Submission to the Department of Industry, Science and Resources

regarding

Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023

Prepared by Lizzie O'Shea (Digital Rights Watch), Professor Nicolas Suzor (QUT Digital Media Research Centre), and Lucinda Nelson (QUT Digital Media Research Centre).

25 August 2023

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[1]

[1] Learn more about our work on our website: https://digitalrightswatch.org.au/

Overview

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts regarding the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023* (the Bill). We have significant concerns about the breadth of powers that the Bill proposes to grant the ACMA with limited mechanisms for oversight and accountability.

Mis- and dis-information are undoubtedly serious problems. Together, they are a symptom of advertising-based business models that prioritise engagement above all else. Platforms collect extensive personal information that underpins the strategic optimisation of features designed to attract new users, retain attention, and increase interaction with these platforms, allowing them to maximise value to advertisers. Platforms use micro-targeted advertising, automated search, active curation, and algorithmic recommendation systems to amplify the most engaging content. Revenue sharing systems, in turn, create direct financial incentives for content creators to create and share engaging content. The result is a media ecosystem that prioritises engaging content – often content that is polarising, controversial or addictive, including misinformation and disinformation. Consideration of collective concerns, such as the public interest, human rights and community obligations cannot compete with these motivations and in practice are not prioritised by platforms.

We welcome efforts to reduce the spread of mis- and disinformation, but these efforts only target the symptoms of the problem rather than the cause. This is not to say such efforts are in vain, but rather to acknowledge the complexity of the task as presented. It is also to ensure that the very real risks of overreach are addressed and not downplayed in pursuit of an over-simplified solution to the very real problems of mis- and dis-information.

A founding myth of the Internet is that it was a haven for free speech and facilitated the liberation of citizens from the authoritarian reach of the nation state. We accept that this was fantastical thinking; that in fact, algorithmic amplification of content for profit has been a feature of the Internet since its earliest days, as it was in the broadcast era. The curation of online content is nothing new. Having said that, a key priority of policymaking in this field should be to avoid contributing to digital authoritarianism. It is important to resist the temptation to over-police content at the expense of human rights like privacy, freedom of association as well as freedom of speech.

In this context, we wish to raise a number of comments and concerns about the exposure draft for your consideration.

The importance of privacy reform

We note that the *Privacy Act 1988* is currently under review. In our view, strong privacy reform, that favours the rights of users over data extractive business models, is central to tackling mis- and dis-information. The commercial exploitation of individual privacy is a key driver of the business models of digital platforms that encourages the production and spread of divisive and controversial content. For too long, Australia's privacy laws have not adequately reflected public expectations, and the lack of an enforceable personal privacy right continues to be a glaring omission in the international context. Reform to limit the kinds of information that platforms are able to collect, as well as imposing strict limits on how such information can be used for advertising purposes, is key to addressing the root causes of mis- and dis-information by ensuring that engagement for its own sake is less of a lucrative design goal.

The mechanism for the development of Codes risks the abrogation of democratic policy making

We remain concerned about the approach set out under Part 3 of the exposure draft that allows for the creation of Codes, either by industry, or by industry upon invitation of the ACMA. Such an approach to regulation is highly resource intensive and risks the abrogation of democratic oversight over rule-making.

In an environment where the resources of civil society are constrained, and industry faces no such limitations, there is a real risk that this process can become a de facto form of self-regulation. Given the documented bad behaviour by digital platforms, and a public mandate to regulate them, we do not consider such a situation is justifiable.

We appreciate that this model of regulatory rule making brings with it flexibility and responsiveness, which are both important in a field which is subject to rapid change and technological development. However, this ought not be prioritised above accountability. To that end, we recommend introducing formal mechanisms for review of the powers exercised by the ACMA by the Parliament on a regular basis.

The definition of harm is too broad

Key definitions in the exposure draft involve the concept of harm, which is itself defined. We remain concerned that this definition is too broad. In particular, we refer to:

> harm means any of the following:
> ...

