18 August 2023

Information Integrity Section
Department of Infrastructure, Transport, Regional Development,
Communications and the Arts

Submission via :https://www.infrastructure.gov.au/have-your-say/acma-powers

Consultation on an exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The **Deakin University Centre for Cyber Security Research and Innovation** ('CSRI') is a Strategic Research Centre that brings together a multi-disciplinary team of researchers drawn from Deakin's four Faculties. CSRI's research program is focussed on the technology, systems, human, business, legal and policy aspects of Cyber Security, and is committed to achieving translational and transformational research outcomes for industry, business and society. CSRI's research program is advised by senior industry and thought leaders through its Executive Advisory Board for Cyber (EABC) and is funded through national competitive grants and industry. More information about Deakin CSRI can be found at https://www.deakin.edu.au/csri.

About this Submission

We are grateful for the opportunity to make a submission to the consultation on the exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 (the Bill). Our submission reflects our views as researchers; they are not an institutional position. This submission may be made public.

We acknowledge the extensive body of work produced by the ACCC and the ACMA on digital platforms since 2017. We also acknowledge the efforts of Digital Industry Group Inc. in developing the *Australian Code of Practice on Disinformation and Misinformation*, and the research it has commissioned and made publicly available. We note the submissions to the Senate Economics References Committee inquiry into the Influence of international digital platforms.

The exposure draft of the Bill contains positive measures for increasing transparency and accountability over how platforms manage misinformation and disinformation. We make the

following key submissions and recommendations on the Bill, followed by our substantive comments on aspects of the Bill.

Summary of our submissions:

1. The complex balancing act to which the Bill is directed continues to favour platform self-regulation as the preferred form of regulation. The Guidance Note does not ask whether it is desirable for platforms to continue to make decisions about what constitutes misinformation and disinformation on their own. It also leaves unquestioned whether the self-regulatory model is still the appropriate model for protecting Australians from the serious harms of disinformation, and problematic misinformation.
2. Our research funded by the Cyber Security Cooperative Research Centre argues that a focus on *disinformation campaigns* is important and necessary. Our research proposes legal sanctions against the most insidious forms of disinformation, which we refer to as disinformation campaigns. The addition of *disinformation campaign* to the definition of disinformation may aid development of a nuanced regulatory response that is calibrated more closely with serious harm. Our research recommends that the Australian government should clearly define the *serious* harms to society that necessitates and justifies interference with free speech of the kind only courts (and not platforms) can impose.
3. Communications technology continues to change and evolve. We note that the Bill refers to *digital* services only, including digital platform services. Our concern is that the concept of *digital* will become obsolete as communications and media technology evolves and develops over the next decade, creating a loophole for non-digital format services.
4. A more active role for the Australian Communications and Media Authority (the ACMA) and other public institutions, such as State and Federal courts, should be explored, including consideration of the advantages and disadvantages of implementing a 'co-design' process within the co-regulatory framework for codes and standards.

Our recommendations

1. **We recommend the insertion of the words "in consultation with the ACMA and taking account of any relevant research conducted by the ACMA" into section 32 of Division 3 (relevant consequential amendments should follow to ensure this provision is operational in the context of the Division).**
2. **The definitions and treatment of misinformation and disinformation should be revised. We recommend the addition of *disinformation campaigns* to the definition of disinformation, and that consideration be given to how courts can be empowered to exercise jurisdiction over extreme cases of disinformation campaigns.**

General comments on the Exposure Draft Bill

As wicked problems, misinformation and disinformation have led governments around the world to intervene using a range of regulatory tools and methods. Globally, governments have placed significant trust in platforms' internal policies on misinformation and disinformation; the platforms' own technological capabilities to enforce these policies; and/or their voluntary cooperation with governments and researchers. Australia has, to date, adopted industry self-regulation as the

preferred regulatory approach for managing misinformation and disinformation. However, some countries, like Germany and Singapore, have legislated broad anti-disinformation laws.[1]

Many countries continue to rely on digital platforms to define and/or identify misinformation and disinformation that do not fall within narrowly defined categories of illegal speech such as defamation, and cyber abuse.

