Defamation Taskforce
Attorney-General's Department
By email: defamation@ag.gov.au

Friday January 21, 2022

Dear Defamation Taskforce members,

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on the *Social Media (Anti-Trolling) Bill* 2021 ('**the Bill**') as advanced in the Exposure Draft.

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, eBay, Google, Linktree, Meta, Twitter, Snap and Yahoo, and its associate members are Change.org, Gofundme, ProductReview.com.au and Redbubble. 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.

DIGI shares the Commonwealth Government's strong commitment to keeping all Australians safe from online harm, including the harm that can occur from cyberbullying, trolling and defamation. Our members have extensive complaints handling processes in place for cyberbullying, trolling and defamation complaints received by Australian users, which are actioned in accordance with both their policies and Australian law.

DIGI supports the need for legislative reform in relation to liability for publication online, following the High Court's decision in *Fairfax Media Publications Pty Ltd v Voller; Nationwide News Pty Limited v Voller; Australian News Channel Pty Ltd v Voller* [2021] HCA 27 ('***Voller***'). However, clarifying the law as it relates to online publication is a process that cannot be rushed and requires significant consideration, including consideration of existing law affecting this area and reviews occurring at a state level. In particular, DIGI notes the work of the Meeting of Attorneys-General in conducting the 'Stage 2' defamation law reform process, which addresses issues relating to digital platforms. It is useful to consider what mechanisms could be introduced in this area paying particular attention to the issues the Bill intends to address.

We believe there is considerable overlap between the mechanisms proposed by the Bill, and those under consideration in the Stage 2 Review. The Stage 2 Review is at an advanced stage, and well-placed to take into account the operation of existing state laws and recent reforms in this area. DIGI welcomes the opportunity to set out, in this submission, comments and suggestions regarding the Bill, but considers that it is prudent to await the results of the Stage 2 Review before taking further steps in relation to the Bill. However, if the Government is intent on progressing the Bill through parliament at this stage, as there are a number of novel features in the Bill's approach, at a minimum we would request a more extensive review than is being afforded by the public consultation process, perhaps through a committee process.

In the context of those overarching recommendations, this submission focuses on the following key aspects of the Exposure Draft:

1. the importance of addressing "vulgar abuse" online;
2. the proposed assignment of responsibility for publication of online defamation claims;

3. removal of the availability of the innocent dissemination defence for social media service providers;
4. the uncertainty and practical shortcomings for social media service providers in light of the current mechanisms set out in the Exposure Draft;
5. the interaction of the proposed complaints mechanism in the Exposure Draft with existing Australian laws and international regimes.

We thank you for your consideration of the matters raised in this submission. Should you have any questions, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director, DIGI
sunita@digi.org.au

Table of contents

Part 1: Introduction

1. The intention of the Bill

1.1. DIGI shares the Commonwealth Government's strong commitment to keeping Australians safe from online harm, including the harm that can occur from anonymous trolls spreading defamatory material online.

1.2. DIGI also supports the initiative to legislate following the High Court's decision in *Voller*. The implications of the *Voller* decision are wide-ranging and will most likely result in increased defamation litigation against administrators of social media accounts and those who may not necessarily be responsible for the making of defamatory comments, including individuals and businesses with social media pages.

1.3. However, addressing instances of abuse online, and redefining liability for online publication, are two separate and complex issues of legal liability that should not be conflated.

1.4. The Bill appears to be primarily concerned with defamation complaints and proceedings, and does not reference the act of 'trolling' anywhere except in its title. Courts have long accepted that 'mere vulgar abuse', including trolling, is not defamatory if it fails to reach the standard of seriously harming a person's reputation or diminishing their standing in the community.[1] Confining the Bill's proposed remedies for online 'trolling' to the tort of defamation misunderstands the nature of the cause of action, the elements underpinning it and importantly, the defences available to publishers of allegedly defamatory material. DIGI contends that the Bill does not address online abuse more broadly.

1.5. DIGI submits that there are more effective means by which people can seek a remedy for online trolling, and that defamation proceedings may not be considered the most suitable course of action for many Australians. We discuss this further in **Part 4** below. We also note that the *Online Safety Act 2021* (Cth) (**Online Safety Act**) comes into force in two days' time on January 23 and includes a cyber-bullying scheme where Australian adults or children who are the victims of seriously harmful online abuse can complain to the Office, if the online service providers have failed to act on reports to them. The Office can direct a request for removal to the social media service, and the service must remove the content within 24 hours.

1.6. The Online Safety Act also includes stronger information-gathering powers for the eSafety Commissioner to obtain identity information including basic subscriber information for anonymous accounts, in order to conduct investigations into harmful online behaviour and issue fines and notices[2].

1.7. While DIGI members have strict policies and enforcement to prohibit and rapidly remove cyberbullying, DIGI posits that availing of the schemes under the Online Safety Act may

[1] *Thorley v Lord Kerry* (1812) 128 ER 367, 371 (Mansfield CJ); *Mundey v Askin* [1982] 2 NSWLR 369, 372; *Bennette v Cohen* (2005) 64 NSWLR 81, 97-98 (Bryson JA).
[2] eSafety Commissioner, 'Online Safety Act 2021 Fact Sheet', https://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf

be a more accessible pathway for victims, in the instance that any platform may not address the abuse in the first instance.

2. Addressing *Voller*

2.1. DIGI agrees that the law in relation to liability for publication of defamatory matter requires modernisation for the digital age, particularly in light of the recent decision of the High Court in *Voller*. However, allocating liability for publication to social media service providers ('**providers**') as contemplated in s 14(1)-(2) of the Bill does not address the issues that *Voller* presents, and that the Bill seeks to resolve.

2.2. Potential liability for defamatory third-party comments online should be attributed to page administrators and providers when a page administrator or provider is made aware of the defamatory comment and fails to remove the comment within reasonable time. We discuss this further in **Part 3** below.

3. The proposed complaints mechanism and end-user disclosure orders

3.1. DIGI supports the introduction of a clear complaints regime which clarifies the responsibilities of providers and individuals in handling complaints of defamatory content being posted online. As detailed below at **Part 2**, DIGI submits that it is more effective to introduce this complaints scheme following the Meeting of Attorneys-General's Stage 2 Review of the Model Defamation Provisions ('**MDPs**').

3.2. In the event that the Commonwealth Government does not accept this recommendation, DIGI has set out a range of specific concerns with the complaints scheme and end-user disclosure orders proposed in the Bill, and encourage a more extensive review than is being afforded by the public consultation process, perhaps through a committee process.

