operators of websites', created a new defence to an action for defamation brought against the operator of a website hosting user-generated content where these operators comply with a prescribed process for addressing complaints of defamatory content on their websites.

3.128 The defence means that, where the operator of a website can show that it did not post the defamatory material, it has a complete defence to a claim. However, the defence is defeated if:

- it was not possible for the claimant to identify the person who posted the defamatory material; and
- the claimant gave the website operator a 'notice of complaint' in relation to the defamatory material; and
- the website operator failed to respond to the 'notice of complaint' in accordance with procedure set out in the regulations.

3.129 The effect of the defence under section 5 means the website operator who has not posted the defamatory statement themselves has the benefit of a defence when:

- a complainant has sufficient information about the identity of the poster of the defamatory material to commence proceedings against them directly, or
- the complainant cannot identify the originator, but has not issued a notice of complaint, or
- the complainant cannot identify the originator, has issued a notice of complaint, and the website operator complies with the process required by section 5, irrespective of the outcome of this process.

3.130 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.

3.131 In Australia, a similar defence could be introduced with an accompanying complaints notice process. A possible complaints notice process is outlined in further detail below in **Issue 3: complaints notice process**. A key issue is to what internet intermediary functions the defence (and by extension, the complaints notice process) would apply.

Application

3.132 In the UK, the defence applies to website operators. The term 'website operator' is not defined in the *Defamation Act 2013* (UK), but a UK Ministry of Justice guidance document[96] notes that it covers websites hosting user-generated content, and does not affect other internet services such as search engines, services that simply transmit information or services that provide access to a communications network.

3.133 The LCO, in its final report, *Defamation Law in the Internet Age*, proposes a new complaints notice regime for defamation. It would apply to 'intermediary platforms' given their 'direct hosting relationship with the users posting content to the platform'.[97] The LCO identified this as including 'social media sites, discussion forums, online review sites, blogging platforms, gaming sites, and any website that permits user comments'.[98] Notably, it does not include search engines.

3.134 In Australia, a broader range of internet intermediaries have been found to be publishers of third-party content than in the UK. In the UK, courts have found that search engines are not considered publishers in relation to automatically generated snippets in search results.[99] In Australia, on the other hand, the High Court of Australia (**High Court**) has found that a search engines can be considered publishers of search results.[100]

3.135 Also, in the recent case of *Voller*[101] the New South Wales Court of Appeal upheld the trial judge's pre-trial finding that media defendants that hosted public Facebook 'pages' were publishers of user comments posted on those pages.

3.136 In considering whether the UK section 5 defence could be adopted in Australia, it is therefore important to determine the extent to which it would be viable and appropriate for different internet intermediaries.

3.137 The defence could apply to different digital platforms as follows.

---

96 UK Ministry of Justice (2014) 'Defamation Act 2013 – Guidance and FAQs on Section 5 Regulations', see: https://www.gov.uk/government/publications/defamation-act-2013-guidance-and-faqs-on-section-5-regulations.

97 LCO Final Report (n 28) 73, citing Jaani Riordan (n 1) chapter 2.

98 LCO Final Report (n 28) 73.

99 *Metropolitan International Schools Ltd v Designtechnica Corp* [2009] EWHC 1765.

100 *Trkulja v Google LLC* [2018] HCA 25. See also Google *LLC v Duffy* [2017] SASCFC 130; *Defteros v Google LLC* [2020] VSC 219.

101 *Fairfax Media Publications Pty Ltd v Voller* [2020] NSWCC 102.

Social media services

3.138 Most social media services function by connecting users individually, in groups, or by sharing the content created by users. These services often require a person or organisation to create an account in order to be able to post content on their platforms. This means that the contact details of the account holder could be held privately by these services. These services (subject to privacy and contractual considerations) could be in a good position to connect the complainant and the originator, or to pass on the complaint to the originator.[102]

Search engines

3.139 Unlike social media services, search engines may not be in a position to act as intermediary between the complainant and the originator. This is because the nature of their service generally does not involve the originator being required to provide the search engine with their contact details (for example, as part of creating an account). Therefore, it may be that in order to receive the benefit of such a defence, the requirements of search engines may need to rely on de-listing content rather than contacting the originator.

Digital content aggregators

3.140 Digital content aggregators do not produce their own content, and instead reproduce snippets or links to other content on the internet. While the content is curated, the originator of the content potentially has no link or relationship to the aggregator. Aggregators are unlikely to have access to the contact details of the originator. However, once on notice of a complaint of defamatory content on their platform, they would have the ability to delist or block access to that content.

Messaging services

3.141 Most online instant messaging services require users to have an account with the service. This means the service is likely to have access to the contact details of the users. The nature of messaging services means users generally have the contact details of other users they are in contact with, even though the contact details may be limited to that messaging service. Users may also be part of forums or groups that can function similarly to other online forums. The defence could apply to messaging services where they have the ability to connect the complainant with the originator.

102 LCO Final Report (n 28).

Forum administrators

3.142 Whether a forum administrator would be able to connect the originator and the complainant through a complaints notice procedure would vary depending on the circumstances of the case. If the forum administrator is the administrator of a public Facebook page, they are unlikely to have access to any more information about the originator of the defamatory matter than the complainant. The forum administrator is, however, likely to be in a position to remove the alleged defamatory content. In situations where the forum administrator does have additional information – for example, if they run an independent blog or host an independent website – they may be able to connect the originator and the complainant. The defence could apply to forum administrators where they have the ability to connect the complaint with the originator.

Assessment

3.143 Where online content can be easily and quickly copied, reposted, repeated or republished, it is often paramount to the complainant that the defamatory material be dealt with as quickly as possible. This defence has the potential to provide a fast and simple path for the complainant achieve a solution when their reputation has been harmed online – particularly where their primary goal is to have the content modified or removed.

3.144 As discussed already in this Discussion Paper, any internet intermediary that is an ISP or an 'internet content host' would have protection under the BSA immunity until they are on notice regarding the offending content. The complaints notice process is in effect putting the intermediary on notice, removing their protection unless they then follow the complaints notice process. There is also a question in relation to whether the BSA immunity would impact on the operation of any complaints notice process available as a defence to the extent that it "requires" the intermediary to monitor, make inquiries about or keep records in relation to content it hosts, in order to qualify for the defence. The extent to which the defence and complaints notice process is effective would likely depend on how straightforward and cost effective it is to use. Some commentary on the section 5 UK defence and complaints notice procedure states that it is quite complicated and onerous for website operators.[103] Publishers of user-generated content may prefer to remove content once a complaints notice is received, rather than follow the requirements set out in the complaints notice process. Arguably this would be a sufficient outcome for many complainants without the need to resort to litigation, but it may have a chilling effect on freedom of expression.

---

103 For example, as noted in the Scottish Parliament Policy Memorandum for the Defamation and Malicious Publication (Scotland) Bill, see: https://beta.parliament.scot/-/media/files/legislation/bills/current-bills/defamation-and-malicious-publication-scotland-bill/introduced/policy-memorandum-defamation-and-malicious-publication-scotland-bill.pdf, p 24.

3.145 The purpose of a defence where there is compliance with a complaints notice process would be to encourage digital platforms be part of the resolution for complainants, in exchange for protection from liability. Where a complaints notice can lead to connecting the complainant with the originator, then it will enable the complainant to either seek to have the content removed or clarified by the originator, or to issue a concerns notice in order to progress a resolution under the MDPs, which may result in proceedings. This focuses the liability back on the originators of the defamatory content, and the protection given to the intermediaries is in recognition of their assistance in permitting the complainant to deal with the originator directly.

Whether the defence should only apply where the originator cannot be identified is also an element worth considering. The UK defence protects website operators where the originator is able to be identified, even if they are recalcitrant. This means that complainants may not have access to an outcome from the complaints notice process where the originator is identifiable but unwilling to cooperate.

3.146 By providing a defence where the digital platform provides recourse for complainants, this approach acknowledges that these platforms have some responsibility for content posted on their platforms. It might also prompt some digital platforms to adjust their business models to provide more venues of recourse for users who allege they have been defamed on their platforms. However, this responsibility can be discharged when addressed through alternative dispute resolution mechanisms.

Question 9: Safe harbour subject to a complaints notice process

(a) Should a defence similar to section 5 of the *Defamation Act 2013* (UK) be included in the MDPs?

(b) If so, should it be available at a preliminary stage in proceedings, where an internet intermediary can establish they have complied with the process?

(c) Should a complaints notice process be available when an originator can be identified? For example, to provide for content to be removed where the originator is recalcitrant?

(d) If such a defence were introduced, would there still be a need to strengthen the innocent dissemination defence?

(e) Should the defence be available to all internet intermediaries that have liability for publication in defamation? For example, could a separate complaints notice process be developed that could apply to search engines?

(f) How can the objects of freedom of expression and the protection of reputations be balanced if such a defence is to be introduced?

Option 4: Immunity for internet intermediaries for user-generated content unless the internet intermediary materially contributes to the unlawfulness of the publication (the USA approach)

3.147 Immunity could be given to internet intermediaries for third-party content – even if they are notified about it – unless they have materially contributed to the unlawfulness of the publication.

3.148 The immunity could be based on section 230 of the *Communications Decency Act 1996* (US) (**CDA**), which provides that 'no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'.[104]

3.149 It provides immunity (subject to some limitations) to interactive computer services for the publication of third-party content and protection for moderating and blocking offensive material.[105]

3.150 In order to be immune from liability, a defendant must satisfy a three-pronged test:

(a) The defendant must be a 'provider or user of an interactive computer service';

(b) The cause of action must view the defendant as the publisher or speaker of the harmful information at issue; and

(c) The information must be provided by *another* information content provider that is not the defendant.[106]

3.151 'Interactive computer service' is defined broadly and includes, for example, website operators.[107]

3.152 There have been a small number of cases where courts have found that a 'provider or user of an interactive computer service' loses the benefit of section 230 if it 'materially contribut[ed] to its alleged unlawfulness'.[108] These tend to be in cases where the website carries out a variety of functions beyond being just an intermediary. In these cases, the courts are largely guided by the material contribution test articulated in *Fair Housing Council of San Fernando Valley v Roommates. com LLC*[109] where the court held that an intermediary loses the section 230 immunity if it develops the unlawful content, 'referring not merely to augmenting the content generally, but to materially contributing to its alleged unlawfulness.'[110] In this case, the Fair Housing Council argued that Roommates.com was actively

---

104 Section 230(c)(1) of the *Communications Decency Act 1996* (US) (Protection for private blocking and screening of offensive material).

