Review of Model Defamation Provisions
c/o Policy, Reform and Legislation, NSW Department of Communities and Justice
By email: defamationreview@justice.nsw.gov.au

May 31, 2021

Dear Defamation Working Party members,

The Digital Industry Group Inc. (DIGI) welcomes the opportunity to provide a submission to the Council of Attorneys-General (CAG) Defamation Working Party (DWP) on the Review of Model Defamation Provisions – Stage 2 Discussion Paper (Discussion Paper).

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia, with Google, Facebook, Twitter, Verizon Media and eBay as its founding members, and Redbubble, Change.org and GoFundMe as its associate members. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

In order for Australia to be a country where technology companies of all sizes can grow and Internet users can access the world's best digital products and services, we need legal protections and certainty for online intermediaries that host content authored by other people. Today, the Internet is where people share opinions and ideas, connect with others and access information; this free exchange is a crucial part of Australian democracy, and the ability for Internet companies to enable this speech must be protected.

In this submission, we provide our position in relation to four key aspects of the Discussion Paper:

1. the categorisation of Internet intermediaries;
2. the way in which liability for publication is attributed to Internet intermediaries;
3. the need for a safe harbour protection for Internet intermediaries in Australia, and the need to revise the innocent dissemination defence to accurately reflect online forms of publication;
4. the need for a uniform and clear complaints handling regime for allegedly defamatory content published online.

We look forward to further engaging in this reform process. Should you have any questions or wish to discuss any of the representations made in this submission further, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director
Digital Industry Group Inc. (DIGI)

1 Modernisation of provisions for the digital world

DIGI supports the proposal to revise the Model Defamation Provisions (MDPs) to reflect the realities of publication in a digital world. At present, liability of Internet intermediaries for publication of defamatory matter online is uncertain and unworkable in light of the reality of online technology.

The Discussion Paper does not propose the inclusion of a definition of 'publisher' in the MDPs as part of the strategy 'to address the question of internet intermediary liability for third-party content'.[1] The Discussion Paper contends that the common law is better able to 'respond to new technological developments' than a statutory definition.[2] In the absence of a clear statutory definition of 'publisher', and with the current common law position as to what constitutes a primary or secondary publisher in relation to content published online remaining unsettled and unclear, it is DIGI's view that what constitutes an internet intermediary should be framed with precision, as discussed in 2.1 below. In turn, legislative certainty as to the defences available to internet intermediaries, as discussed in 4, must also be clearly framed in the MDPs.

We set out below the key areas in which we consider reform is needed. Best practice policy principles would suggest the definitions in the legislation would be more enduring if they were based on the role that internet intermediaries play and the level of editorial control they can have, rather than basing the definitions based on the current nature of the service provided.

[1] Attorneys-General, 'Review of Model Defamation Provisions – Stage 2' (Discussion Paper, Communities & Justice, NSW Government, April 2021) 47, 3.88 ('**Discussion Paper**').
[2] Ibid, p 17, 2.11.

2 A proper consideration of control over type

2.1 Categorisation of Internet intermediaries

DIGI welcomes the DWP's proposal to consider the responsibility and liability of Internet intermediaries for defamatory publication in relation to the role and function of the intermediary. However, the definitions proposed by the Discussion Paper which differentiate solely between basic Internet services, digital platforms and forum administrators, are problematic as this delineation does not contemplate the complexity and variety of Internet intermediaries.

DIGI encourages the DWP to consider further delineating of services beyond these three categories, including a typology that more clearly distinguishes different types of intermediaries; for example, search engines, cloud services, social media or video-sharing services are all fundamentally different services. Laws should accommodate relevant differences between platforms and should be written in ways that address the underlying issue rather than focusing on existing technologies or mandating specific technological fixes. DIGI and its members would be happy to provide further input on specific definitions and corresponding differing liability frameworks.

2.2 Content neutrality and algorithm participation

The Discussion Paper incorrectly asserts that internet intermediaries that use algorithms have a greater level of control over the contents of defamatory material, solely because of the use of algorithms. This misunderstands the role that algorithms play in distributing content, and the limited level of control that internet intermediaries have over whether specific content is defamatory or not.