3.3. Most notably, DIGI is concerned that the obligations imposed by these mechanisms are unclear and do not appropriately address circumstances where the requisite consent is not provided by a commenter, or where a commenter cannot be located.

3.4. DIGI also holds concerns with the process for compliance proposed in the complaints scheme, and the potential legal conflicts that DIGI's members may face in circumstances where the proposed obligations under the Bill conflict with laws relating to privacy and data in other jurisdictions. DIGI's concerns are set out in **Part 5** below.

Part 2: Stage 2 Review of Model Defamation Provisions

4. Overlap between the Bill and the Stage 2 Review

4.1. DIGI submits that the issues contemplated by the Bill may be better addressed following the Meeting of Attorneys-General's Stage 2 Review of the MDPs. DIGI acknowledges that the intention of the Commonwealth Government is for the Bill to complement State defamation reform, however DIGI is concerned that there is considerable overlap between the mechanisms proposed by the Bill and those under consideration in the Stage 2 Review:

a) Part A of the Stage 2 Review addresses the question of internet intermediary liability in defamation for the publication of third-party content. Notably, the Stage 2 Review has sought feedback on a proposal to amend Part 3 of the MDPs to better accommodate complaints to internet intermediaries (which includes the social media service providers that would be captured by the Bill).[3] It considers the appropriate remedies internet intermediaries can offer to complainants in light of the 'concerns notice' and 'offer to make amends' process provided for in State legislation, including whether a complaints notice should be distinct from a mandatory concerns notice.[4] The operation of concerns notices is not considered by the Bill. However, DIGI submits that this is crucial to ensure a streamlined complaints and notification process that does not place onerous and potentially conflicting legal obligations on providers.

b) The Stage 2 Review also contemplates the introduction of a safe harbour defence subject to a complaints notice process and considers this in light of potential reforms to the innocent dissemination defence.[5] Instead of imposing liability for publication on providers but not page owners as contemplated by s 14 of the Bill, the Stage 2 Review considers how the innocent dissemination defence may be amended to take into consideration the role of page owners and providers in the publication process.[6] As outlined in **Part 5** below, DIGI considers that there are circumstances where the blanket removal of an innocent dissemination defence would result in unfair and unintended outcomes, and submits that there is merit in awaiting the Stage 2 Review's recommendations in this respect.

c) The Stage 2 Review more directly addresses particular features of the complaints notice process, including steps required to be engaged by complainants before initiating the process[7] and whether a complaints notice should include an indication of the serious harm to reputation likely to be caused by the publication.[8] Like the Bill, it suggests the mechanism of court orders to identify originators, however makes reference to countervailing considerations such as privacy and whistle-blower protection.[9] As our submission outlines below, further consideration ought to be given to these issues, particularly in relation to sections 16 and 18 of the Bill. Further, unlike the Bill, the Stage 2 Review considers potential orders to have online content removed.[10]

4.2. DIGI welcomes the opportunity to set out, in this submission, its comments and suggestions in relation to the Bill. However, DIGI is concerned that the Bill proposes similar but not identical mechanisms to those currently under consideration by the Meeting of Attorneys-General. DIGI emphasises that the Stage 2 Review is at an

[3] See, e.g., Discussion Paper, Attorneys-General Review of Model Defamation Provisions – Stage 2 <https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/discussion-paper-stage-2.pdf> p. 51, 67.
[4] Ibid.
[5] Ibid p. 59.
[6] Ibid p. 55.
[7] Ibid p. 68.
[8] Ibid p. 70.
[9] Ibid p. 81.
[10] Ibid p. 77.

advanced stage, and well-placed to take into account the operation of existing State laws. DIGI therefore suggests that it is prudent to await the results of the Stage 2 Review before taking further steps in relation to the Bill.

Part 3: *Voller*

5. The importance of reconsidering responsibility for publication post-*Voller*

5.1. DIGI supports the initiative to legislate post-*Voller.* DIGI accepts that the implications of the *Voller* decision are wide-ranging and will likely result in increased defamation litigation against administrators of social media accounts, including individuals and businesses with social media pages. DIGI acknowledges that the expansion of internet publication and the impact of the *Voller* decision has resulted in the need to reconsider and reallocate responsibility for defamatory comments made online, and also recognises the Commonwealth Government's intention to ensure that social media services play a role in this reallocation of responsibility.

5.2. DIGI submits, however, that allocating liability for publication to providers as contemplated in s 14(1)-(2) of the Bill does not address the issues that *Voller* presents, and that the Bill seeks to resolve. Rather, the simplicity of the approach taken may have counterproductive results.

6. Control over third-party comments

6.1. The Bill seeks to address a key concern arising from *Voller*: that people should not be responsible for the comments of third parties over which they have no *control*. Mandating responsibility for defamatory publication on social media to providers in all instances, however, does little to address this issue of control.

6.2. In confirming that page owners are not publishers of third-party comments in any circumstances (s 14), the Bill discourages those with the ability to moderate comments in real time from engaging in such moderation. A mechanism that encourages the proactive management of comments, through the involvement of page owners and social media services, is more suitable to address the issues that arise from *Voller* and the Commonwealth Government's concerns with the harmful impacts of defamatory online comments on Australians.[11]

6.3. DIGI submits that s 14 of the Bill does not adequately address its intended approach of ensuring that page owners are not responsible for comments made by third parties of which they are not aware. Section 14(1) provides that, where a comment is posted by a third party, an Australian page owner is "not taken to be a publisher of the comment." The Bill does not envisage circumstances in which a page owner becomes aware of a potentially defamatory comment on their page. The effect of this provision not only legislates against the findings in *Voller,* but also has the effect of legislating around extensive case law which provides that, upon notification of a defamatory third-party

[11] *Social Media (Anti-Trolling) Bill 2021: Explanatory Paper,* p. 1.

comment and failure to remove the comment within a reasonable time, a host of such comment is a publisher.[12]

6.4. DIGI shares the Commonwealth Government's concern that the imposition of liability for publication post-*Voller* may have the effect of impinging on free speech, as exemplified in the result of some page owners turning off comments entirely on their social media posts following *Voller*. However, DIGI submits that absolving page administrators from liability for publication altogether is not the best mechanism for addressing these concerns. Rather, liability should accrue where the page owner or provider is made aware of the publication, provided with sufficient information about the complaint, and fails to remove the publication within a reasonable time. This suitably aligns with the mandatory concerns notice process required to commence proceedings under State legislation.