105 Section 230 (c)(2) *Communications Decency Act 1996* (US).

106 Ardia, D, 'Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act', (2010), 43 Loy LA L Rev 373, p 412.

107 Ardia (n 106) 379.

108 Laidlaw & Young (n 22) 132.

109 *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Circuit, 2008)

110 Laidlaw & Young (n 22) 131.

participating in unlawful conduct by requiring users to provide details of their age, gender, sexual orientation and other factors that they could then be filtered by, which could lead to them being unlawfully discriminated against by other users, therefore breaching anti-discrimination laws. By actively inducing third parties to express illegal preferences, the Council argued the CDA immunity would not apply.

3.153 The court used several analogies to test the limits of the immunity under the CDA, which are helpful to outline how a similar immunity would work in Australia. These included:[111]

- An individual using an ordinary search engine to search for a 'white roommate'. Here, the search engine has not contributed to any alleged unlawfulness in the individual's conduct by providing neutral tools to carry out what may be unlawful or illicit searches. It does not amount to 'development' for purposes of the immunity exception.
- A dating website that requires users to enter details on their sex, race, religion and marital status, and that provides means for users to search based on these criteria will receive immunity insofar as it does not itself contribute to any alleged illegality.
- A housing website that allows users to specify whether they will or will not receive inquiries from other users based on user-defined criteria that allows users to exclude other users based on race or sex, would be immune, so long as it does not *require* the use of discriminatory criteria.

3.154 In summary, the court noted that, 'requiring website owners to refrain from taking affirmative acts that are unlawful does not strike us as an undue burden. These are, after all, businesses that are being held responsible only for their own conduct; **there is no vicarious liability for the misconduct of their customers**'[112] [our emphasis added]. Therefore, it appears the scope of the immunity under section 230 will protect internet intermediaries from liability for illegal activities carried out on their platforms, so long as the design of their services does not require users to do something unlawful, and they don't actively encourage users to do something unlawful.

Application

3.155 Section 230 applies broadly to all providers and users of interactive computer services, so if a similar approach is adopted in Australia, it would encompass all internet intermediaries, including the digital platforms outlined in the **Categorising internet intermediaries** section of this Discussion Paper. It would prevent anyone bringing a claim in defamation (or result in a claim being summarily dismissed) against an internet intermediary unless they could provide evidence that the intermediary had materially contributed to the publication.

---

111 *Fair Housing Council of San Fernando Valley v. Roommates.com LLC*, 521 F 3d 1157.

112 *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F 3d 1157, at footnote 24.

3.156 Digital platforms like social media platforms have greatly benefitted from the immunity given by section 230 in the US. This wide immunity has meant that social media platforms are not concerned that actively moderating content to ensure harmful content is removed – or being good Samaritans - will lead to liability arising from the interference with the content. They would gain the benefit of this immunity unless they were found to be requiring defamatory comment through the design of their platform, or deliberately eliciting defamatory comments from users.

3.157 A section 230-style immunity, if based on the definition of user or provider of interactive computer services, would likely also capture forum administrators, so long as they are not deliberately eliciting defamatory comments from users. Again, this would encourage forum administrators to moderate content free from fear of liability.

3.158 If the complainant alleges that they have been defamed online, generally they would only be able to pursue the originator of the defamatory statement. For example, if the complaint was regarding:

- A user of a social media platform posting a defamatory comment, then the immunity would cover the social media platform, meaning the complainant may only sue the user who posted the comment.
- An article that was published including defamatory imputations that came up in search engine results (for example, a hyperlink and a snippet), then the search engine would have immunity, and the complainant would need to instead contact the originator or owner of the website where the article was originally published to identify the originator.
- An unsolicited, third-party comment made on a public Facebook page, the administrator of that page would have immunity and the complainant would need to direct their complaint to the person who posted the comment.

3.159 If the originator cannot be identified or refuses to remove the content, then the complainant would have no access to a remedy from the internet intermediary, unless they successfully obtain a court order to identify the originator or have the content removed. This would require significant resources from the complainant.

Assessment

3.160 The argument in favour of this option is that it recognises that internet intermediaries are not the creators of content and should not be held responsible in place of the originator. The immunity given under section 230 of the CDA was designed to ensure internet intermediaries were not deterred from moderating harmful or illegal content on their websites.[113]

[113] Wakabayashi, D, see: https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html.

3.161 Adopting a provision similar to section 230 of the CDA may also be seen as removing a barrier to innovation online. The broad immunity given to internet intermediaries in the US has been credited with enabling the proliferation and financial success of internet companies in the US, as they have certainty of their liability, and are not penalised for actively moderating the content they host on their websites.[114]

3.162 A clear disadvantage is that if it is not possible to pursue a remedy against the originator, the complainant is denied recourse to redress unless they can secure a court order identifying the originator.

3.163 This wide immunity also would be at odds with the approach to traditional secondary publishers such as booksellers, newsagents and librarians. The immunity is also ill-equipped to respond to the varying functions of internet intermediaries due to its 'one size fits all' approach.

3.164 Granting a broad immunity also fails to recognise that many internet intermediaries have the ability to encourage, but also mitigate, the risk of harm to reputation online. Often, their business models, which leverage the network effect to attract users to their platforms for longer periods of time, can lead to heightened risk of harm to reputations, while generating profits for these platforms in doing so. Arguably, this should attract a level of responsibility which this option would fail to deliver.

Question 10: Immunity for internet intermediaries unless they materially contribute to the unlawfulness of the publication

(a) Should a blanket immunity be provided to all digital platforms for third-party content – even if they are notified about it, unless they materially contribute to the publication?

(b) What threshold or definition could be used to indicate when an intermediary materially contributes to the publication of third-party content?

(c) If a blanket immunity is given as described above, are there any additional or novel ways to attract responsibility from internet intermediaries?

114 Ibid.

ISSUE 3: Complaints notice process

Providing a complaints notice process with a safe harbour

3.165 **Option 3** in Issue 2 above presents a safe harbour defence based on section 5 of the *Defamation Act 2013* (UK), which creates a defence to an action for defamation brought against the operator of a website that did not post the defamatory material, provided a complaints notice process is followed.

3.166 This section seeks to investigate how a complaints notice process might work in the Australian context.

Stakeholder feedback on a complaints notice process

3.167 In response to Question 15 of the Discussion Paper released in February 2019, stakeholders told the DWP that a clear procedure is needed in Australia to enable internet intermediaries to respond to requests from complainants to remove, or block access to, content which is alleged to be defamatory.

3.168 Digital stakeholders noted that it is very difficult for an internet intermediary to judge, on the basis of very limited evidence from the complainant, whether or not material is defamatory. The following challenges also exist:

- whether any defences may apply to the publication of the material (such as contextual truth or justification, for example) and it should therefore not be taken down or blocked;
- whether it is justified to 'take down' or 'block' the content when there is the potential for non-defamatory content to be captured in the removal or blocking of defamatory matter, for example where a whole article or website may be removed or blocked where one phrase is defamatory;
- the potential for prompt duplication and republication of defamatory matter in a digital context.

How a complaints notice process could work in Australia

3.169 Under the amended MDPs, proceedings cannot be commenced unless the complainant has issued a concerns notice and sufficient time is allowed for the publisher to make an offer to make amends.[115] The purpose of this process is to encourage dispute resolution without the need for litigation.

3.170 However, there are circumstances where a complainant may not be able to identify the originator of content online, or where the originator is recalcitrant. Additionally, the complainant may simply wish to have the defamatory content removed, rather than seeking to file a claim for damages in defamation. For these reasons, there may be a role for a complaints notice process specifically designed for online publications.

---

115 Clause 12B, MDPs.

3.171 Unlike in the UK, Australian courts have found a wider subset of internet intermediaries to be publishers of third-party content, including search engines and forum administrators. It is therefore important to consider whether a complaints notice process could apply flexibly to different types of intermediaries, who have different relationships with the content and the originators.

3.172 In this section, the DWP will:

- discuss the role of remedies beyond damages
- look at how the mandatory concerns notice and offer to make amends process might interact with a complaints notice process
- discuss the potential application of the complaints notice process
- outline what a complaints notice process could look like, by examining the UK approach as a model including:
    - what steps should be taken prior to issuing a complaints notice
    - complaints notice form and content
    - the process once a valid complaints notice is received.

Remedies

3.173 The traditional remedy in defamation is the award of damages for harm to reputation. If the publication is found to have indefensible defamatory imputations, the complainant will be awarded compensatory damages and possibly aggravated damages depending on the seriousness of the imputations and the behaviour of the originator. However, sometimes damages are not the most appropriate remedy for the complainant. The complainant may instead be seeking for the defamatory publication to be removed or delisted.

3.174 It is important to consider that the nature of an online publication can impact the type of remedy desired by a complainant. This Discussion Paper seeks to address the liability and responsibilities of internet intermediaries for matter posted on their platforms or services by third parties. Sometimes, when engaging with intermediaries, complainants are not necessarily seeking to claim damages, but rather are seeking assistance from intermediaries in removing the alleged defamatory content.

3.175 Under the MDPs, the mandatory concerns notice and offer to make amends process provides a non-litigious method of resolving disputes. There are a number of different ways a publisher can make a reasonable offer to make amends. According to the MDPs, an offer to make amends must include an offer to publish a correction and cover the reasonable costs of the complainant in issuing the concerns notice. The offer to make amends may also include, but is not limited to, an offer to publish an apology, an offer to remove the matter from a website, or an offer to pay compensation. This may be one means of satisfying a complainant who is not seeking an award of damages, provided the publisher is willing to make a reasonable offer.

3.176 A concerns notice can be issued to any publisher of the defamatory content, not just the originator. The concerns notice and offer to make amends process is intended to resolve a defamation dispute prior to trial, which could include content being taken down, blocked or de-listed. If the publisher refuses to remove the material, a complainant may have to seek an order from the court. However, as interim injunctions are not easily granted in defamation proceedings, a complainant may have to wait a considerable time to obtain a final decision and resolution from a court.