DIGI contends that whether an Internet intermediary is 'content neutral' should be considered as a factor in determining liability for defamatory material for both basic Internet services and digital platforms, rather than solely for basic Internet services. The Discussion Paper currently only describes basic Internet services as 'content neutral'.[3] The corresponding characterisation of digital platforms as 'push[ing] out user-generated content through rankings usually managed by algorithms'[4] is problematic. This is because the distinction between content neutrality and algorithms suggests that these features are opposites and that the promotion of material through algorithms cannot occur by an intermediary on a neutral basis. It also ignores the functioning of algorithms as they relate to the neutral indexing of all types of online content within, for example, a search engine.

For this reason, DIGI finds the ACCC Digital Platforms Inquiry definitions of digital platforms that are cited in the Discussion Paper to be problematic, which considers these platforms as 'considerably more than mere distributors or pure intermediaries of the news content in Australia'.[5] This assessment is based on an assumed "active" role of all digital platforms in 'selecting, evaluating, ranking and arranging content',[6] and also does not take into account the different categories of digital platforms in existence, the distinct ways in which they operate and are used and the degree of control that they have over different types of content.

---

[3] Ibid 33, 3.27.

[4] Ibid 33, 3.27.

[5] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final report 2019,* 170 cited in Discussion Paper 37, 3.47.

[6] Discussion Paper 37, 3.47.

DIGI's position is that the use of algorithms does not prevent a digital platform from still acting as a 'mere conduit'[7] or in a way which is 'content neutral''.[8] DIGI strongly disagrees with the proposition in the discussion paper that curation, whether by human or algorithmic means, can negate passivity and neutrality. Automation does not equate to the more "active role" that is ascribed to it by the Discussion Paper and digital platforms should not be solely defined by use of an algorithm. For example, ranking or prioritisation algorithms simply sort material for users in order of material they think are most likely to want to see. Ranking or prioritisation algorithms do not introduce new material to the overall inventory, and are used by a wide array of digital services, from social media feeds to email inboxes.

As such, DIGI disagrees with the Discussion Paper's proposition that the liability of digital content aggregators for publication should depend on the 'extent to which they manipulate and spread the information they collate, including through algorithms that promote certain types of content'.[9] Given algorithms operate at scale, the amplification of content through algorithmic means should not increase liability of Internet intermediaries for content posted by a third party originator (**originator**). This would also be inconsistent with the existing operation of defamation law: a newspaper's liability for a defamatory claim does not change depending on whether the claim was printed on page 1 or page 8. The key question should be the level of editorial control in making the claim, as is currently recognised in the distinction between primary and secondary publishers.

Furthermore, it is unclear from the examples given in the Discussion Paper when functions of Internet intermediaries will be considered to possess the relevant passivity and content neutrality to be considered a basic Internet service, as opposed to a digital platform. For example, the Discussion Paper categorises 'email services'[10] as an example of a function which could be considered a basic Internet service[11] but not instant messaging, which is considered to be the function of a digital platform.[12] DIGI is uncertain as to why there should be a difference and contends that many of the intermediaries encompassed under the third layer of Riordan's taxonomy are still defined by passivity and neutrality.[13]

2.3 Interaction with BSA

Currently under the *Broadcasting Services Act* (**BSA**), Sch 5, cl 91, certain 'Internet service providers'[14] and 'Internet content hosts'[15] are afforded protection from liability. Specifically, Internet service providers and Internet content hosts can rely on cl 91 as a defence where they were not aware of the nature of Internet content and where a service provider or content host would be required to monitor, make inquiries about or keep records of Internet content.[16]

DIGI contends that the MDPs need to consider the interaction of cl 91 with the reforms to determine when and how basic Internet services fall within the definitions of 'Internet service providers'[17] and 'Internet

[7] *Byrne v Deane* [1937] 1 KB; 818, *Bunt v Tilley* [2007] 1 WLR 1243; *Google Inc v Duffy* [2017] SASCFC 130.

[8] Discussion Paper 33, 3.27.

[9] Ibid 38, 3.53.

[10] Ibid 35, 3.4.1.

[11] Ibid 35, 3.4.1.

[12] Ibid 40, 3.63

[13] Ibid 36, 3.43.

[14] *Broadcasting Services Act ('BSA') 1992* (Cth) cl 3 definitions: 'person who supplies or proposes to supply an Internet carriage service to the public'.

[15] Ibid cl 8: 'person who hosts Internet content in Australia, or who proposes to host Internet content in Australia.

[16] Ibid cl 91(1)(a) and (c).

