

Review of the Australian code of practice on disinformation and misinformation

ACMA submission

NOVEMBER 2025

Canberra

Level 3
40 Cameron Avenue
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne

Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney

Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
F +61 2 9334 7799

Copyright notice



<https://creativecommons.org/licenses/by/4.0/>

Except for the Commonwealth Coat of Arms, logos, emblems, images, other third-party material or devices protected by a trademark, this content is made available under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) licence.

All other rights are reserved.

The Australian Communications and Media Authority has undertaken reasonable enquiries to identify material owned by third parties and secure permission for its reproduction. Permission may need to be obtained from third parties to re-use their material.

We request attribution as © Commonwealth of Australia (Australian Communications and Media Authority) 2025.

Contents

Executive summary	4
Introduction	7
ACMA's oversight and reporting role	7
Scope of the submission	8
PART 1: CODE CHANGES	9
Scope of the code	12
Transparency reporting framework	15
ACMA's proposed framework	18
Futureproofing the code	21
Researcher access to data	22
PART 2: OPERATION OF THE CODE	23
Operation of governance arrangements and reporting	23
Code complaints	23
Broader information ecosystem	24
Appendix A: Pilot measurement framework	26
Appendix B: Process to develop framework	37

Executive summary

Australians are increasingly concerned about misinformation online

Misinformation is an issue of concern for Australians. According to new ACMA research¹, 72% of Australian adults who used a digital platform believe they encountered some form of misinformation on a platform in the last 6 months (from June 2025).

The 2025 Digital News Report, undertaken by the University of Canberra, found that 74% of Australian adults were concerned about misinformation – the highest globally².

The Code is the primary way for digital platforms to demonstrate their ongoing commitment to tackling disinformation and misinformation

Reporting under the [Australian Code of Practice on Disinformation and Misinformation](#) (the code) remains the primary way for digital platforms to demonstrate that they are taking Australians' concerns about disinformation and misinformation seriously and are taking active steps to prevent and mitigate harm.

The ACMA oversees the self-regulatory code and platform efforts to address disinformation and misinformation. In this context, our submission provides the ACMA's views on the code and its associated framework, in addition to responding to the issues outlined in DIGI's [discussion paper](#). This submission should be read with reference to the ACMA's [four reports](#) to the Australian Government on the code.

The existing scope of the code should be retained

We strongly recommend that the existing scope is retained to include misinformation. One of the code's key strengths is allowing signatories to commit to reporting on a proportional range of interventions to address different levels of harm caused by disinformation and misinformation.

The ACMA accepts that this topic is complex, poses 'wicked' policy issues, and it is important that freedom of expression concerns are appropriately surfaced. However, rather than limiting the scope of the code we suggest this issue can and is already being addressed by a range of ameliorative interventions which could be expanded. This is appropriate for a self-regulatory arrangement.

We know that misinformation can cause significant harms regardless of whether its dissemination was intentional or not. Removing misinformation is likely to reduce transparency about signatories' actions under the code, and reduce the baseline safeguards the code currently provides for the end-users of signatories' services. While the full impact would be dependent on specific drafting, areas where safeguards may be reduced include overarching policies and processes, digital literacy interventions and advertising on signatories' services.

¹ Annual Consumer Survey 2025, ACMA

² News and Media Research Centre, (2025), '[Digital news report Australia: 2025](#)', accessed 14 October 2025.

Reduced obligations will result in less transparency about platform actions and their effectiveness in signatories' annual reports. This is particularly important given the levels of public concern around misinformation. The contentious nature of the issue and various ways it can be mitigated require greater transparency about the efforts undertaken by signatories and their effectiveness.

Strengthening the code's reporting framework should be an immediate priority

The reporting framework is an area that requires attention, and the review provides the opportunity to uplift arrangements. Improved transparency about signatories' actions and measures will allow the effectiveness of the code to be more accurately measured and is essential if voluntary arrangements are to be successful.

We propose that the reporting framework is incorporated into the code, rather than in associated guidelines, and covers three main areas:

- A more standardised approach to capture signatories' measures to achieve the objectives and outcomes they have committed to under the code. Separate arrangements could be implemented for smaller signatories that offer services that are not directly responsible or at-risk of disseminating misinformation and disinformation.
- A set of cross industry metrics to assess the effectiveness of measures and interventions across the code that signatories have in place to meet their commitments under the code. Metrics may not be relevant to all signatories, depending on the services they provide.
- Key performance indicators developed by each signatory, which will contribute to a better understanding of the impact of signatories' actions under the code. These could be accompanied by Australian specific data which is trended over time.

The ACMA has undertaken work to develop a draft reporting and measurement framework that would better allow more consistent reporting about signatories' efforts. This work has been informed by consultation with signatories and across government, and advice from independent experts.

The review provides the opportunity to look at other improvements such as future proofing the code

Other code amendments that should be considered could focus on:

- Futureproofing the code – including clarifying application to new AI services to encourage broader participation and encouraging signatories to proactively assess disinformation and misinformation risks when introducing major changes to their policies, processes, and systems.
- Increased transparency about what arrangements are available for Australian researchers to access digital platform data to conduct public interest research on disinformation and misinformation.

Improving the governance of the code

We support DIGI's process in reviewing the code's governance framework and administrative arrangements. We recommend the focus should be on improving the code's complaints process, given current numbers do not align with reported community concern about these issues.

We welcome the opportunity to engage with DIGI and code signatories on amendments and improvements to both the code and the associated guidelines and processes to enhance the operation of the code.

Introduction

The Australian Communications and Media Authority (ACMA) is the independent statutory authority responsible for the regulation of broadcasting, radiocommunications and telecommunications in Australia. Our regulatory remit also includes some aspects of online content regulation, for example, restrictions on gambling advertising during live streamed sport and interactive gambling services.

In Australia, minimising the risk of harm from disinformation and misinformation on digital platforms has been the subject of self-regulation since 2021. The [Australian Code of Practice on Disinformation and Misinformation](#) (the code) was developed by the Digital Industry Group Inc. (DIGI) in February 2021 at the request of the Australian government. The code is administered by DIGI and requires that signatories take action to identify, assess and address disinformation and misinformation on their services. The code currently has 8 signatories: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitch.

The voluntary code remains the primary way digital platforms can demonstrate they are taking Australians' concerns about disinformation and misinformation seriously – and taking steps towards preventing and mitigating harm.

As is required under the code, DIGI has recently commenced its second code review and has published a [2025 Review Discussion Paper](#) to inform public consultation.

ACMA's oversight and reporting role

In December 2019, the ACMA was tasked by the then government to oversee the code's development and, since that time, we have [annually reported](#) to the government on the code. Our [fourth report](#) was published in September 2025.

In March 2025, in response to the government's [statement of expectations](#), the ACMA said it would continue working with digital platforms to improve transparency of their actions to combat disinformation and misinformation while protecting freedom of speech under the code.