Interaction of mandatory concerns notice and complaints notice

3.177 Part 3 of the MDPs (concerns notice and offer to make amends process) generally assumes that a publisher is identifiable. It also provides for a process between a complainant and a publisher who has the ability to publish a correction or apology to the same audience. This may not necessarily be possible for an internet intermediary. The Part 3 process can lead to content being removed, but does not address the situation where the internet intermediary is not in sufficient control of the content to remove it from the internet, for example, where a search engine can only de-rank or de-index a search result, but cannot remove the offending content as it is hosted on another platform.

3.178 Some complainants may also be looking for faster recourse that does not involve a legal process or ultimately litigation. They may be looking for an avenue to have defamatory material easily removed, or to identify originators of the content. The Part 3 process does not necessarily provide this redress, so an alternative process may need to be established to better suit the internet intermediary context, and its relationship with the offending content.

Is the complaints notice process compatible with the concerns notice process in instances of online publication?

3.179 The mandatory concerns notice process in Part 3 of the MDPs distinguishes the pre-litigation process in Australia from the UK and may have implications for the effectiveness of a complaints notice process. Three scenarios of how the complaints notice might interact with the concerns notice are set out below:

1. One obvious problem with the Part 3 process is that a concerns notice may not be able to be issued in circumstances where the originator is unable to be identified. The complaints notice process could be used with an internet intermediary to identify originators for this purpose (noting that the internet intermediary is protected from liability if they comply with the complaints notice process per the defence raised in option 4). The complainant would then, once they have identified the originator, need to commence the concerns notice process under Part 3.
2. The complaints notice process between the complainant and the internet intermediary may provide a satisfactory resolution for the complainant, meaning a concerns notice does not need to be issued.

3. The complainant could commence the complaints notice process and the internet intermediary may not comply with the notice, meaning they open themselves up to liability. If the complainant wants to then sue the internet intermediary, they would then need to commence the Part 3 process, which could add further time and complexity to seeking a remedy.

Question 11: Complaints notice process for Australia

(a) Should a complaints notice be distinct from the mandatory concerns notice under Part 3 of the MDPs, or should the same notice be able to be used for both purposes?

(b) Are there any issues regarding compatibility between the mandatory concerns notice and a potential complaints notice process? Are there parts of either that might overlap or be superfluous if a mandatory concerns notice is already required?

(c) What mechanisms could be used to streamline the interaction between the two notice processes?

Application

Complainants

3.180 A complaints notice process would be available to complainants who have a defamation claim which is justiciable (likely to be heard if proceedings are filed) in an Australian court.

3.181 Under the MDPs, as set out in **current legal framework**, only natural persons and 'excluded corporations' can sue for defamation in Australia. 'Excluded corporations' include small corporations with 10 employees or less and non-for-profit organisations.

Internet intermediaries

3.182 As noted in **Option 3** above, the complaints notice procedure could apply to a broad range of digital platforms such as: social media services, search engines, digital content aggregators, messaging services and some forum administrators.

3.183 Internet intermediaries that are not publishers at common law would not need to avail themselves of a defamation defence. Accordingly, they would not need to participate in a complaints notice process in order to obtain a safe harbour defence. A complaints notice process would only apply to digital platforms who are likely to be considered publishers and therefore exposed to defamation claims in respect of third-party material they host, index or distribute.

3.184 A complaints notice process may not be relevant to all digital platforms as depending on its design, they may not hold the relevant information required in order to complete the process. For example, search engines do not directly host content they index in their search results and are therefore unlikely to have contact details of originator of that content, so would be unable to connect a complainant with the originator. However, there may

still be a need for a complaints notice process for these types of platforms. This will need to be considered in the design of any process for Australia.

What would a complaints notice process look like?

3.185 The purpose of this section is to seek stakeholder feedback on what a complaints notice process in Australia might look like.

3.186 The DWP considers the complaints notice process in section 5 of *the Defamation Act 2013* (UK) and its associated regulation the *Defamation (Operators of Websites) Regulations 2013* (UK) ('the **UK process**').

3.187 As a point of comparison, the DWP also considers the recommendations in the Final Report of the LCO which proposes a complaints process where intermediary platforms act as go-betweens between complainants and publishers.[116]

3.188 A flow chart mapping the UK process, and the LCO proposal comparisons, is in **Appendix A**.

Analysis of the UK process

Steps to be taken prior to issuing a complaints notice

3.189 The UK process requires that a complainant confirm in the notice of complaint that they do not have sufficient information about the poster (originator) to bring proceedings against that person. Beyond this confirmation, there is no obligation to indicate what steps were taken to identify the originator.

3.190 It could be argued that the complaints notice process should encourage the complainant to make reasonable steps to identify and contact the originator before issuing a complaints notice to a digital platform.

3.191 However, this raises a number of questions, including what should be done in a scenario where there are numerous originators. It may be too onerous to require an aggrieved person to attempt to contact each and every originator in that scenario.

Question 12: Steps required before engaging in the complaints notice process

(a) Should the complainant be required to take steps to identify and contact the originator before issuing a complaints notice? If so, what should the steps be and how should this be enforced?

(b) Where the complainant can identify the originator, should there be any circumstances where the complainant is not required to contact the originator directly and could instead use the complaints notice procedure?

116 Details of the LCO complaints process can be found in Part VIII of the LCO Final Report (n 28).

Complaints notice form and content

3.192 The UK process requires that a complaints notice must:

- specify the name and email address of the complainant,
- set out the meaning which the complainant attributes to the statement referred to in the notice,
- set out the aspects of the statement which the complainant believes are factually inaccurate or opinions not supported by fact,
- confirm that the complainant does not have sufficient information about the poster to bring proceedings against that person, and
- confirm whether the complainant consents to the operator providing the poster with the complainant's name and electronic mail address.

3.193 If the complaints notice is missing any of the required information, then the operator must inform the complainant within 48 hours of receipt of the notice that their notice is defective, but no further action is required until a valid notice is made.

3.194 In Australia, Part 3 of the MDPs has a requirement for the complainant to issue a concerns notice to the publisher before the complainant can commence legal proceedings (see **Interaction of mandatory concerns notice and complaints notice** above).

3.195 A complaints notice could require many of the same elements as a concerns notice. However, consideration must be given to the interaction between these two distinct processes. If the two notices are identical, it will be unclear for the recipient to know what is required of them – for example, make an offer to make amends or to connect the complainant with the originator. To solve this problem, it might be useful for the complaints notice to include a requirement that it be identified as a complaints notice. Alternatively, there may be merit in providing sufficient overlap between the two notices that should a complainant be unsuccessful through the complaints notice process, they are able to use the same notice as a concerns notice for the purposes of the MDPs, allowing them to file proceedings without having to wait a further 28 days for an offer to make amends.

3.196 Given that there would be no cause of action without serious harm being established, it may be appropriate for the complaints notice process to include articulation of the serious harm caused by the alleged defamatory statement.

3.197 Some digital stakeholders have expressed concern that complaints notices may be used to make wilfully false accusations. For example, a complainant who dislikes a post online could use a complaints notice procedure to have the content taken down even if the content is not defamatory. Some stakeholders have suggested that a complaints notice should be in the form of a statutory declaration to hold the complainant accountable, however, this may make the process overly burdensome for the complainant. Another option would be to require complaints notices to include a 'good faith' clause, to require a complainant to declare that the complaint has been made in good faith as to its accuracy, and where an originator can establish this declaration is not true, it will invalidate the notice.

Question 13: Complaints notice form and content

(a) What content should be required to be included in a complaints notice in order for it to be valid? Should this include an indication of the serious harm to reputation caused or likely to be caused by the publication, or should it be sufficient for the content to be prima facie defamatory?

(b) Should there be a requirement for the intermediary to notify the complainant, within a certain time period, that the complaints notice does not meet the requirements?

(c) Should a complaints notice require the complainant to make a 'good faith' declaration? Should there be any other mechanisms used to prevent false claims?

Once a complaint notice is validly made

3.198 The UK process requires the following steps to be followed on receipt of a notice:

<u>On receipt of notice</u>

3.199 If the website operator has no means of contacting the poster, then it must remove the statement within 48 hours of receiving a notice of complaint.

- In contrast, the approach proposed by the LCO approach does not result in the intermediary platform removing any content.
- Consideration needs to be given as to whether this should apply to search engines, or other internet intermediary which do not generally have the ability to contact originators. As already discussed, requiring intermediaries to automatically remove content where they cannot contact the originator could skew the balance away from protecting freedom of expression.

3.200 If the website operator can contact the poster, then the operator must contact the poster within 48 hours of receiving notice. The website operator does not assess whether the claim is in fact defamatory. The content will remain online while the originator is being contacted.

- The LCO suggest intermediary platforms must take 'all reasonable steps' to forward the notice to the publisher. The intermediary platform is to make no assessment of the merits of the complaint and act as a mere 'go-between' of the complainant and publisher.
- Consideration should be given as to whether the content should remain online, be removed, or potentially 'flagged' as under dispute while the originator is being contacted.
- The timeframe in which a digital platform has to contact the originator also needs to be settled. This should be reasonable based on the business environment the digital platform operates in balanced against the complainants need for a speedy outcome.

Required response from the poster

3.201 The poster must respond to the operator by midnight on the fifth day after the notification is sent, indicating whether or not the poster wishes the statement to be removed.

- Again, consideration as to what a reasonable timeframe for this response is, should be based on balancing the rights of the originator and the complainant.

3.202 If the poster does not wish the statement to be removed, they must provide their full name and postal address, and indicate whether the poster consents to the operator providing the complainant with their contact details.

3.203 If the poster responds but the response does not include the required information, the operator must, within 48 hours of receiving the response, remove the statement and notify the complainant.

3.204 If the poster responds and wishes the statement to be removed, the operator must, within 48 hours of receiving the response, remove the statement and notify the complainant.

3.205 If the poster responds and does not wish the statement to be removed, the operator must, within 48 hours of receiving the response, inform the complainant in writing and provide the poster's contact details (if they have consented) or inform the complainant that the poster has not consented for their contact details to be shared. The statement remains online. If the poster does not consent to their details being shared, and the complainant wants to pursue the complainant for the defamatory statement, then they may need to seek an order from the court to force the website operator to reveal the identity of the poster. These types of orders are discussed further under **Issue 5**.

- An alternative option in Australia could be to provide that where the originator does not consent to having their contact details shared, then the content is removed. On one hand, this would encourage posters to take responsibility for content they post online, but on the other hand, this could lead to a chilling effect on free speech, especially where there are good reasons for the originator not revealing their identity, for example in whistle-blower cases.