6.5. Such a solution will carefully balance the protection of one's reputation to one's right to freedom of expression, and will amend the law in relation to liability for publication as affirmed in *Voller,* to be workable and appropriate for a digital age. This is also consistent with the maintenance of the innocent dissemination defence, which contemplates circumstances where a defendant had no knowledge as to the defamatory content of a matter and was not the primary distributor or originator of defamatory material, and did not have capacity to exercise editorial control.[13] For further discussion of this issue, see **Part 5**.

Summary of recommendations in Part 3

A. Legislation should be introduced which modernises liability for publication in the internet age.

B. Page administrators and social media service providers should be considered in determining liability for publication, *but only* in circumstances where a page administrator or social media service provider is aware of a defamatory publication and fails to remove it from public view within reasonable time after being notified of its existence.

Part 4: Trolling

7. Guarding against vulgar abuse online

7.1. The Bill posits the tort of defamation as the primary remedy to 'trolling' and online abuse. It is intended that potential victims of defamatory statements can be connected to the person who has made the comments for the purpose of instituting defamation proceedings in the Australian courts.[14]

7.2. However, the Bill's championing of the tort of defamation as the most applicable cause of action to address online trolling is misconceived, and has the potential to lead those

[12] *Byrne v Deane* [1937] 1 KB 818.
[13] *Social Media (Anti-Trolling) Bill 2021: Explanatory Paper,* p. 2.
[14] Detailed Explanatory Notes, p 5.

seeking recourse via its proposed mechanisms down a costly, time consuming and potentially ineffective pathway.

7.3. DIGI submits that there are more effective means by which people can seek a remedy for online abuse under the cyberbullying schemes provided by the Online Safety Act, which enable child and adult victims of online abuse to have content removed within 24 hours.

Misapplication of the tort of defamation

7.4. Confining the Bill's proposed remedies for online 'trolling' to the tort of defamation misunderstands the nature of the cause of action, the elements underpinning it and importantly, the defences available to publishers of allegedly defamatory material. The tort of defamation is founded on the premise that a publication, in this case a comment made on a social media service, has harmed the reputation of the person who is the subject of the comment, held them up to ridicule or led others to shun and avoid them.[15]

7.5. It has long been accepted that 'mere vulgar abuse' is not defamatory if it fails to reach the standard of harming a person's reputation or diminishing their standing in the community.[16] 'Trolling', generally understood to be 'the act of leaving an insulting message on the internet in order to annoy someone',[17] or 'with the aim of provoking responses',[18] would have to satisfy a high threshold of harm and scope in order to give rise to a cause of action in defamation. While harmful to its intended target, trolling may not rise to a level sufficient to give its victim a cause of action in defamation.

7.6. Australian courts in multiple jurisdictions have established that, whilst there is no strict dichotomy between mere vulgar abuse and defamatory comments, mere vulgar abuse will not amount to defamatory conduct without considering the person's existing reputation, the extent of the abusive publication, its subject matter and its impact on an ordinary person's perception of the insulted individual.[19] The Supreme Court of South Australia noted in *Aldridge v Johnston:*

> *'[i]t has become quite common for material to be published, particularly on social media, in an abusive and offensive way. Words can be abusive, vulgar or objectionable without being defamatory. Words might injure a person's pride without injuring his or her reputation.'*[20]

7.7. The distinction between injury to pride, and injury to reputation, is central to the nature of trolling. Trolls ultimately aim to provoke and annoy. Their goal and conduct can be upsetting for the individual subject to the online abuse, but it does not necessarily reach

---

[15] *Radio 2UE Sydney Pty Ltd v Chesterton* [2009] HCA 16, [3], [36].

[16] *Thorley v Lord Kerry* (1812) 128 ER 367, 371 (Mansfield CJ); *Mundey v Askin* [1982] 2 NSWLR 369, 372; *Bennette v Cohen* (2005) 64 NSWLR 81, 97-98 (Bryson JA). State law mandates that the harm to the person's reputation must be "serious harm".

[17] Cambridge Dictionary, 'Definition of trolling', accessed 21 December 2021, <https://dictionary.cambridge.org/dictionary/english/trolling>.

[18] Macquarie Dictionary, 'troll", accessed 12 January 2021, <https://www.macquariedictionary.com.au/features/word/search/?search_word_type=Dictionary&word=trolling>.

[19] *Bennette v Cohen* (2005) 64 NSWLR 81 [51]; *Briscinari v Piscioneri (No 4)* [2016] ACTCA 32 [59]-[62].

[20] *Aldridge v Johnston* [2020] SASCFC 31 [119], citing Patrick George, *Defamation Law in Australia* (LexisNexis Butterworths, 3rd ed, 2017) 218.

the threshold of harming their reputation. The argument that a complainant has failed to establish defamatory meaning is one that is readily available to trolls and will prevent the success of potential defamation proceedings for parties subject to online abuse.

Trolling through the prism of the Bill's proposed complaints mechanism

7.8. The Bill predicates its prescribed requirements for providers' complaints schemes as being applicable:

> '*if a person (**the complainant**) has reason to believe that there may be a right for the complainant to **obtain relief** against an end-user of the social media service (**the commenter**) **in a defamation proceeding** that relates to a comment posted on a page of the service by the commenter (**emphasis added**) (s 16(1)).*'

7.9. DIGI's comments on the specific form of the complaints mechanism are set out in detail in **Part 5** of this submission. More broadly, considering the operation of the mechanism in relation to complaints regarding online trolling, DIGI submits that there are several shortcomings.

7.10. The proposed mechanism is predicated on a complainant having a right to obtain relief. Assessing the likelihood of relief being granted to a complainant is a complex and nuanced task which requires consideration of the nature, scope and broader context of the publication in question. Respectfully, such an assessment is not a simple task. The inherent complexities of defamation law mean that members of the public are not necessarily in a position to determine whether a comment is truly defamatory and has caused them sufficiently serious harm, so as to give rise to a right to relief. Where a person has been the subject of trolling, it may be particularly unclear whether there is a right to relief in defamation. The Bill aims to provide fast and efficient access to recourse for harmful online content; however, it seems victims of trolling may either be unable to rely on the mechanism due to having no right to relief in defamation, or be driven to seek legal advice in order to determine this matter, and incur expenses of doing so.