The ACMA has commissioned a range of research to support our oversight of the voluntary code and inform our reports to government. This includes:

- research on Australian adults' experience with encountering misinformation (report to be released later in 2025)
- [research](#) on the experiences of adult Australians who had reported or complained about harmful content (including misinformation) on digital platforms.
- a [longitudinal study](#) by the University of Canberra's News and Media Research Centre on Australians' access to, consumption of, and critical engagement with news, information and misinformation during the COVID-19 pandemic.

The ACMA also works with industry to improve voluntary arrangements that would boost transparency for Australian end-users. During the second half of 2024, we developed a draft measurement framework to assist in improving the quality and consistency of transparency reporting. We consulted with industry on a more targeted list of measures and metrics which – if adopted – would support more consistent, industry-wide reporting on the effectiveness of signatories' efforts to address disinformation and misinformation.

Given our ongoing oversight and reporting role, the ACMA welcomes the opportunity to contribute to the review and welcome further engagement with DIGI and signatories on potential changes to the code.

Scope of the submission

We have structured our submission in two parts:

- > **Part 1: Code changes** – focuses on the evolution of the code and code content. This includes our views on the scope of the code and the transparency reporting framework.
- > **Part 2: Operation of the code** – focuses on other issues not directly related to the content of the code such as the operation of the code's governance framework and links to the code's role in the broader ecosystem.

PART 1: CODE CHANGES

Since its commencement in 2021, the code has provided valuable insights into how major digital platforms in Australia address disinformation and misinformation.

The outcomes-based approach offers signatories the flexibility to opt-in to report on measures that are relevant and proportionate to their individual services and business models. This approach also encourages signatories to regularly review their commitments, providing transparency on any changes to the measures or outcomes adopted in each report.

In its first code review in 2022, DIGI and signatories made improvements to the voluntary arrangements, particularly:

- the expansion of the code's scope to include a broader range of potential signatories, including advertising and technology companies
- changes to the harm threshold to be 'serious and credible' rather than 'serious and imminent', which gave signatories the opportunity to more appropriately reflect the range of measures they have in place to combat disinformation and misinformation
- introduction of a new outcome 1e, which gives information on how users can access general information about the use of recommender systems, and have options related to content suggested by recommender systems
- introduction of a new opt-in commitment to deter advertisers from repeatedly placing advertisements that consistently propagate disinformation and misinformation
- revised reporting arrangements for smaller signatories, aimed at alleviating some of the reporting burden.

The code's reporting framework allows signatories to provide transparency about their systems, processes and measures in combatting disinformation and misinformation. The present review provides an opportunity for DIGI and signatories to examine areas that were not considered in 2022, and to reflect how the code can be improved for the current and future environment.

Australians consider misinformation is a serious problem

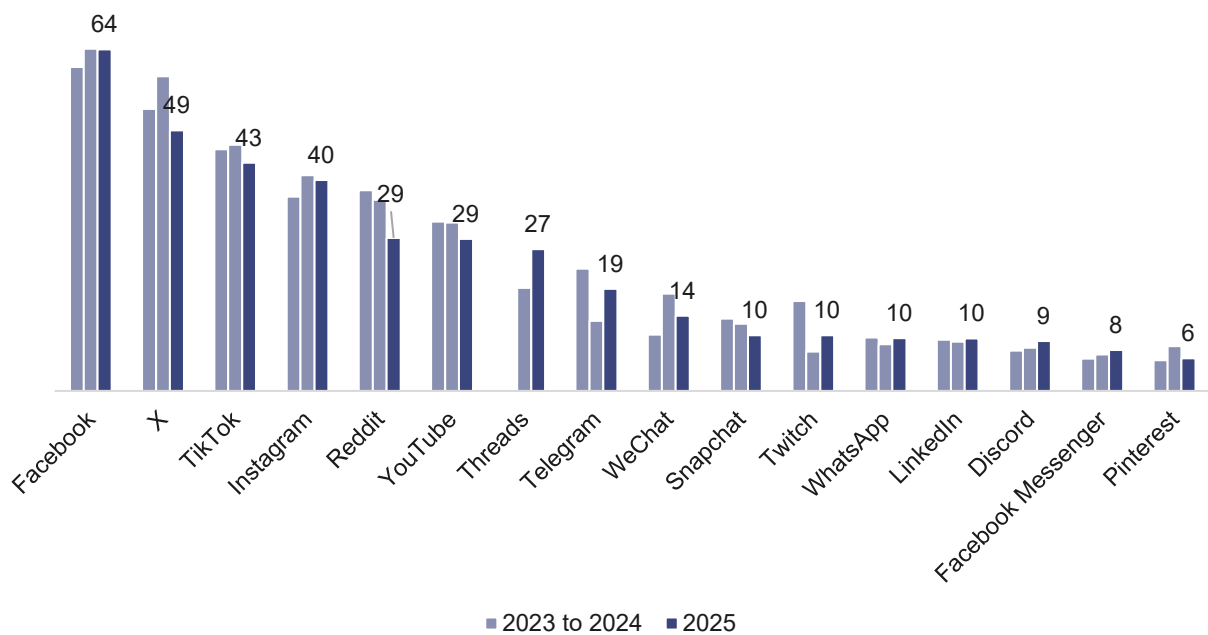
Australia's information ecosystem is challenged by harms from both disinformation and misinformation. The Australian Security Intelligence Organisation's 2025 Threat Assessment identified the erosion of social cohesion and trust in institutions through disinformation and misinformation as critical challenges to our national security environment³. Similarly, the Department of Home Affairs' Strengthening Australian Democracy report highlighted these issues as a key challenge to Australia's democracy⁴.

³ Mike Burgess, ASIO Annual Threat Assessment 2025, Office of National Intelligence, 19 February 2025, accessed 14 October 2025.

⁴ Department of Home Affairs, Strengthening Australian democracy, [PDF], Department of Home Affairs website, 2024, accessed 14 October 2025, p. 2.

74% of Australian adults surveyed for a recent Digital News Report⁵ expressed concern about misinformation – the highest globally. In forthcoming consumer research undertaken by the ACMA in June 2025, 72% of Australian adults who had used a digital platform reported having seen or heard misinformation on digital platforms in the previous 6 months⁶. The proportion of users of each platform who encountered misinformation differed across platforms, as evidenced by Figure 1. The charts below are taken directly from the forthcoming report.