Outcome of process for operators

3.206 If the operator complies with the above process, they receive the benefit of the defence, regardless of the outcome.

Analysis

3.207 The UK complaints notice procedure raises the following issues that will need to be resolved in an Australian complaints notice process:

- Consideration needs to be given as to whether this mechanism should apply to search engines.

- The UK is still subject to the EC Directive (see **Approaches in other jurisdictions**), which already imposes some take down obligations on website operators.[117] It also provides a defence to hosts of illegal content where they are not aware of the content, and expeditiously remove it once alerted to it.[118]
- During the time the digital platform contacts the originator, consideration should be given as to whether the content should remain online, be removed, or potential 'flagged' as under dispute.
- The timeframe in which a digital platform should contact the originator (if and when relevant) also needs to be settled. This should be reasonable based on the business environment the digital platform operates in balanced against the complainants need for a speedy outcome.
- Consideration must be given to what a reasonable timeframe for the originator to respond to the digital platform should be. It should be based on balancing the rights of the originator and the complainant.

3.208 If the originator responds and does not wish the statement to be removed, this outcome could leave complainants without recourse where the digital platform has complied with the process, thereby gaining the benefit of a defence, and the complainant is left unable to identify the originator and the offending content remains online. This could be mitigated by additional powers being given to the court to order material is removed without the identity of the originator. Consideration needs to be given to what other recourse the complainant would have in this scenario (**see Issues 4 and 5 below**). Consideration needs to be given to whether there are any circumstances where the digital platform should be able to remove the material without the poster's agreement.

Question 14: Application and outcome of complaints notice

(a) Should the complaints notice process be available to all digital platforms who may have liability in defamation or only those that can connect the complainant with the originator?

(b) What should happen to the content complained of following receipt of a complaints notice by the digital platform?

(c) Should the focus of the complaints notice process be to connect the complainant with the originator? What other outcomes should achievable through this process?

(d) What steps from the UK process should be adopted in Australia?

(e) Are there circumstances where the digital platform should be able to remove the content complained of without the poster's agreement?

117 Coor, C. (2015) *Opinion or defamation? Limits of free speech in online customer reviews in the digital era*, Communications Law, 20 (3), p 75.

118 Linklaters, (2010), see: https://www.linklaters.com/en/insights/publications/tmt-news/2010/eu--how-robust-is-the-hosting-defence.

ISSUE 4: Power of courts to order that material be removed

3.209 In the online environment, defamatory content can quickly go 'viral', spreading rapidly through reposting and sharing facilitated by digital platforms. In many cases, those who have shared the material may be resident overseas, or unable to be identified. It can be difficult for a plaintiff to sue every individual who reshares such content, or generally to ensure that all copies of the defamatory content are taken offline.

3.210 Sometimes complainants may engage in defamation proceedings with internet intermediaries in order to have defamatory content removed or delisted, and often this is an important outcome of the litigation.

3.211 In most states, defamation jurisdiction is exercised by superior and lower courts, and sometimes tribunals. These courts have different powers and jurisdictions, particularly in relation to the equitable jurisdiction to issue injunctions (final and interlocutory). There can therefore be variation between jurisdictions and courts as to the powers that can be exercised.

Jurisdiction and enforcement for offshore defendants

3.212 Where defamatory online content is downloaded by a recipient in an Australian state or territory, there will be publication of the defamatory content in that jurisdiction. It does not matter where the defendant (i.e., the originator or potentially, an internet intermediary) is located. However, complainants seeking defamation remedies against an offshore defendant may still face difficulties in pursuing that defendant in an Australian court.

3.213 For example, the court may in its discretion refuse leave to serve an application on an offshore defendant where the cost of the proceedings, balanced against the likelihood of a successful outcome of the proceedings, appears to be disproportionate or an abuse of court process, or where another jurisdiction appears to have a closer connection with the proceedings.

3.214 There is also a risk that, even if proceedings can be commenced, an offshore defendant may not appear. There may also be difficulty in selecting the appropriate defendant entity to be sued where there are local subsidiaries of global entities.[119]

3.215 If an offshore defendant does not appear to defend the proceedings, or comply with orders made in its absence in an Australian court, the complainant would need to consider the further step of having the judgment enforced in the jurisdiction where the offshore internet intermediary is based. This may be difficult.

[119] *Bleyer v Google Inc* [2014] NSWDC 897 cf, *Google LLC v Duffy* [2017] SASCFC 130, *Kocwa v Twitter Inc* [2020] QDC 252, *Defteros v Google LLC* [2020] VSC 219.

Where content has been found to be defamatory by the courts

3.216 A question that arises in this context is whether courts should be entitled to order that internet intermediaries 'take down', de-list, or disable access to content that has been found to be defamatory, regardless of who posted it, and regardless of whether they would be liable as defendants if joined to the proceedings.

3.217 Currently, 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 hosts or indexes the defamatory material is not joined to the proceedings. Courts in defamation proceedings, as in other civil proceedings, will generally only grant orders against defendants joined to the proceedings.[120] However, it can be difficult and expensive for plaintiffs to bring proceedings against internet intermediaries. In addition, even if orders are obtained against an internet intermediary, a recalcitrant defendant may then simply move to a different platform and continue posting defamatory material there. [121]

3.218 If material has been judged as defamatory, and yet is still accessible on one or multiple platforms, the claimant may still be subject to injury to their reputation. A remedy to this situation could be a clear capacity for courts to order that internet intermediaries that are not party to the litigation, especially search engines, must 'take down' or de-list the defamatory content when a judgment against the defendant originator is issued.

3.219 Section 13 of the *Defamation Act 2013* (UK) addresses situations where a judgment that material is defamatory has been given, but the defendant may not be in a position to remove or prevent further dissemination of the material on a website they do not control, or refuses to comply with court orders to do so.

3.220 Section 13(1) provides that:

'Where a court gives judgment for the claimant 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.'

---

120 An exception is the granting of preliminary discovery orders to reveal the identity of a potential defendant, which can be made in certain circumstances as discussed in Issue 5, below.

121 See e.g. *Webster v Brewer* [2020] NZHC 3519, which details the plaintiff's attempts to enforce court orders obtained in Australia: see *Webster v Brewer* (No 3) [2020] FCA 1343) relating to defamatory posts made by the defendant on Facebook. The High Court of New Zealand noted that Facebook, which was not joined to the proceedings, had since removed the defamatory posts and deleted the defendant's account, but that there was evidence to suggest that the defendant was aware that her Facebook account was to be shut down and that she intended to continue posting defamatory content on another platform [at 26]. The High Court of New Zealand awarded a contempt of court fine against the defendant.

3.221 It does not appear that section 13 has been the subject of published case law. This may be because operators of websites are generally amenable to taking down such material as soon as a judgment in the complainant's favour is drawn to their attention, in order to avoid liability.

3.222 By way of further comparison, in a recent ruling, the European Court of Justice determined that European Union law permits a national court of a European Union member country to order Facebook Ireland to remove defamatory content from its platform, including variations of such content with 'equivalent' meaning, where that content had previously been ruled by a court to be defamatory, regardless of which user uploaded that content, and to require such content to be blocked worldwide.[122] In contrast, some courts in other jurisdictions have refused to grant such orders, citing concerns about overbroad restraint of speech.[123]

Ordering removal of content prior to final judgment on defamation.

3.223 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.[124] 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. This means that, if the publisher of online content chooses not to remove content pending the outcome of a defamation trial, the content may remain online, in some cases for months or years.

3.224 While interim injunctions are rare, they may be granted against a defendant in exceptional circumstances.[125] For example, in *Webster v Brewe*r,[126] the Federal Court granted an urgent *ex tempore* interlocutory injunction requiring the defendant to remove 'vile' posts she had made on Facebook about the applicants.

---

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

123 See e.g. *Weitsman v Levesque* (USDC (Sth.Cal.) (case no 19-CV-461 JLS, November 20, 2020) United States District Court for the Southern District of California granting a permanent injunction restraining the defendant from making the same defamatory statements about the plaintiff in future, but refusing to grant an injunction in relation to 'variations' of such statements, or to apply the injunction to social media companies not party to the proceedings.

124 *Bonnard v Perryman* [1891] 2 Ch 269 per Lord Coleridge at 284; *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57; [2006] HCA 46.

125 See e.g. *Chappell v TCN Channel Nine* (1988) 14 NSWLR 153; *The School for Excellence v Trendy Rhino Ptv Ltd* [2018] VSC 514; *Webster v Brewer* [2020] FCA 622.

126 *Webster v Brewer* [2020] FCA 622. The interim injunction was subsequently expanded due to the defendant posting further material after the first interim injunction: *Webster v Brewer* (No 2) [2020] 727; and made permanent consequent on the award of default judgment and damages to the plaintiffs: *Webster v Brewer* (No 3) [2020] FCA 1343.

3.225 In its review of *Defamation Law in the Internet Age*, the LCO noted the current test for take-downs in defamation claims has too high of a threshold to be suitable for the emergence of the types of harms that can be perpetuated online. This raises the question of whether the current threshold for a plaintiff to obtain an interim injunction requiring a defendant originator to remove allegedly defamatory content posted online pending trial is appropriate.

3.226 A further question arises as to whether and in what circumstances an interim injunction requiring an internet intermediary to remove such content should be granted. The LCO recommends that reforms be introduced to provide that, on motion by a plaintiff, the court in a defamation action may issue an interlocutory takedown 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 plaintiff 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.[127]

3.227 There have been few cases in Australia concerning interim injunctions against internet intermediaries requiring them to remove, de-list or block allegedly defamatory content posted online by a third-party.[128] Any potential reforms seeking to codify the power of courts to issue such orders would require consideration as to what the threshold for such an order should be (see discussion above on orders courts have made). For example, consideration should be given to whether such an order might be applied for if a court finds, in a preliminary hearing, that the publication meets the serious harm threshold introduced into the MDPs by the stage one defamation reforms.

3.228 There is also a question as to whether such an order could or should be granted against an internet intermediary, such as a social media platform, where the originator of the content, or another intermediary involved in publication on the platform (such as a forum administrator on whose page the content appears), objects to such an order or might have if a party to the proceedings or otherwise was given an opportunity to be heard.

3.229 Another issue is the particular powers of courts within the structure of different jurisdictions, and whether such matters can be addressed through reform of the MDPs, or are matters of civil procedural rules.