[17] Ibid cl 3 definitions.

content hosts'[18]. As they stand, and as acknowledged by the Discussion Paper, these latter definitions are limited in their utility as they are 'unclear' and 'may not cover search engines'.[19] DIGI's Stage One Submission noted these issues, outlining how cl 91 does not clearly include search engines and how the protection is lost once the service provider is made aware of the Internet content in dispute.[20]

The position in regards to categorisation which is reached under the MDPs should be reflective of the *BSA* to avoid new terms like 'basic Internet services' and 'digital platforms' furthering the current lack of clarity about the protection afforded to certain intermediaries. Similarly, the definitions in the *Online Safety Bill 2020* (Cth) as to 'internet service providers' and 'hosting services' need to be considered in the framing of the amended legislation to promote consistency.

2.4 Application to new technologies

The Discussion Paper recognises the need for the MDPs to encompass 'technological innovation and the emergence of new online services and activities' and is seeking to ensure the longevity of the reforms'.[21] It states 'the reforms will focus on functions rather than type of Internet intermediaries, to ensure defamation laws can adapt as technological advances are made'.[22] DIGI's proposed approach to categorisation, that behaviour of intermediaries be the focus in determining liability rather than consideration of their type alone, would allow the MDPs to be more easily applied to new technologies as they develop. While terms may become outdated, determining scope of liability based on conduct would provide defamation law provisions with greater possibilities of enduring.

3 Responsibility for Defamatory Content

3.1 Liability to content originators not intermediaries

DIGI's position is that amendments are required to the MDPs to ensure that Internet intermediaries are not treated the same way as originating publishers for third-party content. The Discussion Paper recognises that the responsibility of an individual or organisation that creates content in the first place 'is not in question'.[23] However, the Discussion Paper subsequently suggests that a justification for Internet intermediaries having responsibility in defamation law for the publication of third party content is that they often have a business model which 'profits from the network effects'.[24] DIGI rejects this premise on the basis that it is also in its business model interests to create a safe, trusted environment as there is no profit to be made from hosting defamatory content.

It is important to recognise that Internet intermediaries are often not in the same position as the originator of content to delete or edit the originator's content. Similarly, an intermediary is not in the same position as an originator to defend a potentially defamatory statement. For these reasons, DIGI contends that it is appropriate for liability for content to remain with originators. To reflect the practicalities of dissemination of defamatory matter through Internet infrastructure, Internet intermediaries should not be considered

[18] Ibid cl 8.
[19] Discussion Paper 31, 3.20.
[20] Digital Industry Group Inc., Submission to the Council of Attorneys-General's Defamation Working Party, *Review of Model Defamation Provisions,* 14 May 2019, 13 [17].
[21] Discussion Paper 29, 3.10.
[22] Ibid.
[23] Ibid 15, 2.4.
[24] Ibid 15, 2.6

publishers unless and until the intermediary is on notice of the content, unless the intermediary created the content concerned. Whether an intermediary is considered to have been put on notice of an originator's publication should depend on the intermediary's awareness of the potentially defamatory nature of the material. The circumstances in which such awareness, and thus liability, should be attributed to an intermediary (rather than resting solely with the originator) should be dealt with through the legislative reform proposed in Part 4.

3.2 Legislative change to respond to common law deficiencies in protecting Internet intermediaries who are not originators

Under the common law, Internet intermediaries are responsible for publication by reason of having provided a platform for use by content originators, over which they may retain some element of control. DIGI contends that legislative change, as outlined below in Part 4, is required to alter the common law and protect Internet intermediaries from being automatically liable for publication in circumstances where it is more appropriate for sole responsibility to lie with the originator.

Currently in Australia, publication occurs once a publisher makes defamatory matter available to a third party for their comprehension.[25] The test as to the requisite mental element for publication is set out in *Webb v Bloch,*[26] in which a person was considered to have published defamatory material '*if he has intentionally lent his assistance to its existence for the purposes of being published*'.

The Court of Appeal in *Voller*[27] took a similar approach in relation to media companies which operated Facebook pages. The fact that media companies operated a Facebook page on which a third party could post any material was considered sufficient to constitute intentional publication by the media companies in question. The Court of Appeal found that the media companies should have operated a screening or filtering function before comments were made public, to mitigate risk of being liable for defamatory matter posted by third parties, despite such a function not being available on the relevant platform. It is to be noted that *Voller* is currently the subject of an appeal to the High Court, where it is likely that the High Court will provide clarity as to the meaning of publication, including whether it is a question of strict liability as set out in *Lee v Wilson*: '*[a publisher's] liability depends upon mere communication of the defamatory matter to a third person. The communication may be quite unintentional, and the publisher may be unaware of the defamatory matter.*'[28]

Many defamation experts have commented that that *Voller* was an unexpected or "curious" decision and consequently that greater certainty is required as to the circumstances when an Internet intermediary's intention, knowledge and awareness will render them liable for publication, as proposed in part 4. Currently, the above unsettled common law principles are unclear as to whether the relevant behaviour which should attract liability (under a conduct over type categorisation) requires some degree of intention or is based on strict liability. The MDPs should be amended to resolve this uncertainty.