7.11. It is unclear whether providers are required to accept the complainant's opinion as to whether they have a potential cause of action, or whether the provider is able to make its own assessment as to whether the complainant has a reasonable belief that they may have a cause of action in defamation. DIGI also notes that the Bill would require a provider (with no contextual information about the publication or parties involved) to disclose to a complainant, within a short timeframe, a commenter's email address and phone number. DIGI is concerned that the process may be utilised for improper purposes (for example, to facilitate stalking, or spurious, vexatious or politically motivated complaints and litigation).

7.12. The requirement to inform a complainant of whether a comment was made by a user located in Australia or another country ignores the use of tools such as Virtual Private Networks (VPNs) and other location-masking technologies. Such technologies allow a user to select a location from which their comments appear to be made, reducing the utility of providers disclosing the location from which trolling comments were made. The availability of such technologies is likely to be exploited by those seeking to evade identification.

7.13. In light of these factors, DIGI submits that while the proposed complaints mechanism may provide victims of online trolling with a sense of agency and control, the nature of trolling comments and those who make them mean that in many cases, the mechanism will be of limited use to those victims. By pointing to defamation as the primary means of recourse against online trolls, even where no cause of action in defamation arises, DIGI contends that the Bill may distract from other existing frameworks that provide better recourse for victims of online trolling (discussed further below).

Criminal liability for trolling

7.14. The Commonwealth Criminal Code makes it an offence to menace, harass or cause offence using a carriage service.[21] It also makes it an offence to use a carriage service to make threats to kill or cause serious harm to a person, regardless of whether the person fears that the threat will be carried out.[22] We note that the Australian Government made an election commitment on May 5, 2019 to increase maximum penalties for end-users who use a carriage service to menace, harass or cause offence to five years of imprisonment.[23]

7.15. These criminal offences do not require the more demanding threshold of defamation proceedings and are considerably more responsive to many instances of r 'trolling'; A person subjected to 'trolling' and who feels menaced, harassed or offended by comments made by another social media user may have recourse to criminal provisions which carry a penalty of imprisonment for up to three years.

7.16. DIGI considers recourse to defamation as limited by costs to the complainant and the alleged 'troll' who has made the statements online. Pre-existing criminal provisions provide a more effective means of ending online abuse and 'trolling' by being more accessible to complainants and by directly addressing 'trolling' behaviour.

7.17. DIGI robustly supports measures that respond to online abuse and its victims. However, as noted above, the measures created by the Bill concentrate remedies in the hands of those who have the extensive means and age to access litigation, and lack provisions for people who do not have that access.

8. Role of the Online Safety Act

8.1. The Online Safety Act establishes an extensive framework for dealing with online abuse, cyberbullying and the sharing of intimate images without consent. DIGI contends that the powers of the eSafety Commissioner are far more effective at addressing a broad range of abusive online behaviour than a complaints process available only where abuse

---

[21] *Commonwealth Criminal Code 1995* (Cth) s 474.17.
[22] Ibid s 474.15.
[23] See media release: Prime Minister The Hon Scott Morrison MP, Attorney-General The Hon Christian Porter, Senator The Hon Mitch Fifield Minister For Communications And The Arts, Joint Media Release (05/05/2019), "Keeping Australians Safe Online", accessed at https://www.liberal.org.au/latest-news/2019/05/05/keeping-australians-safe-online
See also transcript: Prime Minister The Hon. Scott Morrison MP (05/05/2019), Transcript Remarks, Campaign Rally Central Coast, accessed via CCH alerts, see quote: *"But the other thing we're going to do for all Australians, is we're going to increase the penalties for those who have been found to be bullying people online, causing those injuries. You won't go to jail for three years you'll go to jail for five years."*

satisfies the elements of defamation. DIGI supports the issuing of take-down notices to social media companies and the authors of abusive material, as well as reliance on the investigative powers of the eSafety Commissioner.

Specific protections for children

8.2. The protection of children from cyberbullying is of utmost importance to DIGI's members. All relevant DIGI members have strict policies to prohibit and rapidly remove the cyberbullying of Australian children and minors. These policies are regularly updated to ensure they reflect emerging patterns of abuse, in consultation with experts.

8.3. They provide reporting tools where content can be reported for cyberbullying. Such messages are reviewed by teams of human moderators, and addressed as quickly as possible. Enforcement actions include the removal of cyberbullying content, and the suspension or removal of accounts that have instigated it.

8.4. This enforcement infrastructure is often complemented with proactive technology detection that detects problematic content and flags it for human review.

8.5. Relevant members provide blocking tools where any user can be blocked from sending further unwanted messages, and provide tools to enable people to leave or hide group forums.

8.6. These policies and enforcement practices are complemented with a range of initiatives, partnerships and social programs aimed at providing minors with wider support from professionals, parents and teachers in relation to cyberbullying.

8.7. The Bill has been positioned as a measure to protect children. In a press conference announcing the Bill in November 2021, Prime Minister Scott Morrison said:

> *As I look around the playing fields today and I watch all of these young kids and their parents out there, we do everything we can as a government and as a society to make sure that in the physical world in which we all live, and in particular in which these children live, they are safe. We need to, and we have been as a government taking steps to ensure that the online world in which these children, that is now their reality, they will live going forward is also a safe space. And that is why I'm very pleased to be here today to announce that the government is going to take further steps to protect Australians, in particular young Australians, online, because that's what we all deserve.*[24]

8.8. While comments and conduct amounting to cyberbullying could be subject to defamation proceedings, and vice versa, DIGI does not expect the Bill to be used by children as a means to protect them from cyberbullying. Obstacles such as costs and difficulties assessing whether comments reach a threshold of defamation, render it particularly difficult for children to rely on defamation as a means of protection online. Further, children would require a litigation guardian and the means to engage in defamation proceedings. Their online abusers are likely to be their peers, who also lack the means

[24] Prime Minister of Australia, 'Transcript, 28 Nov 2021, Canberra, ACT, Prime Minister' (Press Conference, 28 November 2021) <https://www.pm.gov.au/media/press-conference-7>.

and support to engage in any form of litigious solution. It is therefore unclear that the Bill would be an appropriate means of protecting young Australians.

8.9. The *Enhancing Online Safety Act 2015* (Cth) (**EOSA**) allows Australian minors who are the target of cyberbullying material, and those representing them, to complain to the Office of the eSafety Commissioner (the Commissioner). The Commissioner can direct a request for removal to the social media service, and the service must remove the content within 48 hours. The Online Safety Act, which enters into force on January 23, 2022, reduces the timeframes that a social media service must respond to 24 hours.