Figure 1: Communication and social media websites/apps where misinformation was seen or heard: Users of each platform in the past 6 months to June 2025 (%)

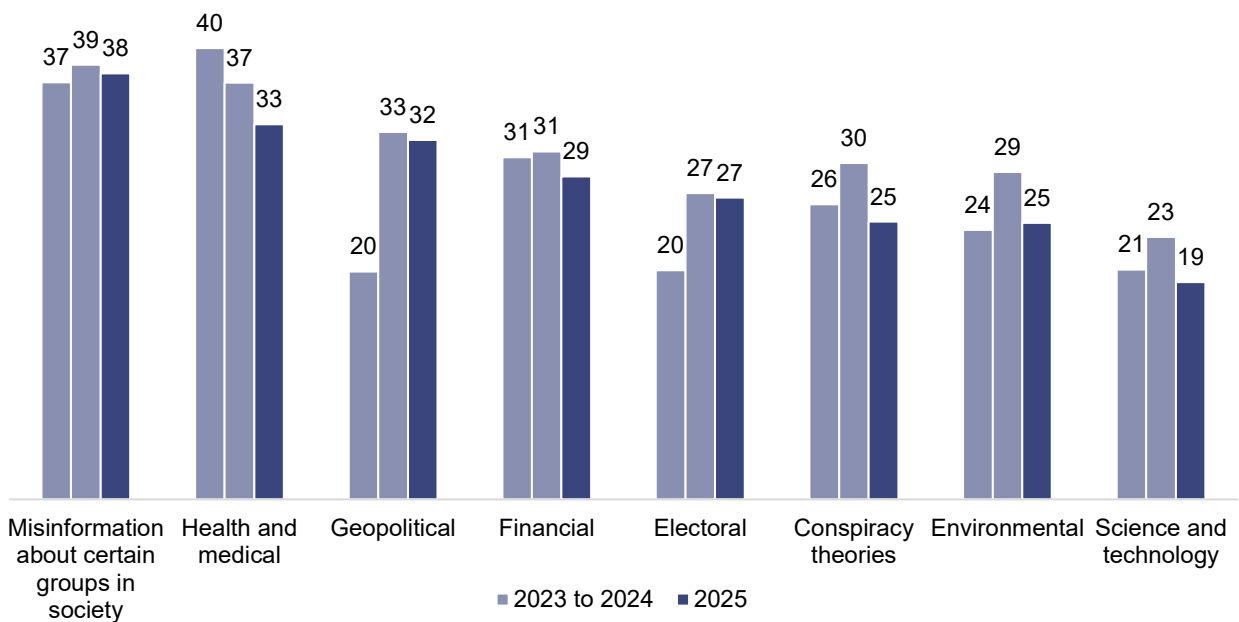


Base: Australians aged 18 and over who used each specific platform in the past 6 months.
Note: ‘Don’t know’ and ‘Refused’ are 2% and 0.1% respectively (of Australian adults who used a communications or social media website or app in the past 6 months (QE2)).
Source: Unpublished research: ACMA annual consumer survey, E22.

Australian adults encountered a diverse range of misinformation topics in 2025. Misinformation about conspiracy theories, health and medical topics, environmental issues, and science and technology saw a decline from 2024.

⁵ News and Media Research Centre, (2025), ‘[Digital news report Australia: 2025](#)’, accessed 14 October 2025.
⁶ Annual Consumer Survey 2025, ACMA

Figure 2: Nature of the most recent misinformation seen or heard: Australian adults who saw or heard misinformation in the past 6 months to June 2025 (%)



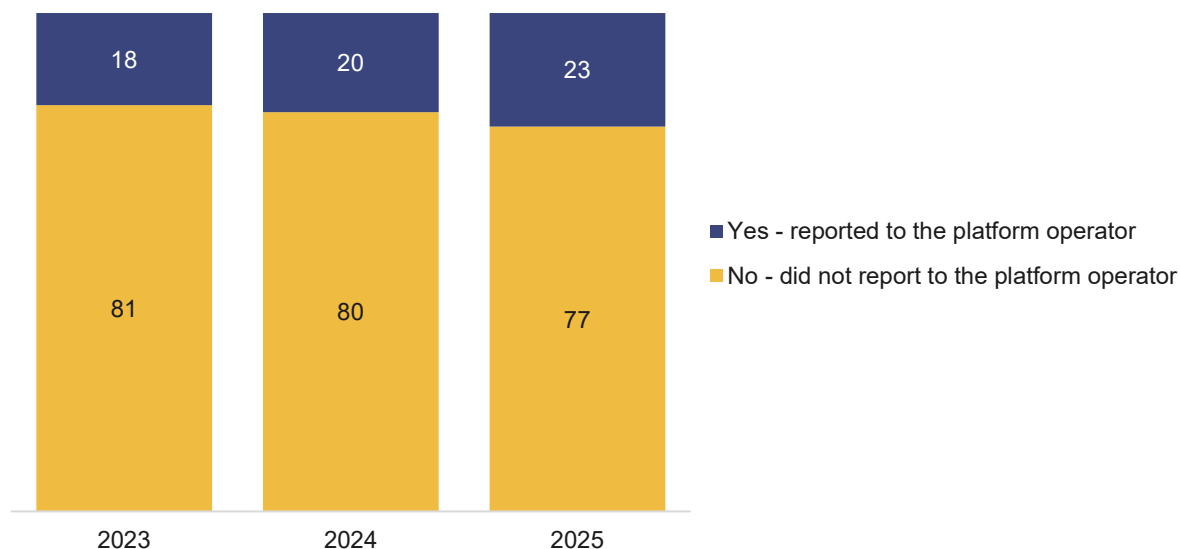
Base: Australian aged 18 and over who saw or heard misinformation in the past 6 months 2023 (n=2,097), 2024 (n=2,336) 2025 (n=4,144).

Note: Results for 'Other', 'Don't know' and 'Refused' are <2% and not shown.

Source: Unpublished research: ACMA annual consumer survey, E26.

Reporting potential misinformation by Australian adults is an area that we have continued to track in our consumer research. In 2025, 23% of Australian adults who saw or heard misinformation made a report to the platform operator about the most recent misinformation type they encountered.

Figure 3: Most recent misinformation seen or heard reported to the platform operator: Australian adults who saw or heard misinformation in the past 6 months to June 2025 (%)



Base: Australian aged 18 and over who saw or heard misinformation in the past 6 months 2023 (n=2,097), 2024 (n=2,336) 2025 (n=4,144).

Note: Results for 'Other', 'Don't know' and 'Refused' are <2% and not shown.

Source: Unpublished research: ACMA annual consumer survey, E27B.

It is clear that Australian end-users are encountering misinformation on digital platforms and are concerned about potential impacts and harms to themselves and broader Australian society.

Scope of the code

In its discussion paper, DIGI pose a threshold question about whether the code should continue to regulate disinformation and misinformation or focus on disinformation only.

DIGI notes that misinformation is often subjective and tied to personal beliefs, while disinformation is more objectively harmful and coordinated. Further, DIGI suggests that high levels of public concern about misinformation aren't necessarily indicative of public exposure to false or misleading materials, and that misinformation comprises only a small proportion of the typical user's news and information consumption online.

