

July 2022

AEC Submission

The Australian Code of Practice on Disinformation and Misinformation | Code Review

Introduction

Protecting the integrity of Australia's electoral processes is critical to maintaining public trust and confidence in the legitimacy of Australian democracy. However, misinformation and disinformation about electoral processes can threaten the perceived and actual integrity of electoral events. With recent studies identifying declining levels of trust and satisfaction in Australian democracy,¹ it has never been more important for the AEC to take a strong stance against electoral mis- and disinformation, to protect and promote the integrity of electoral events.

The 2019 Australian Election Study², conducted by the Australian National University, found Australians' satisfaction with democracy was at its lowest since the constitutional crisis of the 1970s, with only 59 per cent of Australians identifying that they were satisfied with how democracy was working.³ This disillusionment and decreased public trust in democratic processes can lead to declining voter participation and increased political polarisation⁴. It can also result in increased critical attention, as well as false narratives and conspiracy theories, being directed toward the regulation of the electoral process, and hence toward the AEC.

Due to the rise of public distrust and increasing volumes of electoral misinformation, the management of electoral reputation has become an increasingly important and challenging task for the AEC. With the perceived integrity of electoral events so closely linked to the reputation of the AEC, effective reputation management is critical to ensure electoral integrity and inspire public trust in election results.

During the 2022 federal election, the AEC saw high levels of misinformation circulating in Australia regarding postal voting, voter fraud, and the impartiality and integrity of the AEC. Particularly since the rise of anti-government sentiments during the COVID-19 pandemic, these false narratives have been gradually gaining influence in Australia, amplified by social media.

False narratives such as these can also be shaped and exploited by foreign and domestic actors seeking to interfere with and undermine electoral processes. Such interference was alleged to have occurred in likeminded democracies such as the US, UK and France.⁵

The proliferation of mis- and disinformation about electoral processes, via both online and traditional media sources, can also result in real world physical security incidents, further threatening democratic institutions and electoral processes.⁶

Recognising the potential danger of widespread electoral mis- and disinformation, section 329 of the *Commonwealth Electoral Act 1918* (the Electoral Act) prohibits content "that is likely to mislead or deceive an elector in relation to the casting of a vote."

This section of the Electoral Act was most recently clarified by the Federal Court, sitting as the Court of Disputed Returns, in *Garbett v Liu*⁷. The Court explained: 'In s 329(1) the phrase "likely to mislead or deceive an elector" means a real chance of misleading or deceiving any elector, even one who is unintelligent, or gullible, or naïve.'

¹ S Cameron and I McAllister, *The 2019 Australian Federal Election: Results from the Australian Election Study*, December 2019, <www.australianelectionstudy.org>.

² Ibid.

³ AEC, *Electoral Integrity: Reputation Management Strategy*, 2021, <https://www.aec.gov.au/About_AEC/files/electoral-integrity-reputation-management-strategy-2021.pdf>

⁴ E Nisbet, C Mortenson, and Q Li, 'The presumed influence of election misinformation on others reduces our own satisfaction with democracy,' *Harvard Kennedy School Misinformation Review*, 12 March 2021, <<https://misinforeview.hks.harvard.edu/article/the-presumed-influence-of-election-misinformation-on-others-reduces-our-own-satisfaction-with-democracy/>>

⁵ AEC, *Electoral Integrity: Reputation Management Strategy*, 2021.

⁶ Ibid.

⁷ [2019] FCAFC 241, at [91].

This precedent is important to understand as it does not simply refer to the practice of electoral campaigning. Any content produced during an election period (from the date of issue to the date of return of Writs for an election) is subject to section 329.

Misinformation and disinformation can have damaging, real life impacts on public perception and participation in Australian democracy. Regulating false and misleading content about the electoral process, particularly online, where misinformation narratives can quickly gain traction and false legitimacy, is vital for the preservation of Australian democracy. Strengthening online platforms' ability to combat the online dissemination of electoral mis- and disinformation should be a high priority for DIGI.

The AEC's responses to the questions outlined in the Discussion Paper are below. Please note questions 4 and 7 will not be addressed as they are outside of the AEC's remit.

Response to Questions

1) Should the ACPDM cover a broader scope of signatories? If so should:

- a) the ACMA have a continued role in identifying those services that are within the scope of the code; and
- b) what should the criteria be for a company's eligibility to participate in the code?