The preference for self-regulation requires examination

The Bill has been developed in response to recommendations made by the ACMA in its report on the adequacy of digital platforms' disinformation and news quality measures published in 2021 and informed by the ACMA's findings in its second report to government on the efforts of the platforms under the Australian Code of Practice on Disinformation and Misinformation published in July 2023.[2]

We acknowledge that the Bill is an attempt by the Australian government to balance the commercial and operational interests of platforms against urgent and important public interests, which include, among other things, transparency and accountability over platform methods and processes, freedom of expression and freedom from the known serious harms of disinformation and the known problems of misinformation, which can include causing or contributing to serious harm.

We are curious about the preference for self-regulation given the graduated approach that both sides of politics have taken to equally pernicious problems in the communications sector, including: purpose-built legislation, such as the *Spam Act 2003* (Cth), the *Do Not Call Register Act 2006* (Cth), the *Interactive Gambling Act 2001* (Cth), and the *Classification (Publications, Films and Computer Games) Act 1995* (Cth); unequivocal prohibitions, such as tobacco advertising[3] and X-rated content[4]; standards, including Anti-terrorism Standards for Narrowcasting Services[5]; and registered codes of practice.[6]

Australia recently enhanced the regulatory framework for online safety, including adopting a co-regulatory framework for the online content scheme,[7] and enacted the *Criminal Code Amendment (Sharing Abhorrent Violent Material) Act 2019* (Cth), which imposes a reporting obligation on content, internet, and hosting providers to report and remove violent abhorrent content.[8]

---

[1] For example, in Germany, see the Network Enforcement Act (the NetzDG law), which came into effect in January 2018. In Singapore, Protection from Online Falsehoods and Manipulation Act (POFMA), which took effect in October 2019.

[2] See Australian Communications and Media Authority, *A report to government on the adequacy of digital platforms' disinformation and news quality measures* (June 2021, Australian Communications and Media Authority); Australian Communications and Media Authority, *Digital platforms' efforts under the Australian Code of Practice on Disinformation and Misinformation - Second report to government* (July 2023, Australian Communications and Media Authority).

[3] See eg, *Broadcasting Services Act 1992* (Cth) (BSA), Part 3, Division 1, section 7(a)

[4] See eg BSA, Part 6, section 10(1)(f).

[5] See eg, Broadcasting Services (Anti-terrorism Requirements for Television Narrowcasting Services) Standard 2021.

[6] See eg, BSA, Part 9 and Part 9B

[7] See eg, Online Safety Act 2021 (Cth), Division 7.

[8] See eg, *Criminal Code Amendment (Sharing of Violent Abhorrent Violent Material) Act 2019* (Cth), sections 474.33 and 474.34. For a critical analysis of the Act see Mark Nolan and Dominique Dalla-Pozza, 'Clumsy and

We submit that the complex balancing act to which the Bill is directed continues to favour platform self-regulation as the preferred model of regulation, leaving unexamined whether it is still the most effective model for protecting Australians from the serious harms of disinformation and the known problems of misinformation, which may cause or contribute to serious harm.

Self-regulation enables informal workarounds or 'gap-fillers'

The ACMA noted in its 2021 report that the current industry-led self-regulatory code, the *Australian Code of Practice on Disinformation and Misinformation*, lacks certainty as 1) not all service providers are obliged to act in accordance with the voluntary disinformation code, and 2) there are no consequences for non-compliance.[9] Additionally, the preference for self-regulation, has, in turn, enabled informal 'work arounds' or 'gap-fillers'[10] between platforms and government departments and regulators, which operate in the gaps between legislative frameworks.[11]

The Department of Home Affairs' *Online Content Incident Arrangement (OCIA) Procedural Guideline*, revealed in Senate Estimates in May 2023, is an example of a regulatory 'gap-filler'.[12] The procedure is described in documents released under the *Freedom of Information Act 1982* (Cth) as 'the Australian government's crisis response protocol for preventing the viral dissemination of online terrorist and violent extremist content.'[13] The document explains that the OCIA 'outlines the roles and responsibilities of digital industry and government agencies to ensure effective communication and co-ordinated operational responses to contain *the spread of terrorist or violent extremist content online following a terrorist incident*.' However, it was reported in Senate Estimates Hansard that between 2017 and 2021, the procedure was used approximately 13,000 times, enabling the Department of Home Affairs to refer Covid-19 misinformation and other misinformation related to

---

flawed in many respects': Australia's abhorrent violent material legislation' in Shirley Leitch and Paul Pickering (eds) *Rethinking Social Media and Extremism* (2022, ANU Press), 103 – 123.