The ACMA's view is that the existing scope of the code be maintained. In our original position paper to guide the development of the code, the ACMA recommended that industry take a broad view of the issue and develop a code that addresses all kinds of false, misleading or deceptive online information with the potential to cause harm. This recommendation reflects that misleading information shared without intent to cause harm can and does lead to significant harm to both users and the broader community. In the position paper, the ACMA also recommended that responses to misinformation should be proportionate to the risk of harm, with free expression to be an essential consideration in the assessment of misinformation.

The ACMA does not disagree this is a complex issue requiring careful attention to legitimate concerns about freedom of expression. In developing the code, DIGI has already successfully allowed for a flexible framework that supports the protection of freedom of expression (clause 2.1) through the inclusion of a proportionality provision (clause 6.1), outlining that measures should be proportionate and relevant to their specific context. The ACMA also recognises that signatories currently grapple with this balancing act every day in the enforcement of their terms of service and community guidelines.

As a result, the current scope of the code has allowed an appropriate balance between protecting freedom of expression and providing transparency about the actions signatories are taking to mitigate harmful disinformation and misinformation. This approach has encouraged signatories to implement measures to address issues that weaken broader information integrity – such as labelling AI content, fact-checking, improving access for third-party researchers, promoting authoritative information, and engaging in media literacy initiatives. These broader efforts all contribute to building trust and transparency which are critical to the success of the code.

DIGI should continue to utilise existing mechanisms so that freedom of expression is protected while maintaining the scope of the code to include misinformation and the various responses to mitigating its serious harms. Signatories should continue to monitor and address this issue through a range of ameliorative interventions which could continue to be expanded over time. We fear that if commitments relating to misinformation were removed from the code, there may be less incentives for signatories to continue applying effort and resources to combating misinformation on their services.

In addition to the more general comments above, removing misinformation from the scope of the code risks detrimental flow on impacts resulting in less transparency about signatories' actions (as articulated within their annual transparency reports under the code) and reduced safeguards for users of signatories' services. We detail some of these considerations below, noting that the full extent and impact will be dependent on specific drafting changes to the code and any subsequent changes to signatories' services, policies and initiatives.

Reduced transparency about platforms' actions

Reduced obligations that signatories are required to report on will result in less transparency about their actions and their effectiveness in annual reports produced under the code. The ACMA has repeatedly emphasised in our reports that providing consistent quantitative and qualitative data – including Australian-specific points – assists in enabling year-on-year comparisons, improving understanding of platforms' policies, and providing clear and comprehensive information to Australian end-users.

The ACMA is concerned about the utility of reporting under the proposed new scope given the majority of the data provided in platforms' reports relates to misinformation. For example, in our fourth report to government, the ACMA found that signatories did not report Australia to be the target of any coordinated influence operations on their platforms in the 2024 reporting period. Therefore, most data and case studies provided on disinformation has related to international examples. Taken to an extreme, there is a danger that no Australian data points could be provided in future if the scope of the code was reduced, subsequently providing less transparency in reports about signatories' actions.

Further, as the code allows content to be reported under broad 'misinformation and disinformation' policies, it is unclear how content is differentiated to detail specific data points on disinformation. Without any specific case studies or data on disinformation, it is unclear what reporting would look like under the proposed new scope.

This reduction in transparency is particularly important given the levels of public concern around misinformation. The contentious nature of the issue and various ways it can be mitigated require greater transparency about the different efforts undertaken by signatories and their varying effects. Reduced data points may also lead to less Australian data and information being available to independent researchers. This limits transparency around the effectiveness of actions undertaken by platforms to mitigate harm.

Reduction of safeguards against harms that may arise from misinformation

The ACMA's original position paper outlined that a single industry code would enable a more consistent experience for Australians who regularly use multiple platforms. ACMA research has found that three quarters of Australians used an average of 4+ digital platforms in the six months to June 2024⁷.

The code acts as a safeguard across industry to protect Australian end users against harms that may arise from disinformation and misinformation. We know that misinformation can cause significant harms regardless of whether its dissemination was intentional or not. Reducing the scope of the code may provide an incentive for some signatories to change their policies and procedures, limiting the ability of the code as a whole to provide safeguards. Areas in which safeguards would be limited and/or removed may include those listed below.

Relevant code provision	Potential impact
Objective 1 requires signatories to provide safeguards against harms arising from disinformation and misinformation	<ul style="list-style-type: none"> • Clause 5.9 outlines a range of measures platforms may adopt to demonstrate this, including labelling false content, providing metadata about content sources, and enforcing published editorial and content standards. • Excluding misinformation from the code's scope would narrow the application of these measures resulting in reduced data and transparency from signatories.
Objective 2 requires signatories to disrupt advertising and monetisation incentives for disinformation and misinformation.	<ul style="list-style-type: none"> • Excluding misinformation from the scope of the code would reduce platforms' obligations relating to advertising shown on their services. As noted in our original position paper, the control platforms have over their advertising services, and the monetary benefit they obtain, places a greater responsibility on them to address the use of advertising services for the dissemination of misinformation. • Under Outcome 5, political advertising is excluded from the scope of misinformation to protect freedom of expression, while including additional protections to minimise misinformation in advertising more generally.
Outcome 4 Users are enabled to make more informed choices about the source of news and factual content accessed via digital platforms and are better equipped to identify Misinformation	<ul style="list-style-type: none"> • Removing this outcome and its related measures will remove the obligation for signatories to detail their work on promoting digital literacy interventions and supporting partnerships with fact-checking organisations.

⁷ Australian Communications and Media Authority (2024), [Communications and Media in Australia: How we communicate](#), accessed 31 October 2025, p. 8

<p>Clause 5.26 requires signatories to support and encourage good faith independent efforts to research disinformation and misinformation.</p>	<ul style="list-style-type: none"> Reducing the scope of the code could lead to less information and data available to researchers to evaluate the effectiveness of platforms' initiatives; particularly for those platforms that do not independently publish transparency reports. Further, as disinformation typically results in content removal – and therefore may no longer be available to access – data around misinformation is particularly important for researchers to understand the effectiveness of diverse responses in mitigating harm.
<p>Clause 6.1 requires measures taken by signatories to be proportionate to the level of Harm posed by disinformation and misinformation content.</p>	<ul style="list-style-type: none"> This is a key safeguard for balancing harm and freedom of expression. As platforms typically apply stronger interventions to disinformation, such as content or account removal, it is unclear whether the proportionality clause would still be included in the code. Proportionality is particularly important for misinformation given it provides signatories to implement a graduated range of actions commensurate with the relevant context and risk of harm.

The ACMA considers maintaining the current scope of the code to include both disinformation and misinformation is essential to upholding safeguards, transparency and public trust. A narrowed scope will result in fewer opportunities for Australians to see how signatories are working to protect them against misinformation harms, limiting the effectiveness of the code.

Transparency reporting framework

Annual transparency reporting is critical to the success of the code, as we noted in our original position paper and in our four subsequent reports to government. The signatories' flexibility in determining what measures to adopt to meet the code comes with the responsibility of providing enough data and information to assess signatories' progress to achieving the code's outcomes over time.