---

[25] *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575.

[26] (1928) 41 CLR 331 (Isaacs J).

[27] *Fairfax Media Publications Pty Ltd v Voller* (2020) 380 ALR 700.

[28] (1934) 51 CLR 276, 287.

4 Protections and Defences

Legislative reform is needed to provide certainty as to what defences are available to Internet intermediaries in response to claims of defamation. Ideally, a safe harbour protection will be introduced into legislation which exempts Internet intermediaries from liability for defamatory content posted by an originator using an Internet intermediaries technology or platform, in circumstances where that intermediary is not aware of the potentially defamatory nature of the content. This safe harbour provision should apply to Internet intermediaries, which should be clearly and broadly defined, who did not create the content complained of and do not have knowledge that the content is indefensibly defamatory.

The development of the common law in relation to the liability of Internet intermediaries for publication of content posted by originators, is proving inadequate in providing certainty to intermediaries and in balancing the right to one's reputation with the protection of free speech. Findings as to liability of Internet intermediaries are disparate in Australia, and do not align with the position taken in other common law jurisdictions.

4.1 Safe harbour

DIGI supports the adoption of a safe harbour defence which contemplates that where an action is brought against a website operator (for example an operator of an online forum, blog site, social media site, online marketplace or a site which facilitates the posting of user-generated video content) in respect of an allegedly defamatory statement posted on the website, a defence will be available for the Internet intermediary if it shows that it did not post that statement itself. However, an Australian safe harbour regime should recognise the significant practical shortcomings experienced under the current model of section 5 of the *Defamation Act 2013* (UK) (**UK Act**).

Section 5 of the UK Act provides a defence to defamation for the operator of a website, if the operator can establish that (1) they did not post the statement, and (2) that on receipt of a notice of complaint they correctly followed a regulated procedure for taking down the content.[29] The UK defence will be defeated if the complainant shows that it is not possible for the complainant to identify the person who posted the defamatory statement, despite seeking the assistance of the intermediary, or if a notice of complaint has been provided to the intermediary, and the intermediary fails to respond to the notice of complaint in accordance with the regime set out in the corresponding Regulations.[30]

While the lack of judicial interpretation of section 5 by UK courts limits this paper's ability to consider the operation of the defence, DIGI's analysis of the defence is that it creates confusion and uncertainty in practice, due to labyrinthine procedures set out under the Regulations, which place a disproportionate administrative burden on website operators. For example:

- The Regulations provide extremely short time periods within which intermediaries must undertake tasks which are both time consuming and demand considerable resources. This includes a period of just 48 hours within which an intermediary must review the initial complaint, and either identify irregularities and respond to the complainant, or identify the originator and seek their response. On receiving an originator's response, an intermediary has just 48 hours within which to determine whether the information provided is genuine.

[29] *Defamation Act 2013* (UK) s 5; *Defamation (Operators of Websites) Regulation 2013* (UK).

[30] *Defamation (Operators of Websites) Regulation 2013* (UK).

- The Regulations also provide that at a complainant's request, an intermediary must anonymise their complaint before seeking a response from the originator, requiring the originator to respond without being able to determine whether the complainant truly has any legal basis for their complaint.
- In certain circumstances, such as where the intermediary cannot identify the originator within 48 hours, or where the originator does not respond with all required information within 5 days, the Regulations facilitate the removal of content without any consideration of whether the content is defamatory. The requirement that content be removed because of failure to comply with very short timeframes, even where the relevant parties have made efforts to do so, poses concerns for freedom of expression.
- Further, the Regulations afford a complainant an additional period to remedy defects in their complaint, where the intermediary notifies them within 48 hours of receiving the complaint, but does not extend this to originators responding to a complaint. If the originator fails to provide a response that addresses all requirements within the prescribed period, there is no opportunity for them to remedy their response. Rather, the Regulations provide that the matter complained of is to be removed.
- Particularly as many Internet intermediaries are global in nature, there is uncertainty in relation to time zones and how this impacts the 48 hour and other stipulated time zones in the defence. There is also uncertainty in relation to weekends and public holidays, which also differ for the claimant and platform if they are not situated in the same time zone.