8.10. The draft Basic Online Safety Expectations (**BOSE**), when finalised, will come into effect with the OSA, and apply to all social media services, messaging services and websites. A core expectation of the BOSE is that a provider of a service must take reasonable steps to minimise the extent to which cyberbullying material targeted at an Australian child or adult is available, and to make reports about the provider's related activities available to the Commissioner.

8.11. The EOSA and OSA children's cyber bullying schemes enable the Commissioner to issue end-user notices that require a person who posts cyberbullying material to remove the material, refrain from posting any cyberbullying material targeting the child, and/or apologise to the child for posting the material. However, to date, DIGI understands that no such end-user notices relating to cyberbullying have been issued.

8.12. The Online Safety Act provides direct and enforceable protections for children using social media services. The Bill risks undermining these protections with a less focused mechanism of litigating online abuse which remains inaccessible to the children it is said to protect.

Duplication of protections

8.13. DIGI contends that the Bill's inclusion of standards with which social media companies must comply in implementing their complaints and reporting mechanisms for online abuse risks conflicting with the measures already provided for under the Online Safety Act. The overlap between these measures risks diluting the overall intention of the Bill and the Online Safety Act to provide efficient, robust mechanisms for addressing, preventing and ending abuse online.

8.14. Under the Online Safety Act, social media services are obligated to adhere to robust complaints procedures and to assist the eSafety Commissioner in the exercise of its take down and information gathering powers. The Bill clearly contemplates interaction with the Online Safety Act. Section 14 of the Bill provides that if a social media service provider is a publisher by virtue of that section, and becomes a party to defamation proceedings, they are prevented from relying on s 235 of the Online Safety Act. Section 235 excludes Australian 'hosting service providers' from liability in various circumstances relating to abusive, inappropriate or sensitive content. The Bill purports to exclude the operation of that section, presumably in recognition of the broad definition of 'hosting service providers',[25] which may capture social media service providers or page owners.

[25] Online Safety Act, s 17.

8.15. The Online Safety Act will commence imminently, and it remains to be seen how it will operate in practice. However, it appears that there is significant overlap between these laws (including in terms of the processes a social media service would need to have in place to respond to complaints of abusive material), but uncertainty with respect to the definitions and language adopted.

8.16. The Bill should carefully consider the appropriate use of language and cohesive obligations on providers, to ensure that there is clarity and certainty in the obligations of providers in order for the mechanisms to be effective in preventing online harm. Such clarity makes compliance easier– particularly for start-ups, smaller challenger companies, and those without a large local staff presence – who may be struggling to make sense of the complex regulatory environment in Australia

Summary of recommendations in Part 4

C. The Bill should clarify the process for determining whether a complainant has a possible cause of action in defamation.

D. The Bill should be consistent with the Online Safety Act and avoid overlapping or conflicting compliance requirements for social media services, particularly as they relate to children and vulnerable users of social media services. This includes removing sections 3(e) and 3(f) of the Bill and revising section 16 to be consistent with the Online Safety Act.

Part 5: Complaints mechanism and end-user information disclosure orders

9. Introduction

9.1. DIGI supports the introduction of complaints mechanism guidelines and court disclosure processes in order to provide further clarity to providers as to the level of assistance to be provided to users who have allegedly been defamed online. As DIGI's submission has detailed, these mechanisms are presently under consideration as part of the Stage 2 Review of the MDPs, and should not be introduced prior to the conclusion of that review. In the event that the Commonwealth Government does not accept this position, this Part sets out specific concerns with the mechanisms as currently contemplated in the Bill.

9.2. DIGI considers that certain aspects of the Bill, including the proposed complaints process under s 16 and the issuing of end-user information disclosure orders under s 18 (together, in this Part, **'the resolution mechanisms'**), require further amendment and particulars, in order to address some uncertainty arising from the current form and scope of the proposed scheme.

9.3. Addressing this uncertainty will enable providers to comply with the resolution mechanisms proposed and to benefit from the safe-harbour defence under the Bill.

10. Collection of contact details and online anonymity

10.1. The Bill applies to 'social media services', defined broadly to encompass interaction between 'two or more end users.' This definition is by no means limited to large, mainstream social media services as it encompasses a wide range of services, such as local and small business community forums, educational forums, business forums, health support forums, and any blogs with comments enabled. For example, the mental health organisation Beyond Blue operates a number of online community forums on topics relating to anxiety and depression where Australians can share their experiences and connect[26].

10.2. The Bill requires a provider to provide the contact details of the commenter in compliance with both the complaints scheme (s 16) and end-user information disclosure orders (s 18). Under either mechanism, the contact details to be provided are the commenter's name, email address and phone number (s 6, definition of 'relevant contact details'). The Explanatory Paper states that the details 'need to be effective to contact the commenter. Details that turn out to be fake will not allow the provider to access the defence' (pp. 4 – 5). The Bill incentivises those services to collect more personal information from their users by offering legal safe harbours if they do so.

10.3. This means that Australians who prefer not to use their real name online or to share their contact details with a very wide range of websites, often for their own safety or privacy, may not always be able to do so.

10.4. Many end-users have valid and important reasons for anonymity. For example, as the Office of the eSafety Commissioner acknowledges, a valid reason for anonymity and identity shielding is to protect users from unwanted contact. The Office encourages children only to use their given name, a nickname or an avatar online instead of a full real name which makes it more difficult for sexual predators and scammers to interact with them[27].

10.5. As acknowledged by the former UN Special Rapporteur for Human Rights David Kaye, the ability for users to remain anonymous online can also be an important means for keeping them safe and promoting human rights[28]. For example, anonymity enables activists to expose repression, corruption and hate and allows stigmatised or marginalised communities to find safety and support when revealing their real-world identity could expose them to harm. As David Kaye recently told a forum in Australia on anonymity:

> *It's been essential to individual human development in repressive societies – the ability to seek information or receive information in a kind of cone of privacy, if we want to think of it like that, under the blanket of anonymity.*
>
> *It has allowed people historically to explore their heritage, to explore their sexual orientation, their gender identity, and we could go on and on, and anybody could come up with examples where a failure of anonymity or publicity of one's persona*

[26] Beyond Blue, *Online forums,* accessed at: https://www.beyondblue.org.au/get-support/online-forums
[27] Office of the eSafety Commissioner, "Anonymity and identity shielding", accessed at https://www.esafety.gov.au/about-us/tech-trends-and-challenges/anonymity
[28] Kaye, David (2015), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Human Rights Council,* accessed at https://www.undocs.org/A/HRC/29/32

might lead to real harm.[29]

10.6. These regulatory proposals to collect additional information run counter to the universally accepted privacy practice of data minimisation. Data minimisation requires goods or service providers to not seek to collect data beyond what is reasonably needed to provide the good or service. Data minimisation that forms part of the existing APPs under the *Privacy Act 1988 (Cth)*[30] (**'Privacy Act'**), and is also a key principle of the Consumer Data Right[31]. We discuss the privacy concerns in more detail below.