While there have been some improvements in reporting over the years, the reporting framework is an area that requires attention, and the review provides an opportunity to uplift arrangements. Improved transparency about signatories' actions and measures will allow the effectiveness of the code to be more successfully measured and is essential if voluntary arrangements are to be successful.

Development of reporting framework

The ACMA acknowledges the significant evolution and improvements to the reporting framework, since its inception, including the development of the Best Practice Transparency Reporting Guidelines. When the code was first launched in February 2021, it contained an initial report template that signatories were required to complete within 3 months of the code's commencement. Under section 7.3 of the code, signatories also committed to develop and implement, within 6 months of code's commencement, an agreed format for future annual reports and a guideline to inform the data and other information to be included in subsequent reports.

DIGI commissioned the independent reviewer to develop a new template and the guidelines which were introduced in March 2022.⁸ We acknowledge the considerable work that has gone into the development of the guidelines, including its updates in 2024. Following feedback, including from the ACMA, in 2024, DIGI asked its independent reviewer to update the Best Practice Transparency Reporting Guidelines to:

- include specific requests for clear explanations of major changes in policy information
- include specific information about efforts to combat Gen AI misinformation
- update the table of code signatories to reflect withdrawals and additions
- highlight areas for continual improvement based on analysis of past reports including key performance indicators (KPIs).

As a result of these updates, the signatories' annual transparency reports for 2023 and 2024 included increased information about their responses to AI. This was a significant improvement which we were pleased to see. We expect that the reporting framework will continue to develop as the code matures and as community expectations evolve.

Current reporting framework

Each signatory to the report with a user base in excess of one million monthly active Australian end-users is required to reassess the extent that the objectives and outcomes are relevant to their products and services (see clause 7.1) and provide an annual transparency report to DIGI, covering the previous calendar year (see clause 7.3). Each report must list the products and services subject to the code and set out the signatory's progress towards achieving the code's outcomes.

The reporting arrangements are supported by the Best Practice Transparency Reporting Guidelines and the current version is set out in Appendix A to DIGI's 2024 Annual Report on the code⁹. These guidelines request that signatories provide trended, Australian-specific data, accompanied by clear explanations of policy changes, in audience-friendly documents that have a minimum of promotional language. Notably, the guidelines state that a "minimum of three years of reporting should be supplied with any data" and "urge" signatories to "identify and commit to appropriate internal KPIs".

Signatories' annual transparency reports are considered by an independent reviewer before being lodged with DIGI by May 30 each year and are then published on its website. The independent review process involves fact checking each signatory's report, providing feedback to signatories about potential improvements to their reports and making recommendations about best practice reporting. A short summary by the reviewer is included in DIGI's annual report. Recently, DIGI has also begun identifying highlights from the transparency reports in its annual report. The ACMA also reviews and provides feedback on each transparency report for its own report to government, as part of its oversight role.

Separate reporting arrangements were introduced following the 2022 review for smaller digital platforms. Clause 7.4 requires these smaller platforms to provide a report to DIGI within 12 months of entering the code regarding their progress towards achieving the outcomes, to be published on the website. Any material changes to the report are to be provided annually.

⁸ Australian Code of Practice on Disinformation and Misinformation | Annual Report, May 2024, page 10.

⁹ Australian Code of Practice on Disinformation and Misinformation | Annual Report, May 2024, page 14.

Reviews of the Best Practice Transparency Reporting Guidelines are separate to reviews of the code. There does not appear to be a set requirement for regular review of the guidelines.

Assessment of current reporting framework

Developing reporting frameworks is challenging, as evidenced in Australia as well as in the European Union. While signatories are investing considerable amounts of effort in producing their reports, the ACMA has, in each of its reports to government to date, found that the signatories' reporting has gaps and would benefit from uplift. As an outcomes-based code, it is crucial to its success that signatories provide appropriate data and transparency to show how they are progressing to meet the code's objectives and outcomes.

This could be addressed by making specific improvements in the code's reporting framework, some of which are described below.

Lack of key performance indicators and metrics

KPIs

Key performance indicators (KPIs) are an important method to measure how effectively signatories to the code are performing against the objectives and outcomes they have opted in to. While this issue was emphasised in our 2021 report to government and has been highlighted by the independent reviewers, signatories have consistently failed to identify their own meaningful internal KPIs and consistently report against these KPIs. Without KPIs, it is difficult to determine whether signatories consider their efforts to be successful.

Instead, most signatories have continued to provide isolated data points that can change year on year. We have found that there has been a lack of consistent, trended Australian-specific data points against all outcomes, reported to the same level of granularity each year. This limits users' ability to verify whether signatories' measures are effective in combatting misinformation and disinformation and is a significant barrier to the effectiveness of the reporting framework.

In addition to the above, a lack of qualitative analysis, such as an explanation of what has contributed to material changes, makes it difficult to understand the data points that have been provided, or trends over time. Such analysis would help to avoid incorrect interpretations and comparisons of the data.

Metrics

While we are aware this is not an easy task given the diverse range of signatories, the lack of standardised metrics across the code for signatories to report against makes it difficult to compare signatories' efforts or develop an evidence-based assessment of the effectiveness of the code.

Because the guidelines do not specify the metrics for signatories to report against, signatories have only provided isolated data points with limited meaningful analysis.

Inaccessible reports

The suggested template for reports, as set out in Appendix 2 to the code and described further in the Best Practice Transparency Reporting Guidelines, has not been widely adopted by signatories, limiting its usefulness.

The current template was also developed when the code was first established. As we enter the 5th year of reporting, annual reports are becoming harder to understand. It is becoming increasingly unclear, on the face of each annual report, what (if any) year-on-year changes there have been to measures or commitments under the code. Some signatories also do not provide trended data in their annual reports. This requires users to manually examine multiple years of reports to identify changes to measures and any trends, thereby rendering these reports increasingly inaccessible for most users.

Smaller platforms

The current two-tier reporting system was designed to encourage smaller platforms to sign up to the code, but it is not clear how these amendments are operating in practice. This was an issue we identified in our fourth report to government. There is limited transparency about the size of signatories' user bases. As a result, the process for distinguishing between smaller and larger platforms does not appear to be practical and transparent.

Incorporation of reporting framework into the code

We consider that a revised reporting framework should be included in the code itself, rather than left to associated guidelines. Experience to date has suggested that the quality of reporting has not sufficiently improved with the bulk of reporting requirements sitting in guidelines. Experience demonstrates that not all signatories comply with the optional guidelines or adopt the report template provided in Appendix 2 to the code.