The AEC supports the ACPDM (the code) being extended to cover a broader range of signatories. In addition to user-generated content and search platforms, this expanded scope could include platforms which host non-user generated and professionally published content, such as podcasts, shows, videos, news and blogging sites. The inclusion of large-scale groups and chats on private messaging platforms would also be beneficial, as these can be prominent sources of harmful mis- and disinformation.

To broaden the scope of signatories and hence the reach of the code's mandate against mis- and disinformation, DIGI could consider permitting any content-hosting online platform to adopt the commitments outlined in the code. Encapsulating a broader range of platforms could allow the code to more effectively meet the needs of Australian users by combatting the harms of mis- and disinformation on a much wider scale.

The AEC recognises that the code is an industry initiative, making DIGI, as an industry body, the best placed entity to be proactively seeking new signatories. In particular, it would be beneficial to the Australian community for DIGI to seek out platforms which are known vectors of disinformation and encourage them to commit to the code.

2) Should the ACPDM take an opt-out rather than an opt-in approach to the optional commitments under the code?

An opt-out approach to the optional commitments would encourage a more consistent industry-wide standard for the countering of harmful mis- and disinformation. This could enable, for example, a more consistent application of political advertising and authorisation standards across platforms, allowing a wider audience of Australians to better understand the sources of political advertisements they come across online.

As these additional commitments are designed to better protect Australians from the harms of mis- and disinformation, and improve the user experience, where an optional commitment of the code is relevant to a platform's structure, design and/or content, platforms could be required to justify any decision to opt-out.

An opt-out approach also sets a higher standard for the code, recognising that in its most effective, exemplar form, every relevant commitment is adopted by the applicable respective platforms. By encouraging platforms to adopt these further commitments against mis- and disinformation, the code will be better equipped to address the concerns and needs of the Australian public.

3) Should the definition of harm be amended to deal with concerns about the narrowness of 'serious and imminent threat' language?

The AEC endorses the Discussion Paper's view that the current definition of harm adopted by the code is too narrow to adequately protect the online community and broader Australian society from the often cumulative and chronic harms which can be caused by mis- and disinformation.

While acknowledging the difficulties in foreseeing which, and when, instances of mis- and disinformation will cause serious harms in the future, the AEC believes a stronger approach to combatting this content in its early stages will be of significant benefit to the community in the longer term. Patterns, trends, and recurring themes of mis- and disinformation can and should be proactively picked up by platforms before they escalate to the point where they pose a "serious and imminent threat" to society.

Lowering the threshold for the definition of harm adopted by the code, particularly the requirement that it be "imminent", will open the door for more preventative and early-intervention measures against electoral misinformation. This will minimise necessity for the more large-scale interventions that may be required once harmful misinformation trends have gained momentum on an online platform. It will also encourage an approach which prevents misinformation-related harms from occurring in the first place, rather than one which waits for a "serious and imminent threat" to cumulate before attempting to suppress an already widespread misinformation problem.

In particular, the broader societal harms which can result from electoral mis- and disinformation do not always appear to be "imminent", and yet can have serious and damaging effects on Australian society. The cumulative nature of these broader societal harms can critically degrade the ability of Australians to understand and participate in the electoral process, and encourages widespread, unfounded distrust in civic institutions. This distrust, encouraged and fuelled by mis- and disinformation, can result in real world physical security incidents, and threatens the overall stability and longevity of Australian democracy.

To counter the increasing levels of electoral mis- and disinformation, collective government efforts to publicly communicate the integrity of electoral processes increased substantially for the 2022 federal election. With conspiracy theories and false narratives regarding electoral processes gaining influence due to their unrestrained online proliferation, the perceived integrity of electoral events is now being increasingly challenged. The need to positively influence perceptions of electoral integrity and instil public trust in election processes and results has never been greater.

Noting this, the AEC proposes the threshold for defining harmful misinformation be lowered to more accurately reflect all types of misinformation, including those less "imminent" but which nevertheless contribute to broader societal harms.

Currently, code signatories have varied interpretations of what constitutes 'harmful' mis- and disinformation. This was made clear to the AEC during the 2022 federal election, when upon being referred Pauline Hanson's One Nation's 29 April 2022 'Please Explain Voter Fraud' video, some platforms judged the misinformation in the video to be harmful, and removed it, while others disagreed and did not take any action against the content on such grounds. The video made the following false claims:

- Identification is not required to enrol
- Dead people are enrolled to vote
- Australia's 2010 Federal Election was won by a smaller margin than the number of alleged multiple votes
- One political party is engaged in widespread electoral fraud

The lack of consensus around the definition of ‘harmful’ misinformation led to delays in platform action and resulted in an inconsistent industry approach to combating electoral misinformation. Clarity as to the definition of harm can be facilitated through the broadening of its scope, hence allowing a more consistent and effective industry approach to tackling harmful misinformation.