---

127 LCO Final Report (n 28) Recommendation 22(a).

128 See e.g. *KT v Google LLC* [2019] NSWSC 1015 (interlocutory injunction granted against Google requiring it to remove reviews posted on Google Reviews); *Kowca v Twitter Inc* [2020] QDC 252 (application for interim injunction against Twitter Inc requiring it to remove user posts refused).

3.230 Finally, there may be considerations of the jurisdiction of courts to make such orders, or to have them enforced, when dealing with offshore based internet intermediaries with global reach.

Question 15: Orders to have online content removed

(a) What should be the threshold for obtaining an order before a trial to require the defendant to take down allegedly defamatory material?

(b) Is there a need for specific powers regarding take down orders against internet intermediaries that are not parties to defamation proceedings, or are current powers sufficient?

(c) What circumstances would justify an interim or preliminary take down order to be made prior to trial in relation to content hosted by an internet intermediary? Should courts of all levels be given such powers? For example, in some jurisdictions lower courts have limited powers to make orders depending on the value of the claim.

(d) Should a court be given power to make an order which requires blocking of content worldwide in appropriate circumstances?

(e) If such powers are necessary, it is appropriate for them to be provided for in the MDPs or should it be left to individual jurisdictions' procedural rules?

(f) Are there any potential difficulties with jurisdiction or enforceability of such powers which could be addressed through reform to the MDPs?

ISSUE 5: Power of courts to order that internet intermediaries reveal the identity of originators

3.231 It may be difficult for a complainant to obtain details disclosing the identity of an originator posting defamatory material about them online, as the originator may be using a pseudonym. The digital platform may be reluctant to disclose the originator's personal details due to privacy concerns, or may consider that it has no obligation to do so, without a court order.

3.232 In some recent cases, complainants seeking to discover the identity of unknown originators of allegedly defamatory material have obtained orders requiring an internet intermediary to disclose any information it holds concerning the originator's identity as part of preliminary discovery against the intermediary in defamation proceedings.[129] Generally speaking, such orders may be obtained where the applicant satisfies a court that:

- the applicant, having made reasonable inquiries, has been unable to ascertain the identity of a known person for the purposes of commencing proceedings against the prospective defendant; and
- some other person than the plaintiff has information or documents that may tend to assist in ascertaining the identity or whereabouts of the prospective defendant,[130] or knows or is likely to know, or has control of a document that would help establish the identity of the prospective defendant.[131]

3.233 For example, in *Kabbabe v Google LLC* (***Kabbabe***),[132] a Victorian dentist was successful in obtaining an order under rule 7.22 of the Federal Court Rules requiring Google to disclose, by way of preliminary discovery, any information in its possession about the identity of a prospective defendant who posted an allegedly defamatory 'Google review' of his dental practice under a pseudonym.

3.234 Where the making of such an order requires service out of the jurisdiction, as was the case in *Kabbabe,* the prospective applicant must also obtain leave of the court under the applicable civil procedure rule.[133]

3.235 Given the expense of obtaining such orders, it is worth considering whether there is a more efficient method of obtaining such orders to enable a complainant to commence proceedings against the originator. Another consideration is whether countervailing interests, such as the privacy of internet users, are adequately protected.

---

129 See e.g. *Kukulka v Google LLC* [2020] FCA 1229; *Kabbabe v Google LLC* [2020] FCA 126.

130 Uniform Civil Procedure Rules 2005 (NSW), r 5.2.

131 Federal Court Rules 2011 (Cth), r 7.22.

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

133 See e.g. Federal Court Rules 2011 (Cth), r. 10.43(2).

3.236 In the UK, orders to 'innocent' third parties to disclose the identity of alleged anonymous 'wrongdoers' are known as '*Norwich Pharmacal'* orders.[134] Such orders are an exercise of the court's equitable jurisdiction, and under the common law require a plaintiff 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
- 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'.[135]

3.237 Unlike in Australia, UK courts are expressly required to take into account countervailing human rights considerations under UK laws. These rights include the data rights, or rights of privacy, of users of digital platforms and the right of freedom of expression. Such considerations have set the threshold for the test. Under the first limb, the complainant must show that the prospective defendant 'arguably', or (as a recent case has put it)[136] 'well arguably', committed wrongdoing, and, under the second limb, the making of the order must be a 'necessity', which introduces considerations of alternatives and of proportionality. Nevertheless, it is argued that there remains potential for such orders to be abused, and that courts should not grant such orders where the primary aim is to harass or unmask an anonymous critic.[137] In the US, the threshold for making of such orders is higher still, in recognition of the chilling effect on freedom of expression such orders may have.[138]

3.238 By contrast, in Australia, the current threshold for granting of preliminary discovery orders to unmask a prospective defendant appears to be relatively low. In *Kabbabe,* the applicant was not required to show an 'arguable' case of defamation against the prospective defendant. Rather, he was required only to show that he wished to commence proceedings against the unknown originator who had posted the Google review, and that Google 'may' have information which could identify them so that he could do so.[139]

---

134 See *Norwich Pharmacal v Commissioners of Customs and Excise* [1974] AC 133.

135 Lightman J, *Mitsui & Co Ltd v Nexen Petroleum UK Ltd* [2005] EWHC 625 (Ch) [2005] 3 All ER 511 at [21].

136 *Baker v Burford Capital Limited* [2020] EWHC 1183 at [40].

137 Riordan (n 1) 90 citing US authorities such as *Doe v Cahill*, 884 A 2d 451, 459 (Del SC, 2005).

138 Riordan (n 1).

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

3.239 Australian civil procedure rules for preliminary discovery orders to unmask prospective defendants are of general application in all civil proceedings. They do not expressly require the court to have regard to countervailing considerations of the privacy of users, freedom of expression or the protection of whistle blowers. In Australian defamation proceedings, there is a rule known as the 'newspaper rule', which refers to a rule of practice whereby a court will generally not order preliminary discovery where the order would reveal a journalists' confidential sources in advance of a trial. The journalist or newspaper defendant must defend the action without being able to call the confidential source as a witness at trial but will not be required to reveal the source. This rule protects freedom of expression by preventing complainants from seeking to unmask a confidential source, such as a whistle blower, by commencing defamation proceedings against the journalist or newspaper.[140] However, where the newspaper rule does not apply, or unless the internet intermediary itself opposes the order, it appears that these considerations are unlikely to be raised in defence of an unknown originator.

3.240 In its *Defamation Law in the Internet Age* report, the LCO notes that *Norwich Pharmacal* orders are common place in online defamation litigation in Ontario.[141] The courts have developed a test that requires the plaintiff to take reasonable steps to identify the originator, and where there are not overriding privacy considerations, a *Norwich Pharmacal* order may be granted where the 'public interest favouring disclosure outweighed the freedom of expression and privacy interests of the unknown alleged wrongdoers'.

3.241 A further issue for consideration is whether and how the orders referred to in this section could be enforced if a foreign based digital platform does not accept the jurisdiction of an Australian court and does not voluntarily comply with the order.

Preservation of records of internet intermediaries

3.242 To facilitate *Norwich Pharmacal* orders, the LCO recommends that reforms be introduced to provide that, on being served with notice of a motion for a *Norwich* Pharmacal order, an intermediary platform shall retain any records of information identifying an unknown originator for a period of one year to allow the plaintiff to obtain a court order requiring the release of the information.[142]

140 *John Fairfax & Sons v Cojuangco* ('Newspaper Rule case') [1988] HCA 54; (1988) 165 CLR 346 at [23].

141 LCO Final Report (n 28) 60.

142 LCO Final Report (n 28) Recommendation 23.

3.243 It is unclear whether a reform introducing new procedural rules requiring internet intermediaries to retain records which could identify unknown originators are necessary. As case law in this area is recent and scant, it is unclear whether any complainants are being frustrated by internet intermediaries deleting such records. In one defamation proceeding, the court observed that records of deleted social media posts could be recovered with relative ease by following the instructions provided by Facebook for resurrection of a user account.[143]

3.244 A further question arises as to whether such orders are a matter for the MDPs, or should be dealt with under civil procedural rules of different courts exercising jurisdiction in defamation matters. While there are clear benefits in having consistency across all jurisdictions, there are complexities in trying to make model laws work alongside different jurisdictions' procedural rules, and generally these matters are left for each jurisdiction to address.

Question 16: Orders to identify originators

(a) Is it necessary to introduce specific provisions governing when a court may order that an internet intermediary disclose the identity of a user who has posted defamatory material online?

(b) What countervailing considerations, such as privacy, journalists' source protection, freedom of expression, confidentiality, whistle-blower protections, or other public interest considerations might apply?

(c) What types of internet intermediaries should such provisions apply to?

(d) Is it necessary to provide for reforms to ensure that records are preserved by intermediaries where a complainant may wish to uncover the identity of an unknown originator?

(e) Do any enforcement issues arise in relation to foreign-based internet intermediaries who may not accept jurisdiction? How could this be overcome?

(f) Is it appropriate to provide for these types of orders in the MDPs, or should this be left to each jurisdiction's procedural rules?

Other issues

Question 17: Other issues regarding liability of internet intermediaries

(a) Are there any other issues regarding liability of internet intermediaries for the publication of third-party content that need to be considered?

143 *Mosslmani by his tutor Karout v Nationwide News Pty Ltd (No 2)* [2018] NSWDC 113 at [39-40].

PART B – Extending absolute privilege

Extending absolute privilege

The threat of being sued for defamation has the possibility of 'chilling' certain forms of communication. For this reason, in limited situations, certain communications are deemed more important than a plaintiff's right to protect their reputation and are given absolute privilege against a claim in defamation. These are generally situations where there is a strong public interest to protect free and open communication. For example, it would be undesirable for society at large if a judge filtered what he or she said in court for fear of being the subject of an action in defamation. Absolute privilege therefore applies to proceedings in court, parliamentary proceedings, and a small number of other circumstances where a strong public interest exists.

It has been suggested that victims and witnesses may be deterred from reporting alleged crimes to police, or that individuals do not make complaints about sexual harassment to employers, out of fear of being sued in defamation. This has received public attention in the context of the #metoo movement. The Australian Human Rights Commission recently reported that sexual harassment is pervasive in Australian workplaces, and that defamation laws were discouraging the disclosure of this behaviour.[144]

It is possible that an extension of absolute privilege to these circumstances could reduce this 'chilling' effect. However, this raises a number of issues. It is unclear how significant or widespread this chilling effect is. Further, as absolute privilege removes the right of a plaintiff to seek a remedy for damage to reputation, there needs to be strong protection against the making of false or malicious reports or complaints.