10.7. Additionally, DIGI is concerned that a potential increase in data collection for all websites, and the sometimes sensitive nature of the data being collected, will create increased cyber security risks to users of a whole range of websites in Australia.

10.8. In addition to the negative implications for Australians' safety, advocacy, privacy and cyber security, there is evidence that calls into question the correlation between anonymity and online harm. In August 2021, Twitter released an analysis of accounts that were removed or suspended for abuse on its platform in response to the Euro 2020 final, and found that 99% of the accounts suspended were not anonymous and were in fact identifiable[32].

11. Verification of contact details

11.1. In addition to the issues arising from additional information collection, DIGI submits that the process of verifying a commenter's details is a complex one and the current draft Bill places an onerous obligation on providers to verify details, which they may have no means of verifying, or risk losing the benefit of the defence. For instance, it is possible for users of various digital platforms to set up an account with a fake name, even if their email address and phone number are verified. It is also possible to set up an email address for the purpose of registering a social media account, verify that address for the purposes of registering a social media account and subsequently deactivate that address. It is also quite likely that existing and previously registered accounts have provided contact details that are, or may become, out-of-date.

11.2. Where a commenter does not provide consent to disclose their contact details, and an end-user information disclosure order is made under s 18 of the Bill, it may not be a straightforward process to verify that the information the provider has on record is correct. The proposed scheme places obligations on providers that extend well beyond the contemplated scope of holding commenters of defamatory comments to account, imposing an onerous and ongoing obligation on providers to verify the identities of all

[29]Taylor, Josh (5/11/2021), "Twitter says any move by Australia to ban anonymous accounts would not reduce abuse", in *Guardian Australia,* accessed at https://www.theguardian.com/technology/2021/nov/05/twitter-says-any-move-by-australia-to-ban-anonymous-accounts-would-not-reduce-abuse?CMP=Share_iOSApp_Other&s=09

[30] OAIC, *Australian Privacy Principles*, available at: https://www.oaic.gov.au/privacy/australian-privacy-principles, see APP 3 and APP 11.

[31] OAIC, "Chapter 3: Privacy Safeguard 3 — Seeking to collect CDR data from CDR participants", accessed at https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-3-privacy-safeguard-3-seeking-to-collect-cdr-data-from-cdr-participants/

[32] Twitter (10/8/2021), "Combatting online racist abuse: an update following the Euros", accessed at https://blog.twitter.com/en_gb/topics/company/2020/combatting-online-racist-abuse-an-update-following-the-euros

users, and update that verification with the cooperation of users on an ongoing basis. This obligation imposes an unreasonably high and challenging technical responsibility for providers to meet.

11.3. DIGI therefore submits that the Bill must contemplate that there will, inevitably, be situations where the information held and accessed by the provider and entity will not be the correct contact information of the commenter. In these circumstances, if the provider undertakes all relevant steps in the complaints process in compliance with the order, the defence under the Bill should be made available to the provider, including in circumstances where a commenter's contact details cannot be verified.

11.4. Further, DIGI submits that once the contact details are provided by the provider to the complainant, the onus should then shift to the complainant to make a reasonable attempt to contact the commenter before the institution of proceedings. In the absence of such an obligation on the complainant, the provider may be denied a defence despite having complied with all obligations, simply because a complainant's limited efforts to contact a commenter have been unsuccessful.

12. Nominated entity requirements and access to data

12.1. Section 20 of the Bill proposes that if a social media service provider is a foreign body corporate, and the service has at least 250,000 Australian account-holders (or has been specified in the legislative rules), the provider must have a nominated entity in Australia. The nominated entity is required to have "access" to relevant contact information and country location data (s 20(1)(f)).

12.2. DIGI understands the Commonwealth Government's intention to ensure that jurisdictional issues do not present a barrier to the operation of the complaints and end-user information disclosure order mechanisms proposed in the Bill. However, DIGI submits that the nominated entity requirement as it currently stands does little to address this concern, and may be unduly disruptive to providers' existing data arrangements. For example, companies that operate in several jurisdictions usually have particular corporate entities – and nominated personnel within those entities – that have authorisation to access user data. They often impose such restrictions in line with their own human resources practices, cyber security considerations and the consideration of applicable law.

12.3. The Bill does not contemplate any unique purpose for the nominated entity that cannot be fulfilled by a provider in instances exemplified above. The current form of the Bill is drafted so that recourse for complainants are sought from, and obligations to comply are placed on providers, regardless of whether a nominated entity exists. For instance:

a) The complaints mechanism in s 16 of the Bill is an obligation for the provider. Regardless of whether there is a nominated entity in Australia, the responsibility for complying with the requirement to have an appropriate complaints mechanism in place is placed on the provider. The provider must ensure that the complaint is answered, and certain information provided, within specified timeframes. These timeframes are required to be met regardless of whether the provider has a nominated entity as defined under the Bill.

b) Section 18 of the Bill provides that complainants can seek end-user information disclosure orders against the provider.

12.4. DIGI submits that providers should be able to undertake their preferred practice to comply with these timeframes and requirements under the proposed Bill, and that it is burdensome to impose a requirement of creating a nominated entity specifically in Australia to do so. The requirement to grant a nominated local entity access to data that may be held overseas may be practically burdensome and cause disruption to providers' existing arrangements, which are subject to extensive privacy regulations in foreign jurisdictions. For example, in instances where a multi-national company has several corporate entities, they may have arrangements under laws such the *General Data Protection Regulation* (**GDPR)** that determine if or how user data may be shared across those entities.

12.5. Some providers may wish to nominate an existing entity in order to meet the requirements under the Bill, however it is not an essential aspect to ensure compliance with the Bill. The critical factor is whether the complainant will have their complaint answered within the necessary timeframe; the complainant is not concerned with whether the answer is provided by a local entity. The imposition of substantial penalties for failure to comply with this requirement, including the continuing contraventions provision in s 21 of the Bill, is therefore an extreme and unjustifiable result.