[9] Australian Communications and Media Authority, *Digital platforms' efforts under the Australian Code of Practice on Disinformation and Misinformation - Second report to government* (July 2023, Australian Communications and Media Authority). 2

[10] See, for a discussion of soft law in the counter-terrorism context: European Centre for Not-for-Profit law, 'Soft Law, Hard Law Consequences', *Counter-Terrorism and Human Rights Briefing* (2019, United Nations Human Rights – Office of the High Commissioner): < https://www.ohchr.org>. Accessed 17 August 2-23.

[11] For example, the Department of Home Affairs' *Online Content Incident Arrangement (OCIA) Procedural Guideline* was revealed during Senate Estimates hearings on 22 May 2023. See, Hon Senator Alex Antic, Senate Estimates, Legal and Constitutional Affairs Committee, Department of Home Affairs, 22 May 2023, 49-56, 49: The OCIA guideline is used for content that does not meet the thresholds of the *Online Safety Act 2021* (Cth) or the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth). The e-Safety Commissioner also uses informal removal requests in remediating cyberbullying and adult cyber abuse. See Julie Inman Grant, 'Tackling individual harms and systemic reform in 2021-2022 (26 October 2022, eSafety Commissioner Blog); < https://www.esafety.gov.au/newsroom/blogs/tackling-individual-harms-and-systemic-reform-2021-22>. See also eSafety Commissioner, Submission to Parliamentary Joint Committee on law Enforcement Inquiry: Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, 15 October 2019, 9.

[12] The Hon Senator Alex Antic, Senate Estimates, Legal and Constitutional Affairs Committee, Department of Home Affairs, 22 May 2023, 49-56.

[13] Department of Home Affairs, *Submission for Information - Online Content Incident Arrangement – Exercise Event 2022*, Document released by Department of Home Affairs under the Freedom of Information Act 1982, Document number FA220900808, dated 4 August 2022: < https://www.homeaffairs.gov.au/access-and-accountability/freedom-of-information/disclosure-logs/2022#>.

its counter-terrorism functions.[14] The revelation in Senate Estimates highlights some of the problems with 'gap-fillers' and workarounds - its potential to mislead and confuse, and for misuse.[15]

While there is redacted information about the procedure available online through the Department of Home Affairs' FOI Disclosure Logs 2023,[16] information about the kind of material removed and the standard that it was judged by is not available.[17] The risk of 'gap-fillers' is that they result in secret editorial decisions about restrictions on speech, and are at the discretion of the company, or owner of the company.[18] As an informal regulatory mechanism, the OCIA may be designed with good intentions, but inadvertently operate to undermine the efficacy of the self-regulatory framework because it operates outside it and in secret.[19]

While informal workarounds and 'gap-fillers' may be highly flexible and quick to operationalise, they open the way for - at best – over-blocking content, which harms free speech, and - at worst – may lead to misuse,[20] and violations of human rights.[21]

Enduring co-regulatory frameworks administered by the ACMA

The enduring co-regulatory frameworks administered by the ACMA are functioning extant legislative frameworks with a clear sectoral remit. The strength of co-regulation over self-regulation is that co-regulation balances the public interest against the regulatory burden on the sector, and results in enforcement action for non-compliance with obligations under communications legislation.

We submit that the following amendment could be made to section 32 of Division 3:

> The Parliament intends that one or more bodies or associations that the ACMA is satisfied represent sections of the digital platform industry should develop, **in consultation with the**

[14] The Hon Senator Alex Antic, Senate Estimates, Legal and Constitutional Affairs Committee, Department of Home Affairs, 22 May 2023, 49-56, 49 (per Senator Antic '…from 1 January 2017 to 15 December 2022…there were 13,636 referrals to digital platforms. 9,423 related to terrorists and violent extremist related referrals….4,213 related to COVID-19 related content.')