ACMA's proposed framework

To address some of the above concerns, the ACMA undertook work in 2023-24 to develop a draft reporting and measurement framework that would better allow more consistent reporting about signatories' efforts.¹⁰ Our aim was to elicit more consistent and transparent information from signatories about both the measures they are taking to fulfill their commitments under the code and the impact of those measures, while also streamlining some elements of the annual reporting process. Through this, it was intended that the framework would allow for greater 'like for like' comparison of signatories' efforts under the code where practicable and for the broader effectiveness an outcomes-based, self-regulatory approach to combatting mis- and disinformation in Australia to be tracked.

The framework we developed comprises measures, metrics, and KPIs that signatories could report against. These three streams of information types allow for collection of:

- Signatory measures: potentially through answers to qualitative questions about processes and systems. This element of the framework will focus on allowing comparison of the various policy-based levers that signatories are using to combat mis- and disinformation on their platforms but will also provide more transparency about material changes to those policies.
- Metrics: to assess the effectiveness of measures and interventions across the code that signatories have in place to meet their commitments under the code.
- Key performance indicators: developed by each signatory, which will contribute to a better understanding of the impact of signatories' actions under the code.

This is summarised in the diagram below.

¹⁰ The process we undertook is set out in Appendix B.

Figure 4: Measurement framework structure



Part 1: Signatory measures

We consider the reporting framework should contain a standardised way to capture signatories' measures, including processes and systems implemented, under the code. We have suggested an approach where major large signatories could respond to a list of baseline questions against code outcomes. Signatories would consolidate this information in an appendix to their report to enable users to understand easily what measures they have in place. Only information against the outcomes and measures applicable to their service should be included.

This would enable comparison of signatories' measures, provide transparency as to material changes, and assist in supporting the code's complaints facility. We would expect that signatories present this information in an easy-to-understand, consistent way, to support easy comprehension and comparison.

Once established in the first year, we expect that the reporting burden on signatories would reduce year-on-year. We are observing fewer material changes as the code matures. This new framework would allow new developments to be clearly highlighted in the front of the transparency report.

Part 1A: Measures – smaller signatories not directly at risk

This would be applicable only to signatories that offer services that are not directly responsible or at-risk of disseminating of misinformation and disinformation. Such services may instead contribute solutions, work collaboratively with at-risk platforms and contribute to society's efforts to address the issue of misinformation and disinformation.

Like Part 1, this could comprise a list of qualitative questions to understand the measures these signatories have in place, to enable comparison and provide transparency.

These signatories would also report against these measures in an appendix to their transparency report.

Part 2: Metrics

The code should contain a set of cross-industry metrics to measure the effectiveness of efforts to address misinformation and disinformation, comparable in intention to the European Union's structural indicators, which also seek to establish cross-industry metrics. Trended Australian-specific data is essential to allow understanding and comparison of the effectiveness of measures implemented by signatories, and to understand progress made.

Signatories would report data and/or qualitative information against relevant metrics for their services covered by the code, noting that all metrics may not be applicable to all services or signatories.

A set of uniform metrics would enable tracking the effectiveness of signatories' measures and the code in addressing disinformation and misinformation over time. Information provided against these metrics would also facilitate comparison across similar services.

Our suggested set of pilot metrics is set out in Appendix A. These twelve metrics were determined based on consultation feedback, their viability based on independent advice, and because they best reflect the signatories' efforts to meet their objectives under Outcome 1a and Outcome 3 of the code. We consider this is sensible as a starting position to elicit key information, with a view to developing additional metrics over time as required.

We note the challenges in developing code metrics as identified by DIGI in its discussion paper, having closely undertaken detailed work in this area. However, we do not consider these issues to be insurmountable and look forward to working with DIGI and relevant signatories to finalise a set of metrics for inclusion in the code.

Part 3: KPIs

Signatories should develop KPIs for their services and these KPIs should be explicitly listed in their reports. The development of explicit KPIs could be informed by the data signatories have published in their historical reports. Their subsequent reporting will demonstrate their performance against each outcome and should include trended Australian-specific data demonstrating how they have tracked against their KPIs over time.

This is essential for signatories to verify and track progress toward the code outcomes and for industry to demonstrate the overall effectiveness of the code. KPIs will also encourage signatories to set thresholds for success based on the nature of their offering and allow users to hold signatories accountable for their commitments.

Implementation

We look forward to working with DIGI to progress changes to the code to enhance its reporting framework.

We expect the following critical information will continue to be included in the annual transparency reports:

- Qualitative information about key changes and initiatives in signatories' policies to address disinformation and misinformation.
- Qualitative commentary to contextualise provided data about efforts to address disinformation and misinformation.
- Qualitative and quantitative information (including Australia specific data points) to outline, where relevant, how signatories are addressing Outcomes 1a, 1b, 1c, 1d, 1e, 3, 2, 4, 5, 6 and 7.

- Case studies to highlight interventions for topics of particular social significance or in response to evolutions in the misinformation and disinformation environment, such as generative AI.

Futureproofing the code

To remain effective, consideration needs to be given to how the code can proactively consider, adapt and respond to disruptive changes in technology, especially when these changes occur outside of the code's formal review process.

Artificial intelligence technologies continue to evolve rapidly and present significant challenges and opportunities in the mis- and dis-information space. Generative AI can be misused to create and distribute disinformation and misinformation at low cost and at greater scales than previously available, thereby exacerbating information crises.¹¹

Signatories report in around May of each year of the events of the previous calendar year. This demonstrates the opportunities for signatories to provide additional information about rapidly emerging issues outside of the code's formal review and reporting cycles to promote transparency.

We encourage DIGI to consider how the code could be amended to account for future developments. For example:

- amendments to the code to encourage transparency about the impact of AI policies on user behaviour and to include more data about the use of AI tools.
- whether the current code definitions are flexible enough to capture AI powered services such as chatbots, and encouraging the providers of such services to sign up to the code.
- amendments to the code to encourage signatories to proactively assess mis- and disinformation risks when introducing major changes to their policies, processes, and systems.
- amendments to the code to encourage signatories to provide information outside the formal reporting cycle, such as about their response to crises, to support better assessment of the work done by signatories.

We recognise that the code was designed to be technology neutral and that signatories may already proactively assess the potential for disinformation and misinformation when introducing major changes or new products as well as publish information outside of code reporting cycles about emerging issues. However, we believe that explicit references to these actions within the code could increase public trust in the code.

¹¹ UK Parliament, [Social media, misinformation and harmful algorithms](#), UK Parliament Committees website, 2024, accessed 11 July 2025.

Researcher access to data

Since the code was established in 2021, there have been shifts in the level of access to data provided to independent researchers by digital platforms. Researchers in Australia have noted increasing costs and constraints to accessing data initiatives provided by digital platforms – for example, X introduced a paid tiered subscription to its API in 2023, while reducing the free quota offered to approved researchers. Similarly, Meta retired its CrowdTangle tool in 2024, which had allowed the monitoring trends on Facebook and Instagram, and has since transitioned to Meta Content Library and API for approved researchers. We understand that these changes were in part due to increased scraping of digital platform data to train AI models.