In this section the DWP is considering two scenarios:

- Issue 1: Statements made to police and statutory investigative agencies
- Issue 2: Complaints of unlawful conduct made to employers and professional disciplinary bodies.

The DWP is seeking stakeholder views on whether there are problems here that need to be addressed, and, if so, whether extending absolute privilege would be an appropriate mechanism for doing this.

An important consideration is the existing defences that apply to these types of situations. In **Context**, the DWP briefly outlines the existing law of absolute privilege and the other relevant defence of qualified privilege. In **Key issues**, the DWP sets out its understanding of how existing defences apply to these circumstances and whether there may be any gaps. The DWP also considers – if absolute privilege were to be extended – what safeguards would need to be in place to protect against false or malicious reporting. The DWP seeks stakeholder feedback on these matters.

144 Australian Human Rights Commission, (2020), *Everyone's business: Fourth national survey on sexual harassment in Australian workplaces. Respect@Work: Sexual Harassment National Inquiry.*

4. Context

Absolute privilege

4.1 Absolute privilege is a complete immunity, which applies irrespective of the speaker's motive or reasonableness. The likely availability of an absolute privilege defence discourages the commencement of defamation proceedings, or when commenced, often results in their summary dismissal.[145]

4.2 Absolute privilege is, accordingly, only available in limited circumstances when a plaintiff's right to protect his or her reputation must be subordinated to a superior interest.[146]

4.3 Circumstances that attract absolute privilege are occasions where the immunity is indispensable to the public interest. Australian courts have limited absolute privilege by reference to the concept of 'necessity'.[147] Traditionally, these occasions are the administration of justice, Ministers advising the Crown, and the proceedings of Parliament.[148]

4.4 Common law absolute privilege in respect of the administration of justice includes evidence to and findings of courts and tribunals exercising quasi-judicial powers.[149] Complaints to professional disciplinary bodies may also attract absolute privilege at common law. This depends on the composition and powers of the professional body, and, in particular, whether the body has the power to make disciplinary findings of interest to the public. Absolute privilege applies to complaints made to the body which are 'part of an established procedure which must be set in motion if it is to result in disciplinary proceedings even if disciplinary proceedings will not necessarily eventuate'.[150] The extension of absolute privilege to these bodies has been stated to be a safeguard against the abuse of defamation law to dissuade a complainant from 'supporting the continuation of an investigation'.[151]

---

145 See e.g. *Vescio v Guardianship Tribunal of New South Wales* [2009] NSWDC 341.

146 Rolph, D. 2016, Defamation law, Thomson Reuters, Sydney at [10.20].

147 *Mann v O'Neill* (1997) 191 CLR 204 per Dawson, Toohey, Gaudron, McHugh, Gummow and Kirby JJ.

148 *Dawkins v Lord Rokeby* [1873] LR 8 QB 255 at 268, cited in Rolph, at [146].

149 *Mann v O'Neill* (1997) 191 CLR 204, Lassanah v NSW [2009] NSWDC 73.

150 *Mann v O'Neill* (1997) 191 CLR 204 per Dawson, Toohey, Gaudron, McHugh, Gummow and Kirby JJ. For an example where absolute privilege has applied to a complaint to a disciplinary body, see *Hercules v Phease* [1994] 2 VR 411 (complaint to Law Society of Victoria by client of solicitor was subject to absolute privilege).

151 *Hercules v Phease* [1994] 2 VR 411 per Ormiston J.

4.5 The common law position on absolute privilege has been extended and clarified by the MDPs. Clause 27 of the MDPs provides that it is a defence to the publication of defamatory matter if the defendant proves that it was published on an occasion of absolute privilege. This includes if:

(a) the matter is published in the course of the proceedings of a parliamentary body

(b) the matter is published in the course of the proceedings of an Australian court or Australian tribunal

(c) the matter is published on an occasion that, if published in another Australian jurisdiction, would be an occasion of absolute privilege in that jurisdiction under a provision of law in the jurisdiction corresponding to the proposed section

(d) the matter is published by a person or body in any circumstances specified in Schedule 1 ('Additional publications to which absolute privilege applies').

4.6 Under clause 27(2)(d) of the MDPs, states and territories may specify additional matters within their jurisdictions that are subject to absolute privilege by way of Schedule 1. The effect of clause 27(2)(c) is that, if a state or territory includes a publication in its equivalent of Schedule 1, then that publication will also have the benefit of absolute privilege in all other states and territories.

4.7 South Australia and New South Wales are the only states to prescribe additional matters in Schedule 1 (or Schedule A1 as it is in South Australia). New South Wales has specified 29 additional publications in Schedule 1 of the *Defamation Act 2005* (NSW), including matters related to the *Anti-Discrimination Act 1977* (NSW), *Legal Profession Uniform Law* (NSW), and *Independent Commission Against Corruption Act 1988* (NSW). South Australia (under Schedule A1 of the *Defamation Act 2005* (SA)) provides absolute privilege to matters published by the Parole Board of South Australia.

4.8 Statutory extensions of absolute privilege also exist under a range of other state and territory laws. Examples include laws extending absolute privilege to complainants making public interest disclosures under 'whistle-blower' laws[152] and in relation to investigations or reports by industry regulatory bodies and ombudsmen.[153] Section 111 of the *Sex Discrimination Act 1984* (Cth) extends absolute privilege to complaints concerning sexual harassment made to the Australian Human Rights Commission and to witness statements made in relation to such complaints.[154]

---

152 See s 36 *Public Interest Disclosure Act 2012* (ACT); s 10 *Public Interest Disclosure Act 2013* (Cth); s 21 *Public Interest Disclosure Act 1994* (NSW); s 38 *Public Interest Disclosure Act 2010* (Qld); s 41, *Public Interest Disclosures Act 2012* (Vic); s 120 *Biodiversity Act 2004* (Qld); s 289 *Integrity Commission Act 2018* (ACT); s 26F *Safe Drinking Water Act 2003* (Vic); s 16 *Public Interest Disclosures Act 2002* (Tas).

153 See s 48 *Judicial Officers Act 1986* (NSW); s 276 *Health Ombudsman Act 2013* (Qld); s 81 *Gas Safety Act 2018* (Tas).

154 The protections are not limited to sexual harassment complaints but apply to any action or proceeding for damages under the *Sex Discrimination Act 1984* (Cth). Equivalent provisions are also contained in the *Disability Discrimination Act 1992* (Cth), the *Age Discrimination Act 2004* (Cth) and the *Racial Discrimination Act 1975* (Cth).

Qualified privilege

4.9 The qualified privilege defence recognises that there are circumstances where a person has a legal, moral or social duty to communicate information to a recipient who has an interest in receiving it – for example, giving a job reference, answering police inquiries, or parent-teacher interviews. Unlike absolute privilege, it is a defence that may be defeated in some circumstances.

4.10 To rely on a defence of qualified privilege, a defendant does not need to prove that a defamatory imputation is true. Nevertheless, it is more costly and time consuming for a defendant to rely on a qualified privilege defence than an absolute privilege defence. This is because the qualified privilege defence is fact dependent and can be defeated by evidence of malice, or in the case of statutory qualified privilege, of lack of reasonableness. These issues will generally be required to be the subject of evidence given at trial.

4.11 Accordingly, the cost of defending a claim based on the defence of qualified privilege can pose a significant financial burden on the defendant, even if the defendant is ultimately not found liable.[155]

4.12 The defence of qualified privilege exists both at common law and in clause 30 of the MDPs (statutory qualified privilege).

Common law qualified privilege

4.13 Common law qualified privilege applies where there is a public or private legal or moral duty to publish a matter, and a corresponding interest on the part of the audience to receive it.[156]

4.14 The classic example is the giving of an employment reference. The categories or circumstances where common law qualified privilege can arise are not closed.[157]

4.15 The defence can be lost if the scope of publication exceeds the privileged occasion, for example, the publication is made to a wider audience than necessary, or includes gratuitous additional statements, subject to the caveat that the privilege is not to be interpreted 'narrowly'.[158]

---

155 See e.g. *KSMC Holdings Pty Ltd t/as Hubba Bubba Childcare on Haig v Bowden* [2020] NSWCA 158 (referencing that the costs of the original defendants, who ultimately proved qualified privilege on appeal, totalled $476,219.54).

156 Parke B, Toogood v Spyring (1834) 149 ER1034 at 1044-1045, cited in *Papaconstuntinos v Holmes A Court* (2012) 249 CLR 534; *Cush v Dillon* (2011) 243 CLR 298; [2011] HCA 30 at [22]; *KSMC Holdings Pty Ltd t/as Hubba Bubba Childcare on Haig v Bowden* [2020] NSWCA 28 per Payne JA at [50].

157 See *Papaconstuntinos v Holmes A Court* (2012) 249 CLR 534.

158 See e.g. *KSMC Holdings Pty Ltd t/as Hubba Bubba Childcare on Haig v Bowden* (2020)101 NSWLR 729; [2020] NSWCA 28, whereby the New South Wales Court of Appeal determined on appeal that a child care manager's communication to parents regarding the circumstances of departure of an employee was made under qualified privilege, reversing the trial judge on this defence.

4.16 The common law qualified privilege defence can also be lost due to 'malice', which broadly refers to improper motive or dishonesty.[159] However, burden of proving malice rests on the plaintiff, and is a 'heavy burden' which must displace 'the presumption of honesty' in favour of the defendant.[160]

Section 30 qualified privilege

4.17 Under clause 30 of the amended MDPs, the defence of qualified privilege applies to the publication of defamatory matter to a person where:

- the recipient has an interest or apparent interest in having information on some subject,
- the matter is published to the recipient in the course of giving to the recipient information on that subject, and
- the conduct of the defendant in publishing that matter is reasonable in the circumstances.

4.18 Clause 30(3) provides a non-exhaustive list of factors which the court may take into account when assessing whether the defendant's conduct was reasonable. These factors include the extent to which the matter published is of public interest, the nature of the business environment in which the defendant operates, and whether the matter published contains the substance of the defamed person's side of the story.

159 *Roberts v Bass* (2002) 212 CLR 1; *Fraser v Holmes* [2009] NSWCA 36; *KSMC Holdings Pty Ltd t/as Hubba Bubba Childcare on Haig v Bowden* [2020] NSWCA 28.

