BCA
Business Council of Australia

Social Media (Anti-trolling) Bill 2022

February 2022

Contents

1. About this submission

This is the Business Council's submission to the Senate Legal and Constitutional Affairs Legislation Committee on the Social Media (Anti-Trolling) Bill 2021 ("the Bill"). The Bill is focused on changes to defamation law, and follows the High Court decision in *Fairfax Media Publications v Voller*.

This submission reiterates many of the same points we have made in response to the exposure draft of the Bill released by the Attorney-General's Department last year.

The Business Council represents businesses across a range of sectors, including manufacturing, infrastructure, information technology, mining, retail, financial services and banking, energy, professional services, transport, and telecommunications.

2. Key recommendations

The Business Council recommends not proceeding with this Bill, and instead encourages the government to continue to work through the Online Safety Act and the existing Model Defamation Provisions reform process to achieve meaningful improvements in Australia's online safety and updating defamation laws.

If the Committee is of the view this Bill is necessary, we recommend:

1. The 'innocent dissemination' defence be maintained, and platforms be able to access a defence where they can show reasonable efforts made in good faith to connect a complainant with the originator of the comment.
2. Not proceeding with any changes that would have the net effect of removing anonymity from Australians participating online.
3. Reconsidering the need for the nominated entity provision, given it appears in breach of the AUSFTA and Australia's global leadership on digital trade.

3. Overview

We support the government's commitment to keeping Australians safe from online harm. This includes defamatory or harmful comments made anonymously. Like many laws and regulations, defamation law has not kept pace with changing social interactions and expectations prompted by an increasingly digital Australia. The online environment has also created new avenues for 'trolls' and malicious individuals to attack or bully Australians. We note, however, that 'trolling' activity is typically harassing or abusive and is not the same as defamation.

Australians should, and do, have appropriate recourse where they have been victims of these attacks, subject to the appropriate checks and balances. This includes being able to launch actions against those who post defamatory or harmful content online. It is important that we improve these safeguards without compromising Australians' freedom to express their views nor reduce their privacy unnecessarily. We agree that the current laws have not kept pace with technology.

It's for this reason that our members, including large digital platforms, have been engaging with the ongoing work of Attorneys-General across Australian jurisdictions on the Model Defamation Provisions, which is being led by New South Wales. Stage 2 of this process has specifically been considering the question of internet intermediary liability in defamation for the publication of third-party content.

While we support the government's intention with this Bill (to provide recourse for Australians where defamatory material has been posted online) we do not consider the model as currently presented by government will have

the impact that government intends for individual Australians. Online harms are the right problem to address, but this is not the right solution.

This position reflects evidence provided by a range of witnesses to the House Select Committee Inquiry into online harms and at Senate Estimates, including the eSafety Commissioner. Indeed, the eSafety Commissioner highlighted that in her experience individuals would rather the Commissioner 'use the [existing] powers … to adjudicate those cases for them', and not pursue defamation.

The government's new Online Safety Act establishes a new Adult Cyber Abuse content removal scheme, designed to facilitate the rapid removal of abusive online content targeted at Australian adults. For individuals who are the subject of online abuse, this scheme empowers the eSafety Commissioner to have the abusive content quickly taken down.

This Bill will have a limited impact on safety outcomes for individuals. However, it will be a substantial change in approach to how defamation laws are considered. For this reason, the Business Council welcomes the Legal and Constitutional Affairs Legislation Committee's consideration of this Bill. As we have noted in our previous submission to the Attorney-General's Department on this Bill, the Commonwealth does not have a constitutional basis for making legislation relating to defamation – this Bill relies on the communications head of power. This Bill we be a substantial step away from the accepted practice of states and territories being responsible for defamation.

For individuals who are victims of defamation – which, as we have noted above, should not be confused as synonymous with trolling / abuse – the Bill does not currently contemplate the removal of the content that is subject to a potential defamation claim. Indeed, removing the material in question does not actually provide a company with access to a defence. We recommend amending the Bill to include an innocent dissemination defence for companies that opt to make the potentially defamatory content unavailable in good faith on receipt of a valid complaint. Many operators of these platforms have systems and processes in place to support users faced with this type of content to have it removed, including as part of the Online Safety Act.

Moreover, the explanatory material provided with the Bill states it is inappropriate for liability concerns to restrict free speech and that the intent of the Bill is to focus legal proceedings between the victim and the originator of the alleged defamatory comment. As part of this, the Bill explicitly carves out 'page owners' (ie those who maintain or administer a page on a social media service). As others have highlighted as part of the consultation on the earlier exposure draft, this poses substantial problems, including potentially increasing the volume of defamatory or otherwise problematic material posted, as page owners will have less incentive to moderate comments.