[15] See Greg Weeks, 'Soft law and public liability' (2018) 39 *Adelaide Law Review* 303, 308 ('Soft law instruments might mislead or confuse particularly where they have not been published' and 'We can characterise soft law as a tool, such as a sharp knife.[footnote omitted]. Its sharpness might indicate that it is well-made, but that fact alone tells us nothing about the 'good' or 'bad' uses to which it might be put. Its potential for misuse is what causes concern. This potential comes from the fact that soft law is frequently treated by those to whom it is directed as though it were hard law.')

[16] Department of Home Affairs, *Online Content Incident Arrangement (OCIA) Procedural Guideline* (20 July 2023, FA 22/12/000629), FOI Disclosure Logs 2023: < https://www.homeaffairs.gov.au/access-and-accountability/freedom-of-information/disclosure-logs/2023>. Accessed 18 August 2023. At the date of access, the document released under the *Freedom of Information Act* was not able to be downloaded due to what appears to be a broken link. We notified the Department of Home Affairs by email on 1 August 2023.

[17] See Greg Weeks, fn 15, 308.

[18] See Shirley Leitch and Paul Pickering (eds) *Rethinking Social Media and Extremism* (2022, ANU Press) quoting Seth Oranburg, 'Social media and democracy after the Capitol riot', *Duquesne Lawyer*, 4. (In the context of the United Staes: 'Twitter, Facebook, Instagram, YouTube, TikTok, Reddit and Discord…do not 'censor' speech, in the technical sense, because only governments can censor. Private actors merely exercise editorial discretion – and they may do so virtually at will.')

[19] See Greg Weeks, fn15, 308.

[20] Ibid.

[21] See Terry Flew, 'Platforms on trial' (2018) 46(2) *InterMedia*, 24-29, 29 (for soft law to be effective it requires an institutional framework).

ACMA and taking account of any relevant research conducted by the ACMA, one or more codes (misinformation codes) that require participants in those sections of the digital platform industry to implement measures to prevent or respond to misinformation and disinformation on digital platform services.

This minor amendment, in addition to any consequential amendments, maintains the graduated approach to compliance and enforcement. It still leaves the digital platform industry with the space to develop suitable codes. However, a 'co-design' framework that includes the ACMA at the outset increases the footprint of public institutions, civil society, and consumer advocacy groups over the process, and sets minimum standards and expectations around consultation and community standards.[22]

The ACMA is an experienced industry regulator. Its broadcasting investigations consider issues of speech under codes of practice and standards; from racial hatred through to terrorism content to determine if a code or standard has been breached by the service provider. Telecommunications consumer safeguard investigations seek to establish regulated industry participant's compliance with their regulatory obligations.

Australia's fully functioning and operational communications co-regulatory framework already balances the public interest, including citizen and consumer concerns, against commercial and technological practicalities. The ACMA would benefit from targeted funding focused on increasing the knowledge and skills of its workforce to effectively regulate digital platforms and services, including building knowledge of business models, technology, products and services, and further research.[23]

Recommendation 1

We recommend the insertion of the words "in consultation with the ACMA and taking account of any relevant research conducted by the ACMA" into section 32 of Division 3 (relevant consequential amendments should follow to ensure this provision is operational in the context of the Division).

Definitions of misinformation and disinformation

The Bill defines misinformation as 'content that contains information that is false, misleading or deceptive'[24], and disinformation as 'content that contains information that is false, misleading or

[22] See Holly Raiche, Derek Wilding, Karen Lee & Anita Stuhmcke, *Digital Platform Complaint Handling: Options for an External Dispute Resolution Scheme* (UTS Centre for Media Transition, 2022). See also Karen Lee, T*he Legitimacy and Responsiveness of Industry Rule-Making* (2018, Hart Publishing). Further, Dr Karen Lee and Professor Derek Wilding, along with their colleagues in the UTS Centre for Media Transition and the UTS Faculty of Law were awarded an ARC Discovery Grant in 2022 to inquire into digital platforms regulation (See DP230101322 - *Optimising Industry-led Regulation for the Digital Platforms Era*: https://www.arc.gov.au/sites/default/files/2022-12/Senate%20Order%20-%20Pratt%20motion_November%202022.pdf)