(b) disruption of public order or society in Australia
(c) harm to the integrity of Australian democratic processes or of Commonwealth, State, Territory or local government institutions
...
(f) economic or financial harm to Australians, the Australian economy or a sector of the Australian economy

As an example, content that advertises or broadcasts rallies or protests that take place without formal authorisation may meet the definition set out in (b). We remain concerned that content aimed at holding police accountable for violence or discriminatory conduct might constitute harm under (c). Equally, content that challenges Australia's reliance on the fossil fuel industry could potentially be interpreted as giving rise to financial harm to that sector of the Australian economy under (f). Defining harm is undoubtedly challenging, and without any clear and enforceable commitment to human rights principles there is a real risk that such a definition could be interpreted in ways that undermine democratic principles.

The ACMA's powers in relation to misinformation codes and misinformation standards should be limited by Article 19 of the International Covenant on Civil and Political Rights

In its current form, the exposure draft requires the ACMA to consider matters including any burden on the implied freedom of political communication. The regulation of mis- and disinformation raises important human rights concerns, particularly about the right to freedom of expression. The Bill should require that the ACMA be satisfied that any codes or standards are compliant with the international standard for the right to freedom of expression under article 19 of the *International Covenant on Civil and Political Rights*, and that the explanation and rationale for compliance is made public.

The ACMA's information-gathering powers under clauses 18 and 19 should be limited to situations in which there is an identifiable cause of action against the digital platform provider or other person.

Currently, the Bill provides the ACMA with extremely broad information-gathering powers. We are concerned about this expansion of executive power without appropriate mechanisms for oversight and accountability. The extents and limits of these powers should be clearly articulated in legislation, and their exercise should be transparent and reviewable. Given the serious privacy concerns involved, we suggest that their introduction should be postponed until after the completion of the current review of the *Privacy Act 1988*. The information gathering powers should ensure that the ACMA is only permitted to collect information in a de-

identified form. Further, explicit safeguards should be introduced to prevent the use or disclosure of any personal information collected for the purpose of this legislation, including to law enforcement agencies and other public entities. This will ensure that the integrity of protections within other data retention and access regimes is not undermined by additional powers to collect information under this Bill.

The ACMA's powers to require digital platforms to keep records should come with the responsibility to report on these records publicly

Clause 25 of the exposure draft allows the ACMA to publish certain information obtained from digital platform providers about digital platform services. However, it creates no obligation to do so, and it will be up to the ACMA to decide what is published. We think this lacks adequate transparency. A key method for incentivising good behaviour among platforms is to allow the public to make up their mind about the efforts they have made to address mis- and dis-information. Unless there are reporting obligations imposed on the ACMA, there is a risk that information that is the public interest will not be available to the public.

For example, virality of content is very important for engagement on digital platforms, but the viral spread of harmful misleading content is difficult to understand without additional information that is only visible to these platforms. Reporting on the kind of content that goes viral, in ways that allow comparison across platforms and other content types, could be an important insight for the public, the media and academia to assess and assist with designing systemic responses that might justify limits on virality.

The exclusion of professional news content from the definition of mis- and dis-information is problematic

Mis- and dis-information exist and spread within a complex media environment that includes mainstream media organisations as well as social media platforms. The strong financial incentives to create engaging content also apply to content created by mainstream media (defined as 'professional news content' in the exposure draft), and mainstream news organisations encourage, adopt, and amplify harmful and misleading content created by others. Advertising business models provide incentives for mainstream media sources to create an information environment that sows doubt and legitimises disinformation, and professional news organisations are often responsible for concentrating attention on otherwise discredited fringe content.

We think that the government should consider removing the exemption of professional news content from the definition of disinformation.

The Bill should include minimum requirements for the misinformation codes and misinformation standards, grounded in the current research on misinformation and content moderation

The Bill currently provides examples of matters that may be dealt with by misinformation codes and standards, but does not provide sufficient protection for due process. We recommend that the Bill should explicitly require that any misinformation codes or standards mandate appropriate transparency from platforms about their enforcement of misinformation codes and misinformation standards. We also suggest that the Bill should explicitly clarify that the powers to approve codes and standards are to be exercised in relation to systemic responses to mis- and disinformation, rather than focusing on or requiring the removal of individual pieces of content.

Contact

Samantha Floreani | Program Lead | samantha@digitalrightswatch.org.au