The challenges of the section 5 defence are exemplified by the lack of judicial consideration since its introduction in 2013: many website operators prefer to avoid the impractical procedures set out in the Regulations in respect of the section 5 defence, instead relying on the existing defences, where such defences are required. An Australian defence modelled on the section 5 defence would prove equally challenging.

DIGI makes the following comments regarding the form of a safe harbour provision to be introduced in Australia:

- It is appropriate that a safe harbour defence in Australia include a process by which Internet intermediaries can be notified about content that is allegedly defamatory. However, DIGI contends that rather than requiring a prescribed complaints process which requires Internet intermediaries to dedicate considerable resources to developing and managing such a process, the defence could be available where the intermediary establishes that it was not responsible for publishing the content in question, and that its conduct in dealing with the complaint was reasonable in the circumstances. In assessing reasonableness, factors to be considered would include, for example:
    - the intermediary's complaints handling process, including the time within which the intermediary responded to the complaint; and
    - the nature of the complaint, including the means by which the complaint was communicated to the intermediary, the information provided, and the seriousness of the content complained of.
- Immunity should not be limited to only those services which do not involve algorithmic or human curation in the dissemination of content (the passivity/neutrality concept considered in the Discussion Paper is problematic, see section 2 above).
- The provision should address the shortcomings of the current defence available under Schedule 5 of the BSA*,* in that it should be made clear to which Internet intermediaries the safe harbour mechanism is available. Currently Schedule 5 of the BSA does not specify which Internet

intermediaries may have the protections afforded to an “Internet content host”. An adequate safe harbour regime needs to make its application clear.

The above procedures do not preclude an online intermediary from determining its own content standards about how it responds to complaints about material that is alleged to be defamatory, false, or harassing. Safe harbour protections would simply offer a level of legal certainty about an intermediary’s legal position and exposure to liability, including when triggered by actual notice.

4.2 Innocent dissemination

The law in Australia is unsettled as to whether Internet intermediaries have the benefit of the defence of innocent dissemination in relation to online publications. In its present form, the innocent dissemination defence has shortcomings in its application to the Internet and in particular, to social media, due to the immediacy with which content is published online without an editorial process.[31] The availability of the defence to Internet intermediaries requires clarification as to what will constitute knowledge, or constructive knowledge, of the defamatory matter for the availability of the defence to be lost. The burden on the Internet intermediary to establish that it was not aware that the content was defamatory is high.[32] The approach adopted in some jurisdictions that Internet intermediaries will have constructive knowledge of the defamatory nature of third party content published in search results, or on digital platforms, as soon as the intermediary is made aware of its existence, is inappropriate. Such an approach risks stifling freedom of speech and does not appropriately consider the way in which digital technologies work and the immediacy with which publication takes place.[33]

Ideally, the statutory mechanisms proposed at 4.1 above will remove the need for Internet intermediaries to rely on the defence of innocent dissemination, as liability will be clarified at the commencement of a cause of action, reducing costs and enhancing certainty. This is because a safe harbour regime will limit the circumstances in which an Internet intermediary, who does not hold the requisite degree of knowledge of publication of the defamatory matter, will be found to have participated in the publication to give rise to liability.[34]

However, if an Internet intermediary loses the protection of a safe harbour defence, the innocent dissemination defence as drafted does not translate to the way in which content is published in a digital age; Rather, it is tailored to a traditional publishing hierarchy in which editorial filters exist, and does not appropriately consider content neutral Internet intermediaries. In relation to digital platforms, publication by a user is instantaneous through automated technology provided by the Internet intermediary. The current defence should be revised to:

- provide clarity as to which Internet intermediaries would be considered ‘subordinate distributors’. The default approach should be that digital platforms are not primary distributors;
- provide clarity as to the extent of knowledge required of an Internet intermediary, before it loses the benefit of the defence.

The defence should be available based on the behaviour and knowledge of intermediaries, rather than based on the type of intermediary; for example, the defence should explicitly apply to Internet

[31] See *Murray v Wishart [2014] 3 NZLR 722; Google Inc v Duffy [2017] SASFC 130; Tamiz v Google [2013] 1 WLR 2151; Metropolitan International Schools v Designtechnica Corporation [2011] 1 WLR 1743.*

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

[33] See *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.