The ACMA encourages DIGI and signatories to adopt stronger transparency obligations in the code on researcher access to data in Australia. We acknowledge in our fourth report that many signatories currently offer some form of API access or grant programs for researchers looking to study the platform. However, it is unclear what level of access is offered to Australian researchers studying disinformation and misinformation. By codifying transparency around this process, researchers will benefit from understanding what level of access to data is available to them and how they may apply for it. This can then support how Australians receive information about the effectiveness of signatories' systems, processes and measures for combatting disinformation and misinformation.

Reporting under Outcome 6 of the code (for signatories that provide data access) may include reporting of data and information on the number of Australian researchers accessing APIs, the number of applications received or denied, as well as contextual information to support public understanding of the factors that influence signatories' decisions to grant or deny API access for researchers in Australia.

PART 2: OPERATION OF THE CODE

The ACMA welcomes the inclusion of governance and operational considerations into scope of the 2025 code review. We agree that effective code governance and administration are critical to the code's success. This includes clarity around subcommittee operations and robust complaints handling. It is particularly important that the 2025 review assesses the effectiveness of these frameworks as they were not considered in the 2022 review due to their infancy.

Operation of governance arrangements and reporting

The ACMA's second report to government acknowledged DIGI's implementation of governance arrangements – including their annual report – as a positive development to increasing transparency. Our most recent report to government commented on improvements that DIGI has implemented in their annual report. This includes additional detail in Appendix A which made it easier for Australian users and interested stakeholders to see signatories' platform-specific data points, policy changes, and code commitments in one place, and Appendix B which further outlined governance arrangements under the code. DIGI's annual report also included information on the specific functions of the administration sub-committee, the role of the signatory steering group, and the annual event.

The ACMA supports further consideration of the administration subcommittee's role, remit, and membership in the upcoming review. This would assist in safeguarding the impartiality of decision-making and maintaining trust in the work of the subcommittees.

The ACMA supports DIGI's proposal for the subcommittee to formally report on its activities. This report may help to consolidate the subcommittee's work to make it more accessible and transparent to Australians. The report could include further information on decision making processes, the review of DIGI's annual report, and observations on the broader reporting and information integrity environment.

The ACMA considers that transparency could be strengthened by publishing the independent reviewers' findings – currently contained in DIGI's annual report – as a standalone report. A separate report may help distinguish the independent reviewer's oversight from DIGI's work as the code administrator. The report may be similar to that [published by the independent reviewer](#) under the [Aotearoa New Zealand Code of Practice for Online Safety and Harms](#). In the long term, this report may also facilitate the transition of some of the ACMA's feedback on signatory reporting to the independent reviewer.

Code complaints

The ACMA supports consideration of how the complaints facility under the code can be improved. An effective complaints process is essential to ensuring Australian end-users feel empowered to raise issues with platforms where necessary and supported when signatories fail to uphold their commitments.

To date, DIGI has reported receiving 96 complaints via its portal, with only 2 meeting the criteria for consideration by the Complaints Committee. We acknowledge that consumers may be complaining directly to platforms, however this low number appears inconsistent with broader community concern about misinformation outlined earlier in this submission and suggests that the current complaints mechanism may not be sufficiently accessible or understood.

As outlined in previous ACMA reports, strengthening the complaints facility should include establishing a clearer referral pathway between signatories and DIGI's complaints process, particularly where escalation is appropriate. Currently, there is a lack of information about the operation of the complaints process and how to effectively lodge a complaint. Further clarity is also required around signatories' commitments. As the code matures, the ACMA considers that the existing reporting framework does not best support transparency around existing commitments, which may discourage users from making complaints.

Broader information ecosystem

The ACMA acknowledges the ecosystem approach highlighted by DIGI in the discussion paper – that the code alone cannot address disinformation and misinformation. The need for collaboration and cooperation among all relevant stakeholders is recognised in the current code under Clause 1.9¹². The ACMA has been working closely with other sectors that we regulate to encourage them to improve safeguards in this area under their respective codes of practice – this includes the Australian Subscription Television and Radio Association, Free TV Australia, and Commercial Radio and Audio. The Community Broadcasting Association of Australia's (CBAA) new Community Radio Broadcasting Codes of Practice came into effect on 1 July 2025. The new CBAA code requires community radio broadcasters to 'exercise special care when reporting on contentious or controversial matters where facts may be contested and not settled and avoid the amplification of misinformation and disinformation'¹³.

The European Union's (EU) Code of Conduct on Disinformation (under the Digital Services Act) takes a wider approach by incorporating more than 40 signatories which include civil society, research organisations, fact-checking organisations and organisations offering tools against disinformation and misinformation. The EU model acknowledges that disinformation and misinformation risks are not limited to digital platforms but instead, have the potential to spread and affect the wider online information ecosystem¹⁴.

By broadening the approach to consider how each stakeholder shapes the ecosystem, Australian end-users, signatories and the wider industry stand to benefit from a more transparent, collaborative and resilient online information ecosystem. We encourage DIGI to consider how to cultivate support from other related industries through their representative bodies e.g. FreeTV, Australian Press Council etc.

Content authenticity, media literacy and community notes

The ability for disinformation and misinformation to be created and shared – at scale – is a challenge for information integrity globally and in Australia. This problem is likely to grow as generative AI continues to support the creation of potential low-quality information in the coming years. This makes investments in content authenticity measures and effective media literacy efforts by signatories increasingly important. We acknowledge in our fourth report that signatories continue to report on work they have undertaken to support media literacy under Outcome 4 of the code, including programs and partnerships undertaken with third-party organisations to bolster end-users' news literacy and digital literacy focused on using AI tools or features. We also recognise the cross-industry efforts to collaborate on developing global technical standards through the Coalition for Content Provenance and Authenticity and understand the potential role that the implementation of these standards will play in supporting media literacy efforts and the broader fight against misinformation and disinformation.

¹² Clause 1.9, [Australian Code of Practice on Disinformation and Misinformation](#), 22 December 2022, DIGI.

¹³ Section 5.1 (f), Community Broadcasting Association of Australia, [Community Radio Broadcasting Codes of Practice 2025](#), ed 15 October 2025.

¹⁴ Code of Conduct on Disinformation, [Transparency Center](#), 2025, accessed 15 October.

In December 2024, the Australian Government announced the development of Australia's first National Media Literacy Strategy. The strategy will be co-designed in partnership with the media literacy research sector, education sector and communities, to better equip Australians to critically engage with news and media from 2025–26 onwards. The ACMA encourages signatories to support the development of the strategy and work together to communicate consistent messages about media literacy to the Australian public.