160 *KSMC Holdings Pty Ltd t/as Hubba Bubba Childcare on Haig v Bowden* [2020] NSWCA 28 per Payne JA at [59], citing *Roberts v Bass* (2002) 212 CLR 1; [2002] HCA 57 at [96]-[97].

5. Key issues

ISSUE 1: Statements made to police and statutory investigative agencies

5.1 There is a strong public interest in making sure victims and witnesses of crimes are not deterred from reporting alleged criminal conduct out of fear that they will be sued for defamation. These individuals may seek to report criminal conduct either to police or a relevant statutory investigative agency. At the same time, it is important to ensure appropriate safeguards are in place to prevent false or malicious reporting.

5.2 The DWP is seeking views on whether current defamation law is having a chilling effect on reporting of allegations of criminal behaviour to police and to statutory investigative agencies, such as crime or corruption commissions. Views are sought on whether there is a need to extend absolute privilege to these statements to provide clarity and certainty to all those reporting criminal conduct to the police or a statutory investigative agency.

Types of reports

5.3 With respect to types of reports, the DWP is considering reports of any alleged conduct that is a criminal offence, made to police or statutory investigative agencies. For example, reports may relate to domestic violence, assault, theft, corruption or fraud.

Police and statutory investigative agencies

5.4 Reports could be made to police (state and territory police or the Australian Federal Police) or statutory investigative agencies. Statutory investigative agencies means agencies established by legislation and given powers to investigate alleged criminal conduct. This includes, for example, the NSW Independent Commission Against Corruption, the NSW Crime Commission and the Victorian Independent Broad-based Anti-Corruption Commission.

Existing protections for reports made to police

5.5 There are no states or territories where absolute privilege applies to reports made to police.

5.6 Currently in Australia, if a report of criminal behaviour made to the police were the subject of an action in defamation, it is likely that it would attract the defence of qualified privilege.

Existing protections for reports made to statutory investigative bodies

5.7 There does not appear to be consistency across states and territories as to when absolute privilege will apply to complaints made to statutory investigative authorities, as this depends on the enabling legislation of that authority.

5.8 As noted above, South Australia and New South Wales are the only states to use Schedule 1 of their defamation legislation to extend absolute privilege to certain statutory bodies and circumstances. In addition, the enabling legislation of some statutory bodies can extend absolute privilege to certain communications.[161]

5.9 Qualified privilege is likely to apply for reports of alleged criminal conduct made to bodies responsible to investigate those matters.

Is there adequate protection for those making reports?

5.10 There is an argument that the qualified privilege defence does not provide adequate protection or adequate certainty to those making reports of alleged criminal conduct. It is possible that fear of being sued for defamation, with the associated financial and personal burden of litigation which is incurred even if the defendant is not found liable, may deter victims or witnesses from reporting alleged criminal conduct to police or statutory investigative agencies.

5.11 The potential burden of defamation litigation where a qualified privilege defence is pleaded at trial can be significant. For example, in *Bechara v Bonacorso*[162] (***Bechara***), the plaintiff became aware of a confidential complaint made to police by the defendant through a subpoena issued to police in an unrelated matter. The plaintiff obtained an extension of time to file proceedings.[163] After multiple interim hearings and a ten-day trial, the defendant proved a qualified privilege defence.

Are people inhibited from making reports?

5.12 The DWP is seeking submissions on whether there is evidence to suggest that individuals are deterred from reporting alleged crimes to police or statutory investigative agencies because of the threat of defamation litigation.

---

161 See e.g. s 289 *Integrity Commission Act 2018* (ACT) (absolute privilege applies to information in a complaint to the Commission in certain circumstances).

162 *Bechara v Bonacorso* (No 4) [2010] NSWDC 234.

163 *Bechara v Bonacorso* (No 1) [2009] NSWDC 131.

5.13 The DWP is currently not aware of any cases where a person has been successfully sued in defamation for making a report to police or an investigative agency. Nevertheless, this does not negate a complainant's exposure to lengthy defamation proceedings requiring determination of the qualified privilege defence at trial, as *Bechara* illustrates. In addition to *Bechara*, the DWP is aware of other cases which were commenced in such circumstances, even though they did not proceed to trial.[164] The introduction of an absolute privilege defence would be a deterrent to such proceedings. If they were commenced, it is likely they would be summarily dismissed.

Question 18: Defamation and reports of criminal conduct

(a) Are there any indications that defamation law is deterring victims and witnesses of crimes from making reports to police and other statutory investigative agencies charged with investigating criminal allegations?

(b) Are victims and witnesses of crimes being sued for defamation for reports of alleged criminal conduct to authorities?

Extending absolute privilege to reports to police

5.14 In the UK, common law absolute privilege now extends to reports to the police of alleged criminal conduct. In *Westcott v Westcott*,[165] the England and Wales Court of Appeal found that a complaint to the police by a person claiming to be the victim of criminal conduct would be subject to a defence of absolute privilege:

> *'...immunity for out of court statements is not confined to persons who are subsequently called as witnesses. The policy being to enable people to speak freely, without inhibition and without fear of being sued, the person in question must know at the time he speaks whether or not the immunity will attach. Because society expects that criminal activity will be reported and when reported investigated and, when appropriate, prosecuted, all those who participate in a criminal investigation are entitled to the benefit of absolute privilege in respect of the statements which they make. That applies whether they are informants, investigators, or prosecutors.'*

164 See e.g. *Jones v Williams* (pseudonyms) [2018] NSWSC 954 (complaint to police by the family of wife of estranged husband. Application for extension of limitation period in defamation proceedings refused); *Calabro v Zappia* [2010] NSWDC 127 (statutory declaration made to police in apprehended violence application. Application for extension of limitation period in defamation proceedings refused).

165 *Westcott v Westcott* [2008] EWCA Civ 818.

5.15 A similar approach could be adopted in Australia on the same basis. Extending absolute privilege to those who report criminal conduct to the police could bring it in line with existing absolute privilege applying to all publications published in the course of proceedings of an Australian court. The adoption of the UK approach could create greater clarity, removing the distinction between those who have made a report to police and whether or not that report ends up associated to court proceedings. Furthermore, there are strong public policy grounds to ensure victims and witnesses of crimes can make reports to police freely without the risk or threat of defamation proceedings.

5.16 If absolute privilege is extended, there is a need to guard against false reports being made to the police and statutory investigative agencies. All jurisdictions in Australia have criminal offences for the making of false reports to police.[166] This provides a strong disincentive for the making of false or malicious reports to police.

Extending absolute privilege to reports to statutory investigative agencies

5.17 As above, the MDPs provide for each state and territory to add a schedule to its defamation legislation listing statements and entities that attract absolute privilege. Schedule 1 to the *Defamation Act 2005* (NSW) extends absolute privilege to certain communications in relation to 29 statutory organisations or professional bodies. The professional bodies relate to the medical profession and the legal profession. The majority of statutory bodies are investigative bodies, such as the NSW Ombudsman, and, the NSW Independent Commission Against Corruption. Schedule A1 to the *Defamation Act 2005* (SA) extends absolute privilege to proceedings arising out of the Parole Board of South Australia. No other jurisdiction has added a schedule of this nature to its defamation legislation.

5.18 To protect reports of alleged criminal conduct made to statutory investigative bodies across Australia, other jurisdictions could adopt an approach similar to NSW. That is, jurisdictions could include in their Schedule 1 of their Defamation Acts statutory investigative agencies they intend to be covered by absolute privilege.

5.19 A key consideration is what types of statutory investigative agencies should be covered (e.g. all agencies dealing with complaints of alleged criminal conduct). These agencies will vary slightly in their functions and composition between jurisdictions. Secondly, consideration needs to be given whether there should be agreement across jurisdictions to promote a higher level of consistency, or whether each jurisdiction should decide on which bodies to include on their own.

166 For example, ss 574B and 314 of the *Crimes Act 1900* (NSW).

5.20 Lastly, consideration must be given to the need to protect against the making of false or malicious reports. Agencies that are included in Schedule 1 should have authorising legislation that protects against false reports and provides for rigorous processes for maintaining confidentiality. Those that do not have safeguards against false reports and protections for confidentiality could have their authorising legislation amended to include these two protections. Consideration should be given to whether investigative agencies without protection against false or misleading reports should simply be excluded.

5.21 All states and territories have general criminal offences for the making of false statements to government agencies or to a person exercising powers under a law of that state or territory, producing false documents, and providing false evidence.[167] These general laws could be sufficient safeguards against false reporting to statutory investigative bodies investigating allegations of criminal conduct.

5.22 Any potential solution will need to balance the public interest in protecting witnesses and victims, with the right to effective and fair remedies for persons whose reputations are harmed by the publication of a report that is defamatory.

Question 19: Absolute privilege for reports to police and investigative agencies

(a) Should the defence of absolute privilege be extended to statements made to police related to alleged criminal conduct?

(b) Should the defence of absolute privilege be extended to statements made to statutory investigative agencies related to alleged criminal conduct? If yes, what types of agencies?

(c) What type of statutory investigative agencies should be covered and what additional safeguards, if any, may be needed to prevent deliberately false or misleading reports and to protect confidentiality?

(d) What is the best way of amending the MDPs to achieve this aim (for example, by amending clause 27 and/or by each jurisdiction amending its Schedule 1)?

167 See e.g. ss 574B and 314 of the *Crimes Act 1900* (NSW); s 53 *Summary Offences Act 1966* (Vic); s 72 *Public Interest Disclosures Act 2012* (Vic); s 62 *Summary Offences Act 1953* (SA) in regards to reports to police; s 22 *Independent Commissioner Against Corruption Act 2012* (SA) in relation to reports to ICAC; s 44A *Police Offences Act 1935* (Tas) in regards to false reports to police.

ISSUE 2: Complaints of unlawful conduct made to employers and professional disciplinary bodies

5.23 There is a public interest in ensuring that people are not prevented or dissuaded from reporting alleged misconduct to employers (or to investigators appointed by employers to investigate such complaints) and professional disciplinary bodies out of fear that they will be sued for defamation. Equally, there is a need to protect against false or malicious reporting.