Instead, the Bill places responsibility on social media services. This is because the government is concerned that Australians, in their role as page owners or administrators, might be liable for defamatory material despite not knowing about its existence or intending its publication. However, this logic holds as true for social media page 'administrators' as it does for the platforms themselves, who in many cases will be even less well placed to determine whether content is likely to be defamatory. This is particularly the case given potentially defamatory comments are likely to be highly context-specific or relate to local concerns.

The Business Council supports government modernising laws, regulations, and processes to make Australia a leading digital economy. But additional regulation must be scrutinised to ensure the proposed benefits outweigh the costs, such that it does not discourage businesses modernising or offering new services in Australia that will ultimately benefit Australians. In its current form, any benefits of this Bill will be substantially outweighed by the costs – both the direct regulatory implementation costs and the wider social costs.

As drafted, the proposed Bill will do little to reduce trolling or provide Australians with a safer online environment. As has been noted elsewhere (including in evidence to the Select Committee on Social Media and Online Safety), recourse through defamation proceedings is 'almost impossible' because of the cost. But it will reduce privacy outcomes for all Australians who use social media services, and have a chilling effect on Australians' engagement in online discussion or debate. Moreover, the proposed model does not reflect the way both users

and businesses interact with social media. It will set a bad precedent for government intervention across all parts of the economy by creating unrealistic liabilities for businesses operating in Australia while creating potentially unwarranted protection for others.

4. Key points

4.1 Defences and privacy

The Bill defines social media services as 'publishers' of defamatory comments made in Australia. Businesses will be able to access defences if they 'comply with a complaints scheme and/or end-user disclosure order, and actually disclose the originator's contact details to the victim'. However, the Bill explicitly removes the defence of 'innocent dissemination' for businesses.

4.1.1 Access to defences

The defences prescribed in the Bill place unrealistic requirements for businesses to access them. The Bill will not allow regulated entities to access a defence where an individual who has posted allegedly defamatory content declines to provide their contact details and a court *declines* to grant an order requiring disclosure of the individuals contact details. This is disproportionately punitive, preventing business from accessing a defence because of a decision made by a third party that they have no control over and where a court may have determined not to disclose these details.

The approach places an inappropriate amount of emphasis on businesses as the primary entities liable in defamation. These businesses will be more attractive targets for complainants, as they are more readily identifiable, more likely to have means to afford compensation, and unable to access defences available to the original creator of the allegedly defamatory material (such as truth or honest opinion).

The explanatory memorandum suggests this is to ensure an aggrieved individual has a respondent to bring proceedings against, even if that respondent is not the originator of the alleged defamatory content. As discussed above, there is no clear policy rationale for social media providers being deemed this respondent, or for the removal of the 'innocent dissemination' defence. We support the Committee considering the unintended consequences of this outcome.

Moreover, the current drafting of the Bill will create substantial and burdensome business and consumer costs. Businesses will need to collect and verify the contact details of individuals to make them available in response to a disclosure order or where an individual has given consent, to access a defence. However, the current approach will require businesses to not only verify these details at a single point, but also to regularly verify the currency of these contact details. This is because of the requirement that a nominated entity in Australia will must have access to the 'relevant contact details of posters … in Australia'.

This requirement will be onerous and burdensome – not only to the regulated social media businesses involved, but also for Australian users and businesses. To have the level of confidence necessary to meet the requirements in the Bill will create substantial business costs and be highly intrusive for users of the services, well out of proportion to the problem being resolved. It also does not resolve a fundamental problem with the approach taken in the Bill, which is that an individual may choose to simply not respond to a request, even where they are contacted via accurate contact details.

4.1.2 Privacy implications

The Bill will also require businesses to collect substantially more personal information on all Australians that use their services. The definitions in the Bill specify that a business will need to be able to supply details of a person's:

- name,

- email address,
- phone number, and
- any other details determined by the legislative rules.

As noted above, for a business to access a defence in any defamation proceedings, they will (among other requirements) need to 'actually disclose' this information in response to a request either from a complaints scheme or a court making an end-user disclosure order. Further, these businesses will need the agreement of the originator of a comment to supply that commentor's details as part of their complaints scheme or a court order to be able to access a defence. This is deeply problematic.