12.6. DIGI also notes that the requirement to have a nominated entity as it is currently defined under the Bill may conflict with Australia's free trade obligations relating to the provision of services. Namely, Article 10.5 of the Australian-United States Free Trade Agreement (AUSFTA) provides that Australia cannot require a service supplier in the US to establish or maintain a representative office or any form of enterprise, or to be resident, in Australia as a condition for the cross-border supply of a service.

12.7. Ultimately, there is little utility in requiring the nominated entity to be an agent or related body corporate of the provider (s 20(1)(f)); all that the entity requires is access to the relevant contact details and country location data; and authority to receive, on behalf the provider, complaints and requests made under the scheme by Australian persons.

13. Removal of innocent dissemination defence under s 14(3) and interaction with s 15 defence

13.1. DIGI's ultimate position is that the removal of the innocent dissemination defence for providers is unfair, unnecessary, and fails to understand the very nature of the defence as providing recourse for defendants with a lack of knowledge of, and control of, the defamatory content. DIGI submits however, that if the innocent dissemination defence is removed under the Bill, s 14(3) should be revised to ensure that the innocent dissemination defence is only unavailable to providers in circumstances where a complainant has engaged the resolution mechanisms in the Bill.

13.2. Section 14(3) of the Bill prevents a provider from relying on the defence of innocent dissemination in circumstances where the provider is a publisher of the comment and is a party to defamation proceedings related to the comment. Section 15 of the Bill provides a defence to a provider that complies with the s 16 complaints scheme or a s 18 disclosure order. The removal of the availability of the innocent dissemination defence

for providers is not limited to circumstances where a complainant has engaged in either dispute resolution mechanism under the Bill. Rather, the Bill proposes a wholesale removal of the innocent dissemination defence. Despite the intentions of the Bill, it is possible for a prospective applicant to commence proceedings without first engaging in the resolution mechanisms, most notably through the issuing of a compulsory concerns notice as is required to commence proceedings under State legislation. This is highly problematic for providers, as it is not mandatory for a complainant to engage a resolution mechanism under the Bill before commencing defamation proceedings against a provider, leaving a provider without access to a defence as contemplated by the Bill, nor the defence of innocent dissemination. This is an unjust outcome for a provider who is joined to defamation proceedings in which the resolution mechanisms have not been engaged.

13.3. It is also likely that prospective applicants may not wish to undergo either of the resolution mechanisms provided in the Bill for a range of reasons. Most notably, they may not wish to subject themselves to additional processes to find the individual commenter when a cause of action lies against a provider as a publisher pursuant to s 14(1)(d) of the Bill. The legislative mandate that providers are publishers, and that the defence of innocent dissemination does not apply (whether or not the resolution mechanisms were engaged) is likely to contribute to increased litigation in Australia by encouraging prospective applicants to commence proceedings directly against a provider rather than attempting to identify and join the individual commenter. This would have the opposite effect of the Government's intended result, which is to ensure that post-*Voller*, individual commenters are held accountable for their comments online.

13.4. DIGI recommends that, if the innocent dissemination defence is to be removed for providers, s 14(3) be revised to ensure the defence is removed only where an applicant has initiated at least one of the two mechanisms provided in sections 16 and 18 of the Bill.

14. Availability of s 15 defence where consent has not been provided

14.1. Section 16 of the Bill provides that upon the request by a complainant for the commenter's contact details, the provider may only disclose such details with the commenter's consent (s 16 (1)(g)(iii)). A defence under s 15 of the Bill is not available to a provider where the provider has not received consent for disclosure and the complainant has not subsequently applied for or been granted an end-user information disclosure order under s 18.

14.2. Given that disclosure of contact details is for the purpose of providing a complainant with a means for redress against the commenter directly, DIGI anticipates that the commenter will invariably not consent to the provider providing the contact details to the complainant. It is DIGI's view that in these circumstances, the defence should be available to providers who have complied with all relevant requirements in seeking to obtain consent, whether or not consent is ultimately provided. This will ensure further certainty for providers that compliance at all stages will guarantee them the benefit of the safe-harbour defence in s 15.

14.3. DIGI therefore suggests amending s 15(2)(d) to insert the following condition: under the complaints scheme, the applicant has requested the provider to disclose the relevant

contact details of the commenter to the applicant in order to assist the applicant in relation to the potential institution by the applicant of a defamation proceeding against the commenter in relation to the comment, and the provider has sought consent of the commenter to disclose the commenter's details to the applicant, and a court has not made an end-user information disclosure order in relation to the comment.

15. Section 16 timeframes

Practical effect of 72 hour timeframes on providers

15.1. The complaints mechanism in s 16 of the Bill contains numerous requirements for certain steps to be undertaken within a 72 hour timeframe. DIGI understands the need to impose timeframes to ensure the efficient and effective engagement by all parties in the complaints process. However, there are issues with compliance within this 72 hour timeframe, especially where the provider of a social media service is a body corporate incorporated in a foreign country with a nominated entity in Australia, as required by s 20 of the Bill.

15.2. Although the nominated entity is required to have access to the relevant contact details and country location data of end-users (s 20(1)(f)), this data may be stored on overseas servers, the data will likely need to be verified, and the data will need to be transferred into a comprehensible form. Undertaking this process may not always be achievable within 72 hours, particularly in circumstances involving international time differences, and where the 72 hour timeframe does not account for working days. DIGI therefore submits that the requirements to inform the commenter of a complaint (s 16(1)(b)), subsequently inform the complainant of such (s 16(1)(c)) and to disclose the country location data of the commenter (s 16(1)(d)) cannot always feasibly be achieved within a 72 hour timeframe.

15.3. DIGI submits that:

a) the timeframes in s 16 should be by reference to working days, excluding weekends and public holidays in Australia and the country where the relevant user information is stored; and

b) the timeframe should be amended from 72 hours (i.e. 3 working days), and appropriate timeframes should continue to be considered as part of the Stage 2 law reform process.

Implementation of timeframes for commenter to consent

15.4. It is inevitable that some commenters, upon being contacted by a provider, will not respond to a request for consent to disclosure of contact details. Further clarity is required so that providers understand when to conclude that consent has not been provided, and to inform the complainant of such.