[23] See Johanna Weaver and Sarah O'Connor, *Tending the Tech-Ecosystem – who should be the tech-regulator(s)?* (May 2022, Tech Policy Design Centre, Australian National University). The report discusses models for tech regulation. A key finding of the research - 'Upskilling existing regulators was the preferred base model, supported by increased funding, and enhanced transparency and accountability.' 29

[24] Exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, section 7(1)(a).

deceptive'[25] which is disseminated or caused to be disseminated by a person with the *intention* 'that the content deceive another person.'[26] Intention is an important distinction between the two types of communication.

Misinformation is difficult to categorise as malicious. Misinformation can be simply a person or group of people expressing muddled, false, or wrongheaded points of view or beliefs. It may also be about ideas and beliefs held to be true at a particular point in time, but later proved to be incorrect or false, or untrue. The extra requirement of 'reasonably likely to cause or contribute to serious harm' is a step towards limiting the kinds of misinformation that will be regulated.

Harm is broadly defined in the Bill, but serious harm is not.[27] Researchers have identified various harms to individuals, families, communities, democratic institutions, society, and the economy, which are the result of the spread of misinformation and disinformation on the internet. Several serious harms constitute challenges to important national interests such as public health (e.g., the COVID-19 infodemics).[28] It is important that the Bill is clear that the regime applies to *serious* harm, and that it clearly defines serious harm.

We submit that the definitions of misinformation and disinformation require careful consideration as there is still the problem that the definition – even with the limitation of causing or contributing to serious harm - will capture opinions, discussions and points of view that may be false or wrong at the time they are expressed, but through advances in knowledge and debate, are later shown to be true or correct.[29]

A missing concept from the definition of disinformation is the concept of a *disinformation campaign*. We suggest amending the definition of disinformation to include disinformation campaigns. A disinformation campaign is a highly coordinated series of actions within platforms, perpetrated by a network of actors, and has a socially harmful purpose. This concept implies that some instances of disinformation are more serious than others because they are highly organised, showing a greater degree of ill will by harnessing platforms' recommendation algorithms, generative Artificial Intelligence, and other technologies to achieve their harmful purposes. In contrast to the term *disinformation* which often implies a single action, and *misinformation* which lacks the element of intention to do harm, a *disinformation campaign* involves planning and organisation that cannot be mistaken for mere human carelessness or the effects of natural emotional contagion.

[25] Exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, section 7(2)(a).
[26] Exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, section 7(2)(e).
[27] Exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, section 2.
[28] For example, the World Health Organisation conducted a systematic review of literature regarding infodemics and health misinformation. The systematic review found that 'people feel mental, social, political and/or economic distress due to misleading and false health-related content on social media during pandemics, health emergencies and humanitarian crises.' See Israel Junior Borges do Nascimento et.al, 'Infodemics and health misinformation: a systematic review of reviews' (2022) *Bulletin of the World Health Organisation*. Published online 30 June 2022: doi:10.2471/BLT.21.287654
[29] Exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, section 7(1)(d) and section 7(2)(d).

The ACMA and Federal and State courts are well placed to consider serious harms. The definition of harm listed in (a) of the definition of harm in the Bill is directed to some areas already assessed by the ACMA under codes of practice and standards it administers. The ACMA also has experience in considering the harms listed in paragraphs (b) to (f) through its regulatory remit over other parts of the media and communications sector, such as telecommunications and communications infrastructure.

Courts should intervene in extreme cases of disinformation campaigns

For more serious disinformation cases, such as disinformation campaigns, courts have the expertise, independence, and public trust that make them preferable to platforms in adjudicating complex matters of serious harm in the context of speech acts and practices that amount to a disinformation campaign.

Research funded by the Cyber Security Cooperative Research Centre undertaken by researchers at Deakin University and UNSW argues that a focus on disinformation campaigns is important. In cases of *disinformation campaigns*, the law should attach criminal or tort liability to their perpetrators necessary to exact accountability and repel future wrongdoing. In these extreme cases, courts should be empowered to exercise the role currently performed by platforms. This move is intended for public institutions to regain control over speech regulation and reduce government's over-reliance on opaque and unaccountable platform decision-making for at least the most insidious forms of disinformation.