The requirement for businesses to hold this information will effectively deny Australians the ability to maintain their privacy through anonymous/pseudonymous accounts. For businesses to ensure they can access the defences set out in the Bill, they will need to both *confirm* the accuracy of any details that are provided to ensure they can '*actually disclose*' this information. The removal of anonymity will have a regulatory and social cost well beyond the problem government is seeking to solve, and it needs to be balanced against legitimate opportunities for people to exchange ideas and information and express their opinions and beliefs.

As noted above, social media businesses also agree that the current defamation laws have not kept pace and need to be updated to address harmful content created by anonymous users online, including potentially defamatory content online. This includes by working through the agreed New South Wales-led process on the Model Defamation Provisions.

In addition to engaging in the agreed process to update defamation laws, social media businesses have also demonstrated their commitment to working with government to address harmful content created by anonymous users, including through new powers under the Online Safety Act that allow the eSafety Commissioner to obtain information about the owners of anonymous accounts who engage in online abuse. Further, these businesses have already demonstrated they are willing to comply with court orders under existing laws to provide identifying information in defamation proceedings.

The explanatory memorandum suggests government believes the proposed approach strikes a reasonable balance for privacy outcomes. The explanatory memorandum suggests that it does not *require* platforms to collect this information. However, it also effectively removes any avenue for these businesses to access a defence against liability for defamation claims without it. It is not clear, in practical terms, how government expects businesses to operate in an environment where these incentives are so heavily skewed.

The approach suggested in the Bill does not adequately balance the need for Australians to have recourse against those who would defame them, with the legitimate need for Australians to have their privacy protected. The Bill takes a very narrow view of privacy (that it is only an issue enlivened when information is disclosed in response to a complaints mechanism or court order). However, the suggested approach has much wider ramifications for Australian's privacy, creating substantial incentives for businesses to ask for more information about individuals that they might otherwise have no desire to otherwise collect or hold.

While Australian consumers may choose to provide the kinds of details required by the legislation (such as their name and contact details), this has not been a requirement for most services that will be captured under this Bill. For some, such as people seeking support for mental health concerns, victims of domestic violence, whistle-blowers, or people exploring their sexual identity, there are substantial benefits to being able to access these services anonymously or pseudonymously. The Bill, as drafted, is a blunt instrument that will run counter to the best interests of these groups and all Australians without any tangible improvements to online safety outcomes.

Beyond the costs of removing anonymity for all Australians online, the requirement for social media businesses to collect and hold even greater volumes of Australians' personal information runs counter to other government initiatives and general best practice privacy principles, such as data minimisation. Underpinning government initiatives such as the Online Privacy Code and the review of the Privacy Act is a concern about the amount of information being collected by large digital platforms. This Bill would seem to undermine these other efforts for

only minimal gain. We do not support measures which would remove anonymity online without sufficient justification.

Instead of focusing on ending anonymity to prevent abuse online, we consider the Online Safety Act remains a better mechanism to ensure the systems and processes are in place to prevent and detect abuse.

Rather than proceeding with the approach proposed in the Bill, we recommend the 'innocent dissemination' defence be maintained, and platforms be able to access a defence where they can show reasonable efforts to connect a complainant with the originator of the comment. Conversely, where platforms cannot show these reasonable efforts, they could still be held liable if they do not qualify for the other defences.

4.2 Nominated entities

The Bill requires entities captured by the Bill (under threat of substantial penalties) to have a 'nominated entity' capable of meeting the obligations arising under or in connection with the Bill. These obligations include requiring the nominated entity to have access to 'the relevant contact details … and country location data of end-users … in Australia'.

This requirement is unnecessary. The Bill is already designed such that entities operating in Australia will be required to comply with obligations that may arise under or through the operation of the Bill. We understand the strong intention of government is to avoid any data localisation requirements. Australia has long been a champion of a rules-based global order that supports the digitalisation of trade and has argued against data localisation requirements. Unfortunately, the current drafting of the Bill could create the perception that Australia was supportive of regulatory regimes that would justify these requirements, increasing barriers to cross-border data flows.

Given many of the entities likely to be regulated by this legislation are headquartered in the United States, it also appears in breach of the Free Trade Agreement (FTA) between Australia and the United States. Article 10.5 of the FTA explicitly states that neither party will 'require a service supplier of the other Party to establish or maintain a representative office or any form of enterprise, or to be resident, in its territory as a condition for the cross-border supply of a service'.

Though government may be of the view that this requirement is allowable within the specific text of the FTA, it is not clear it is within the spirit of the agreement. To give confidence to our trading partners that we stand by the commitments make in signing trade agreements, and to show that we do not support requirements for data localisation, we recommend the Committee reconsider the need for this requirement.

BUSINESS COUNCIL OF AUSTRALIA

42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au