15.5. DIGI therefore recommends that s 16 be amended to provide a specified timeframe for the commenter to provide consent to the provider. Upon a lapse of this timeframe, unless the commenter advises otherwise, the provider can interpret a commenter's failure to

respond as a lack of consent to disclosure. It is suggested that the provider inform the commenter of this timeframe upon requesting consent.

16. Clarifying the 'reasonable belief' of the provider requirement

16.1. Section 16(1)(h) of the Bill provides that the provider is not required to take any action under the complaints scheme if the provider 'reasonably believes' that the complaint 'does not genuinely relate to the potential institution by the complainant of a defamation proceeding against the commenter in relation to the comment'.

16.2. This provision is uncertain. It is not clear what is required for a provider to substantiate its 'reasonable belief', or whether the statutory defence in s 15 will be available to a provider in circumstances where the provider reasonably holds this belief, and proceedings are subsequently instituted by the complainant in any event. DIGI recommends that the Bill resolves these uncertainties.

17. Addressing Privacy Concerns

Australian privacy jurisdiction: collection of personal information

17.1. The Bill requires providers to collect personal information from users in order to have access to the safe-harbour defence. As noted, the definition of a social media service provider in s 6 of the Bill, by reference to s 13 of the Online Safety Act, extends the definition beyond large social media organisations to include any electronic service with the primary purpose of enabling online social interaction between 2 or more users. As this submission has explored, the requirement to collect personal information from users is likely to have adverse consequences for internet users who will be required to hand over personal information to a broad range of online services and expose providers to increased risk of privacy violations.

17.2. It is possible that some of these providers may not be covered by the *Privacy Act 1988* (Cth) ('**Privacy Act**'). The Privacy Act applies to organisations with an annual turnover more than $3 million (and Australian Government agencies), however it only applies to small business operators in limited circumstances – for instance, private sector health service providers. As such, certain providers incentivised to collect personal information by the Bill may not be required to comply with the protections of personal information upheld in the Privacy Act.

Australian privacy jurisdiction: disclosure of personal information

17.3. The disclosure of personal information under an end-user information disclosure order, where consent has not been obtained, also raises issues concerning an individual's right to privacy. Although the Privacy Act allows for the disclosure of personal information where it is required or authorised by or under an Australian law or a court order (Australian Privacy Principles 6.2(b)), such disclosure should not be taken lightly and should consider an individual's right to refuse consent to the disclosure of their personal information. The Bill should specify that the disclosure of personal information in accordance with the Bill is for the limited purpose of actual or anticipated defamation proceedings. It is otherwise possible that the resolution mechanisms contemplated by

the Bill could be used for other purposes other than the commencement of defamation proceedings. In order to address these concerns, the court may wish to consider factors that extend beyond "a risk to the commenter's safety" (s 18(3)) when making an end-user information disclosure order.

17.4. DIGI therefore submits that s 18(3) be amended to include non-exhaustive factors for the court to consider when making an end-user information disclosure order, including but not limited to:

i. whether disclosure presents a risk to the commenter's safety;
ii. whether the comment was made for whistleblowing purposes;
iii. an individual's right to privacy; and
iv. the ability of the provider to obtain the information.

Interaction with privacy law in other jurisdictions

17.5. The requirement for providers to collect and hold information in order to be in a position to comply with the Bill also raises issues regarding potential conflicts with providers' existing privacy obligations under law in other jurisdictions. Where a social media service is a body corporate incorporated in a foreign country with a nominated entity in Australia, data sought by the complaints mechanism may be stored in the servers of the foreign body corporate. This body corporate would therefore be subject to the relevant privacy and information collection and disclosure regimes within the jurisdictions in which it operates and stores data.

17.6. DIGI foresees conflicting obligations between the mechanisms contemplated by the Bill and the legal obligations of its users under regimes in other jurisdictions, for example, under Article 17 of the *General Data Protection Regulation* (**GDPR**), which provides that an individual has the right to obtain erasure of their personal data by the controller under various grounds. There may be circumstances where an individual deletes their account and/or requests for their personal data to be erased by the foreign corporation, however, a nominated entity is required to hold or access the data for at least the limitation period, in order to meet the requirements of the compliance scheme and be afforded the benefit of a defence. We also note that the current review of the Privacy Act recommends a right to erasure in Australia that may create similar conflicts if this proceeds.

17.7. Whilst the Bill applies to comments that are made in Australia (see ss 9 and 16), the Bill does not require the commenter to be an Australian resident, therefore it is possible that an individual user who makes a comment within Australia has privacy rights under an international jurisdiction, to which a body corporate holding the data, potentially in an overseas jurisdiction, must uphold. DIGI submits that consideration should be given to this potential conflict.

Summary of recommendations in Part 5

E. The Commonwealth Government considers that the broad definition of social media services in the proposed Bill encompasses a wide range of services and incentivises those services to collect more personal information from their users. The Bill should therefore be amended to

more closely consider a user's right to online anonymity and the increased cyber security risks that come with the collection of personal data.

F. The defence in s 15 be made available in circumstances where a provider undertakes all relevant steps to comply with an end-user disclosure order, however the commenter's contact details cannot be verified.

G. Where the provider provides verified contact details of the commenter to the complainant, the onus shifts to the complainant to make a reasonable attempt to contact the commenter before the institution of proceedings.

H. The Commonwealth Government reconsiders the nominated entity requirement in s 20 of the Bill.

I. The innocent dissemination defence should remain available to providers. If the defence is removed under section 14(3), it must be removed only where an applicant has initiated at least one of the two mechanisms provided in sections 16 and 18 of the Bill.

J. Section 15(2)(d) be revised to ensure the availability of the defence in circumstances where a provider has sought the consent of the commenter to disclose the commenter's details to the applicant, and a court has not made an end-user information disclosure order in relation to the comment.

K. The timeframes in s 16 be amended from 72 hours and appropriate timeframes should continue to be considered as part of the Stage 2 Review.

L. Section 16 be amended to provide a specified timeframe for the commenter to provide consent to the provider.

M. The Bill clarifies the 'reasonable belief' requirement in s 16(1)(h) and its impact on the availability of a defence under s 15.

N. The Bill reflects the impact of the collection and disclosure of personal information by providers on an individual's right to privacy, including by providing this consideration in a list of inclusive, yet non-exhaustive factors to be considered by the court in making an end-user disclosure order.

O. The Bill is amended to more closely consider how the requirement for providers to collect and hold the personal information of individuals may result in conflicting privacy and data obligations in other jurisdictions and areas of Australian law.