[34] *Defamation Act 2005* (NSW) s 32(1).

intermediaries including social media services, search engines, digital content aggregators and messaging services. The scope of the defence's application should be clearly articulated in the MDPs.

5 Complaints

DIGI supports the notion of Internet intermediaries having clear procedures to respond to requests from complainants. However, DIGI is concerned about the introduction of a prescriptive complaints process modelled on the UK Act, for the reasons discussed in section 4.

Should a uniform complaints procedure be introduced, DIGI's position is that it should include:

- a preliminary requirement that the complainant takes demonstrable steps to identify and contact the originator of the content before issuing a complaints notice. These steps could include contacting the originator directly through for example, the originator's relevant social media page or advertised email address or messaging service. The intermediary could assist with this process if the complainant can demonstrate that they have taken all reasonable steps to identify and make contact with the originator of the content and have been unsuccessful in doing so. It is recommended that the complainant include in the complaints notice the steps they have taken to seek to resolve the issue with the originator prior to lodgement; and
- a reasonable time period within which an Internet intermediary is required to respond to a complaint which factors in the administrative requirements involved in this process for an Internet intermediary. The difficulty of meeting the short timeframes associated with the steps in the complaints process as set out in the UK Act, whilst handling the large volume of complaints often received by larger website operators, and time differences associated with operations of multinational companies being spread across multiple jurisdictions, means that website operators' compliance with these procedures is, in reality, exceedingly difficult and burdensome and often unworkable.

In addition, DIGI does not support the current UK Act model which effectively places the onus on the intermediary to remove the content. This risks hindering freedom of expression, as content is required to be removed by the intermediary to mitigate liability, when that content may not in fact be defamatory of the complainant. The Internet intermediary will very rarely be in a position to determine if the material complained of is defamatory. The risk of non-defamatory material being captured is high, as is the possibility of the complaints mechanism being overused by complainant's who simply do not like content posted. This is important when we consider that defamation claims can be made with purpose of silencing whistleblowers or victims of sexual harassment whose goal in posting content online is the pursuit of advocacy, meaning the act of content removal on the part of the intermediary can have serious consequences in such examples. DIGI supports a complaints notice which does not create an obligation on the Internet intermediary to remove the content complained of while the originator is being contacted. The originator is in the best position to justify any statement complained of; without the cooperation of the originator, who is highly unlikely to be forthcoming given there is no relationship between the intermediary and the originator which would incentivise the originator to assist, the Internet Intermediary is unable to justify or determine the accuracy of the statement.

Clarity is also required as to the way in which a complaints notice will interact with a concerns notice as prescribed in the MDPs. It is not clear whether a complaints notice is a preliminary step to a concerns notice, for the purpose of a complainant accessing contact information of an originator from an Internet intermediary, or if it is lodged at the same time as a concerns notice, or is intended to function as a concerns notice itself. DIGI supports a complaints notice process which is a prior step to the issue of a

concerns notice, rather than allowing both a complaints notice and a concerns notice to be lodged simultaneously.

A further area of concern for DIGI is the potential overlap between the complaints process proposed by the Discussion Paper and the *Online Safety Bill 2020* (Cth) adult cyberbullying scheme. Part 3 of the Bill provides a complaints system for cyber-abuse material targeted at an Australian adult, enabling that person to make a complaint to the e-Safety Commissioner, which the Commissioner may then investigate (clause 31). Part 7 of the *Online Safety Bill* outlines how the provider of a social media service, relevant electronic service, designated internet service or host may be given a removal notice, requiring them to remove specified material. It is unclear the extent to which this process will interact with the proposed complaints process contemplated by the Discussion Paper in relation to allegedly defamatory material.

DIGI's position is that clearer delineation is required between the complaint's process in the *Online Safety Bill* and the complaint's process contemplated by the Discussion Paper, so as to avoid administratively burdensome obligations and the duplication of obligations on internet intermediaries under the two regimes. The approach adopted for a complaints procedure should consider the process under the *Online Safety Bill* and the existing process for concerns notices, to avoid administrative duplication and confusion. Ideally, if a complainant has submitted a complaint under the *Online Safety Bill* complaints mechanism, it should not be permitted to lodge a duplicate complaint under the MDPs complaints procedure. DIGI recommends that a complainant be required to elect to lodge its complaint under either the MDPs complaints process or the *Online Safety Bill* process.