5.24 The DWP is particularly interested in looking at complaints related to unlawful behaviour such as sexual harassment or discrimination. The #metoo movement, and other movements like it, have increased the visibility of the issue of sexual harassment, particularly sexual harassment in the workplace.[168]

5.25 There is significant evidence that sexual harassment is pervasive in Australian workplaces. The Australian Human Rights Commission released *Everyone business: Fourth national survey on sexual harassment in Australian workplaces* 2018 and the Report of its *Respect@Work: National Inquiry into Sexual Harassment in Australian Workplaces* in 2020. The 2018 National Survey results indicate that 33% of people who had been in the workforce in the previous five years said they had experienced workplace sexual harassment. Women (39%) were more likely than men (26%) to have experienced workplace sexual harassment in this period.[169] In a study annexed to the Commission's report, Deloitte reported that workplace sexual harassment was estimated to cost the Australian economy approximately $3.8 billion in 2018.[170]

5.26 The Australian Human Rights Commission heard during its *National Inquiry into Sexual Harassment in Australian Workplaces* that Australia's defamation laws discourage the disclosure and public discussion of sexual harassment claims, emphasising the need for reform in this area.[171] The Commission found a lack of protections for witnesses in defamation matters could have a chilling effect on victims reporting incidents of sexual harassment as defamation matters offered very few legal protections for privacy and confidentiality. The Report did not detail to what extent current defamation law has a chilling effect on the reporting of sexual harassment arising out of incidents occurring in the workplace.[172]

---

168 Australian Human Rights Commission (n 144) 86.

169 Australian Human Rights Commission (n 144) 26.

170 Deloitte Access Economics, *The Economic Costs of Sexual Harassment in the Workplace* (Final Report, February 2019), p 5.

171 Several submissions to the Commission's inquiry referenced the need for a public interest defence to facilitate public discourse on sexual harassment complaints.

172 The Commission has elsewhere published a Code of Practice for employers outlining the circumstances in which qualified privilege will protect the complainant and recipients of a sexual harassment complaint in the workplace: Australian Human Rights Commission, Effectively Responding to Sexual Harassment Complaints: A Code of Practice for Employers (2008), Chapter 10.

5.27 Other unlawful conduct may include discrimination or certain threatening behaviours in the workplace which are prohibited by legislation. The extent to which conduct is unlawful varies across jurisdictions.

Question 20: Defamation and reports of unlawful conduct in the workplace

(a) Is fear of being sued for defamation is a significant factor deterring individuals from reporting unlawful conduct such as sexual harassment or discrimination to employers or professional disciplinary bodies?

(b) Are victims and witnesses of sexual harassment or discrimination being sued for defamation for reports of alleged unlawful conduct to employers or professional disciplinary bodies?

Complaints to employers

5.28 'Employer' is a very broad and varied categorisation. It includes large multinational corporations, government agencies, small businesses such as cafes or convenience stores, and everything in between.

5.29 Currently in defamation law, a complaint made by an employee to their employer about unlawful conduct in the workplace, such as sexual harassment, is likely to be covered by the defence of qualified privilege. Arguably, this would also extend to disclosures made to an investigator appointed by the employer, effectively as its agent to investigate such a complaint. Qualified privilege may also attach to a response by a person accused of such misconduct.[173]

5.30 As noted above, the disadvantage with qualified privilege is that it is fact dependent, and generally requires determination at trial, after the accumulation of legal fees and court time. The potential need to expend time and money on this may be enough to discourage individuals coming forward.

5.31 It should be noted that where a sexual harassment or other claim does not involve criminal conduct or require investigation by a statutory body such as a discrimination commission, the offences of making a false statement or giving false information to authorities mentioned above would not apply, unless the complainant has been required to provide a statutory declaration or affidavit. Accordingly, the question arises as to whether it is appropriate to consider removing an accused's right to sue for defamation if a malicious false complaint to an employer has been made where no potential criminal sanction applies.

173 See e.g. *Dye v Commonwealth Securities* [2012] FCA 242.

5.32 In this context, it should also be noted there may be civil[174] or criminal[175] consequences under anti-victimisation provisions of discrimination[176] or employment discrimination[177] laws if a person accused of discrimination, takes or threatens to sue the complainant for defamation. Victimisation generally refers to taking, or threatening to take, adverse or detrimental action against a complainant. Victimisation can include threats of defamation action, or the issuing of a concerns notice. [178]

5.33 An improvident defamation threat could also aggravate damages for sexual harassment, if the complainant proves the allegations were true. For example, in one case,[179] a shop employee complained to her manager that a delivery driver had sexually harassed her while on the shop premises. The manager then made a complaint on her behalf, without her knowledge, to the delivery company. The delivery driver responded by issuing a defamation concerns notice to the complainant, demanding a retraction, an apology and $30,000. The complainant then commenced proceedings against the delivery driver alleging sexual harassment in contravention of section 17(2) of the *Anti-discrimination Act 1998* (Tas). She also claimed that the delivery driver's conduct in sending the defamation concerns notice constituted victimisation in response to her complaint of sexual harassment, in contravention of section 18 of that Act. The Tasmanian Anti-Discrimination Tribunal found for the complainant on the allegation of sexual harassment, awarding her $25,000. While the Tribunal did not uphold the victimisation claim, it awarded an additional $20,000 in aggravated damages, principally because of the 'sending of the defamation letter', which had a 'profound' effect on the complainant's mental health.[180]

5.34 In light of these issues, the DWP is seeking views on whether absolute privilege should be extended. The MDPs could be amended to extend absolute privilege to complaints of unlawful conduct made to employers, and to persons engaged by the employer to investigate allegations of misconduct, such as allegations of sexual harassment or unlawful discrimination.

---

174 See e.g. s 50 *Anti-Discrimination Act 1977* (NSW).

175 See e.g. s 94 *Sex Discrimination Act 1984* (Cth).

176 See e.g. s 50 *Anti-Discrimination Act 1977* (NSW).

177 See e.g. s 210, *Industrial Relations Act 1996 (NSW)*. For an example of a victimisation claim arising out of a threat of defamation by a defendant in an employment discrimination context, see *Narda Tapia v Lagoon Seafood Restaurant* [2003] NSWIRComm 341 (disability discrimination).

178 For examples of victimisation claims arising out of threats of defamation by a defendant in the context of discrimination tribunal proceedings concerning alleged sexual harassment, see *Orchard v Higgins* [2020] TASADT 11; *Saje and Cohen* [2018 WASAT 102; *Bernard v Manly Lawn Tennis Club Ltd* [2006] ADT 225; *S v J and NJ and WR* [1997] QADT 24.

179 *Orchard v Higgins* [2020] TASADT 11.

180 *Orchard v Higgins* [2020] TASADT 11 at [323].

Complaints to professional disciplinary bodies

5.35 Professional disciplinary bodies are bodies that can receive complaints and investigate the conduct of an individual in a particular profession through disciplinary proceedings. These bodies are organised by profession, for example, the Council of the Law Society of New South Wales or the Queensland Legal Services Commission investigate complaints about legal professionals in their respective states, and the Medical Board of Australia investigates complaints about medical practitioners. Many professional disciplinary bodies have authorising legislation that provides penalties for providing false or misleading statements or documents.[181]

5.36 Where a complaint is made to a professional disciplinary body with quasi-judicial functions, a common law absolute privilege defence is likely to apply to the complaint.[182] However, there may be some uncertainty as to whether an absolute privilege defence applies to all professional bodies to which a complaint may be made, or to all communications which are related to the investigation of the complaint.[183] Again, if absolute privilege does not apply, the complainant would need to rely on a qualified privilege defence, or other available defences, if sued for defamation.

5.37 As noted above, some professional disciplinary bodies in NSW are covered by absolute privilege as they are included in Schedule 1 to the *Defamation Act 2005* (NSW). However, there is no uniformity between the application of absolute privilege between different professional disciplinary boards and between jurisdictions.

5.38 The DWP is seeking views on whether it would be desirable to introduce uniform absolute privilege for complaints to all professional disciplinary bodies.

Risk of false or malicious complaints if absolute privilege is extended

5.39 A key consideration is protection against false or malicious complaints. Unlike with reporting criminal matters to police, where it is a criminal offence to make a false statement or false report, it is not a criminal offence to make false or malicious statements about conduct made to an employer or professional disciplinary body, except to the extent that rarely used criminal defamation or libel laws may apply.[184] As noted above, some professional disciplinary bodies do impose penalties such as fines for false statements or false documents.[185]

---

181 See e.g., Schedule 5, Part 2, ss 20 and 21 of the *Health Practitioner Regulation National Law Act 2009* (Qld).

182 See e.g. *Hercules v Phease* [1994] 2 VR 411 (complaint to Law Society of Victoria by client of solicitor was subject to absolute privilege).

183 See e.g. Medical Practitioners Board of *Victoria v Mann* [2000] VSCA 89 (communication to complainant advising that the Medical Practitioners Board of Victoria would not further investigate a complaint not subject to absolute privilege).

184 Criminal defamation or criminal libel remains in the laws of Australian states and territories, but prosecutions are very rare, see Rolph, at [146] Chapter 4.

185 See e.g. Schedule 5 Part 2, ss 20 and 21, *Health Practitioner Regulation National Law Act 2009* (Qld).

5.40 This lack of protection is a serious issue. If a false or malicious complaint is made about an individual and absolute privilege applies, that individual will have no recourse to protect their reputation under defamation law. Qualified privilege on the other hand does not provide a defence for false or malicious complaints as the defence is defeated by malice.

5.41 Given the great variety of types of employers, it may be challenging to find an adequate safeguard against false or malicious complaints if absolute privilege were to apply. If there is no reliable means to safeguard against false reports, absolute privilege might be unsuitable in this circumstance.

5.42 For professional bodies, the introduction of new fines and penalties, or the reliance on existing fines and penalties in authorising legislation, may be a sufficient protection. However, further consideration of whether these penalties are effective at deterring false statements or complaints would be needed.

Question 21: Absolute privilege for reports to employers and professional disciplinary bodies

(a) Should absolute privilege be extended to complaints of unlawful conduct such as sexual harassment or discrimination made to:

  i. employers, or to investigators engaged by employers to investigate the allegation?

  ii. professional disciplinary bodies?

(b) If so, to what types of unlawful conduct should be included providing this protection?

(c) If yes to a), what is the best way of amending the MDPs to achieve this aim (for example, by amending clause 27 and/or by each jurisdiction amending their Schedule 1)?

(d) Are there sufficient safeguards available to prevent deliberately false or misleading reports being made to employers or professional disciplinary bodies? If not, what additional safeguards are needed?

Appendix A

Overview of the UK notice of complaint procedure for website operators with LCO proposal comparison