5) Should the code be extended to include private messaging?

The AEC notes that ‘private messaging’ is not currently defined in the code. In practice, the term appears to be used to define any form of messaging ranging from one-on-one messages between individuals, to public chatrooms, groups or channels in applications such as Telegram, Facebook Messenger, and other ‘private messaging’ apps. These groups may include tens of thousands of users. The AEC views this latter form of communication as a strong and currently unregulated vector for electoral mis- and disinformation.

The AEC endorses the ACMA’s proposal to amend the code to introduce a category of public or ‘semi-public’ messaging.⁸ This would rectify the loophole in the current code and allow the AEC to work more closely with platform holders to address this vector for electoral mis- and disinformation.

6) Should the approach to issues-based advertising be clarified?

As noted in DIGI’s Discussion paper, the code does not regulate truth in political advertising if it has not been identified as part of a disinformation campaign. Additionally, truth in political advertising is not regulated by federal legislation. One limited exception to this is the offence listed in the Electoral Act, which prohibits the publication or distribution of material during an election period that misleads voters regarding the casting of a vote, including political advertisements. This legislation is specific to content misleading voters about the electoral process and does not regulate other advertisement information during an election campaign. Any changes to the current regulation of truth in political advertising would be a matter for the federal parliament.

The Electoral Act’s provisions on misleading material apply to federal elections and do not extend to referendums. However, the *Referendum (Machinery Provisions) Act 1984* also makes it an offence to publish or distribute material during a referendum period that misleads voters regarding the casting of a vote.

8) Is the code meeting community and industry needs to balance concerns about mis- and disinformation with freedom of expression?

The AEC opposes the proposal to drop the term ‘misinformation’ from the code. While the AEC recognises the difference between misinformation and disinformation, largely relating to the intent of the communicator, the experience of the AEC during the 2022 federal election (as well as previous electoral events) was that deliberately circulated electoral disinformation can and does quickly evolve into unintentionally circulated electoral misinformation.

As such, only including disinformation in the code, and not the misinformation which so often accompanies disinformation campaigns, can only serve to weaken DIGI’s perceived and actual power to prevent the spread of electoral disinformation. Taking a stance against disinformation while permitting the proliferation of misinformation only allows disinformation narratives to spread further and faster, without restraint.

Regardless of its lack of malintent, misinformation still has the potential to cause harm, just as disinformation does. The AEC therefore pursues similar courses of action to prevent the spread

⁸ Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia: A position paper to guide code development*, June 2020.

of misinformation as it does disinformation. This synonymous approach to mis- and disinformation recognises the potential for harms in both forms of misleading content.

Contrary to DIGI's proposal to remove misinformation from the code, the AEC instead recommends adding malinformation to the Code. Malinformation, like mis- and disinformation, can be described as digital content that is reasonably likely to cause harm. Unlike mis- and disinformation, however, malinformation is not necessarily false information, and yet it is presented, often out of context, in a way that misleads. For example, an out of date news article used as 'evidence' of a false conspiracy theory would constitute malinformation. While aspects of the fight against malinformation are addressed by the code's definition of inauthentic behaviour, the AEC considers the specific inclusion of malinformation in the code to be beneficial for the following two reasons.

Firstly, the inclusion would draw a 'line in the sand' on the practice of malinformation, sending a clear message from DIGI members that the use of malinformation to mislead the community is unacceptable. Secondly, the inclusion would complete the code, which currently excludes an important aspect of inauthentic behaviour.

As an example, in April of 2022 the AEC referred to a code signatory platform holder a widely-shared post using articles from 2019 in such a way as to suggest they referred to a current issue. This was a clear example of electoral malinformation, but despite the AEC's report citing the platform's own manipulated media policy the referral was rejected and the post allowed to remain online. A clearer focus on malinformation in the code could clarify matters for platform holders at future elections.

The AEC notes concerns in the Discussion Paper around the protection of freedom of expression. The AEC shares these concerns, however, notes that disseminating mis- or disinformation in relation to the casting of a vote is already prohibited by section 329 of the Electoral Act.