Recommendation 2

The definitions and treatment of misinformation and disinformation should be revised. We recommend the addition of *disinformation campaigns* to the definition of disinformation, and that consideration be given to how courts can be empowered to exercise jurisdiction over extreme cases of disinformation campaigns.

Definition of digital platform services and the types of services we propose be subject to the new framework.

The definitions of digital platform services and the types of services proposed to be subject to the new framework are adequate for capturing *digital* technology of the current environment. We welcome the addition of the declarative power granted to the Minister to respond to technological change and new services and products that may be used to spread misinformation and disinformation. However, we also note that the concept of *digital* is very much tied to the technology in which the format is deployed. For example, the digital platform service definitions do not contemplate quantum computing and quantum communications technologies, networks and platforms, which use *qubits*, a different format. While this might be some way off, it is preferable to use a technology-neutral term now to avoid interpretation questions down the track.

How instant messaging services will be brought within the scope of the framework while safeguarding privacy?

There are undoubtedly new and evolving instant messaging services already deployed or being developed and proliferating amongst individuals and groups, some of whom actively create and

spread disinformation to the end-users of those services. The methods of spreading disinformation and recruiting end-users to those communications are constantly evolving.

It is important that matters concerning disinformation and *disinformation campaigns* be decided within a co-regulatory framework, where the ACMA can formally and transparently liaise with other agencies, such as DHA, ASIO, the OIPC, the AFP and the e-Safety Commissioner, and platforms, for the exchange of expertise and advice on matters concerning disinformation and *disinformation campaigns* through instant messaging, and where there is a direct dialogue between the digital platform industry and the ACMA on how disinformation is evolving in the context of instant messaging services.

In terms of protecting end-user privacy and free speech, the ACMA's technology trial regimes could be examined and potentially adapted for the purposes of the Bill, [30] to support trials of technical solutions that detect disinformation and disinformation campaigns, yet also seek to protect end-user privacy and free speech.

Preconditions that must be met before the ACMA can require a new code, register a code and make an industry standard.

Serious consideration should be given to introducing a co-regulatory framework, which would create an obligation on the digital platform industry to develop a code in consultation with the ACMA, rather than the ACMA's current passive oversight role. Misinformation and disinformation need to be decoupled, and regulated as distinct wicked problems, with disinformation and *disinformation campaigns* requiring a higher level of regulatory intervention. The listed harms have serious consequences for Australian society, and disinformation and *disinformation campaigns* in particular warrant the involvement of experienced public institutions acting in the public interest.

How the digital platforms industry may be able to operationalise the Bill and various content exemptions (e.g. professional news, satire, authorised electoral content)

The preference for self-regulation hands this important function to the platform industry. However, there is scope within the BSA to involve the ACMA in assisting the digital platforms to operationalise the Bill by giving them certainty, for example, adapting the BSA's Section 21 Opinion provisions to the framework and requiring consultation with the ACMA in the development of codes.

This submission is made in the context of increasing the remit of the regulator over the misinformation and disinformation framework. This kind of function would open the dialog between platforms and the ACMA around disinformation and misinformation, around the content of the misinformation and disinformation, but also the form it takes, and the kinds of services it is appearing in.

The ACMA is an experienced content regulator on matters relating to professional news, satire and authorised electoral content. It has a long history of dealing with these matters and deciding them according to law, and in the public interest.

[30] For example, the ACMA administers technology trial regimes under the *Telecommunications Act 1997* and the *Radiocommunications Act 1992*.

Appropriate civil penalties and enforcement mechanisms for non-compliance.

The civil penalties and enforcement mechanisms for non-compliance proposed in the Bill are adequate and reflect the graduated compliance and enforcement process applying in the co-regulatory frameworks administered by the ACMA, and which apply to other communications and media sector participants.

Yours sincerely

Dr Susanne Lloyd-Jones (UNSW)

Dr Jayson Lamchek (Deakin)

Professor Lyria Bennett Moses (UNSW)