Throughout 2025, some major digital platforms have adopted or transitioned to a community notes model, which is designed for end-users to contribute to fact-checking content that is misleading or missing context. This change has highlighted a greater need for stronger media and digital literacy skills and capability for end-users. While recent studies have shown that community notes may reduce engagement with misleading content¹⁵, notes have to be timely, receive enough contributor activity and pass a bridging test¹⁶ (which requires agreement from contributors who typically disagree with one another). A 2025 report by Maldita, a Spanish fact-checking site, ranked professional fact-checkers among the three most cited sources on X's Community Notes, with users trusting notes citing an accredited organisation more¹⁷ – allowing notes to appear faster on misleading posts.

The ACMA considers that third-party fact-checking plays an important role in digital platforms' ability to assess the accuracy of content and provide warning labels to users about misinformation content.

¹⁵ Slaughter, I., Peytavin, A., Ugander, J. & Saveski, M., 2025. Community notes reduce engagement with and diffusion of false information online. *Proceedings of the National Academy of Sciences*, 121(43), e2503413122. Available at: <https://doi.org/10.1073/pnas.2503413122>.

¹⁶ Bassett, K., 2025. *X's Community Notes and the South Asian Misinformation Crisis*. Washington, D.C.: Center for the Study of Organized Hate. Available at: <https://www.csohate.org/wp-content/uploads/2025/06/Xs-Community-Notes-and-the-South-Asian-Misinformation-Crisis.pdf>.

¹⁷ Canetta, T., 2025. *The Role of Fact-Checkers in X's Community Notes: Faster, Trusted, and More Effective*. European Digital Media Observatory (EDMO). Available at: <https://edmo.eu/publications/the-role-of-fact-checkers-in-xs-community-notes-faster-trusted-and-more-effective/>.

Appendix A: Pilot measurement framework

Definitions

These definitions are only intended to be used for the pilot metrics and list of measures. Where applicable, terms used reflect definitions drawn from the code.

Account

Account includes:

- > a free account
- > a pre-paid account
- > anything that may reasonably be regarded as the equivalent of an account.

Action

Steps taken by the platform to prohibit and/or management of user behaviours that may result in the publication or propagation of content that violates a services' terms of service. 'Action' that a Signatory may take may include, amongst other things, labelling the content, providing trust indicators of content to end-users, demoting the ranking of content or removing that content from the service.

Appeal

Appeal means where a user seeks a review of a decision made by a platform with the aim of getting the decision reconsidered and/or reversed.

Artificial engagement

The use of automated systems or inauthentic behaviours to artificially inflate engagement metrics (views, likes, comments).

Australian active end-users/accounts

A unique end user with an Australian IP address who engages with a digital platform's product or service, on a month as averaged over a given time period, through being logged-in, opening a page, scrolling, clicking, liking, making a query, posting, commenting, or otherwise interacting with a feature of the digital platform's product or service. An 'end-user' is intended to include a 'user' within the scope of the code.

Available to active Australian end-users

Content will be 'available' to an active Australian end-user when the content is accessible to an Australian end-user, generates 'impressions' from an active Australian end user or have user 'engagement' from an active Australian end user.

Community guidelines

The rules that cover the content that is posted on the platform. These rules cover the types of content that is and isn't allowed on the platform and the types of user behaviour that is acceptable and unacceptable when they post content. These are a subset of the 'terms of service'.

Note: A complaint refers to a complaint to a digital platform and not a complaint to a regulator.

Content

Content means content:

- > whether in the form of text
- > whether in the form of data
- > whether in the form of speech, music, or other sounds
- > whether in the form of visual images (animated or otherwise)
- > whether in any other form
- > whether in any combination of forms

posted during the relevant reporting period.

Coordinated Inauthentic Behaviour or CIB

Coordinated inauthentic behaviour (CIB) is a manipulative communication tactic that uses a mix of authentic, fake, and duplicated social media accounts. This may include operating as an adversarial network across multiple social media platforms.

Digital platform

A digital platform provides digital products and services to Australian end-users.

Enforcement action

An enforcement action refers to an action taken against end-users by a digital platform in response to a breach of their policy.

Engagement

See the definition of 'user engagement'.

Impressions

As defined per Qualitative Baseline Indicator¹⁸ 6 by the relevant Signatory for the relevant service.

Note: in general terms, 'impressions' refer to the number of times content was seen.

Inauthentic Behaviour

Inauthentic behaviour includes spam and other forms of deceptive, manipulative or bulk, aggressive behaviours (which may be perpetrated via automated systems) and includes behaviours which are intended to artificially influence users' online conversations and/or encourage users of digital platforms to propagate digital content.

Monthly active user

The total number of active users who engage with a digital platform on a month as averaged over a given time period.

On-platform activity

On-platform activity refers to the ways in which users can access, engage with, filter, organise and deliver content while on a digital platform and without leaving the platform.

Policies

Policies means a service's terms of service, community guidelines, standards of conduct or other documentation applicable to Australian end-users that allows a Signatory to regulate its service including through content moderation.

¹⁸ Qualitative Baseline Indicator's refer to the numbers used in Part 1 and Part 1a below.

Reach

As defined per Qualitative Baseline Indicator 5 by the relevant Signatory for the relevant service.

Note: in general, 'reach' refers to the number of unique people who see a piece of content.

Recommender system

Recommender systems means a fully or partially automated system used by an online platform to suggest or prioritise in its online interface specific items of digital content to recipients of the service, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of the items of digital content displayed.

Reporting period

6 months commencing either on 1 July or 1 January of the relevant year.

Service

A service means a specific product made available by signatories to Australian users.

Signatory

A signatory is a digital platform that has voluntarily signed up to the Australian Code of Practice on Disinformation and Misinformation.

Note: Should the framework be used to assess evaluate the efforts of non-signatories, references to signatories in the framework will be redefined to include those platforms.

Terms and conditions

See 'terms of service'.

Terms of service

Terms of service means all documents (whatever they are called) comprising the contract for use of the service, also may be called user agreement. May also be called 'terms of use' or 'terms and conditions'.

Terms of use

See 'terms of service'.

Trust indicator

A trust indicator provides additional information to end-users about the source and reliability of content they see on digital platforms.

Examples include: labels, warnings, interstitial notices, turning off options for engagement and/or resharing.

User engagement

As defined per Qualitative Baseline Indicator 7 by the relevant Signatory for the relevant service.

Note: in general terms, 'engagement' refers to active interactions with content on a platform's service such as likes, comments, or shares. Platforms determine 'engagement' differently according to the nature of the service.

Part 1: Measures – Policies, processes and systems implemented under the code

Signatories are only expected to include information against the outcomes and measures below that are applicable to their service.

No.	Information sought for relevant reporting period
1.	<p>Does the service have policies (such as terms of service, community guidelines, standards of conduct or other policies) that prohibit disinformation content?</p> <p>If yes, include relevant information including links to relevant documentation, where available.</p> <p>If no, are there any other policies that may apply to prohibit disinformation in in some circumstances? If yes, include relevant information including links to relevant documentation, where available.</p> <p>If no, are any relevant policies currently under development or consideration? If yes, provide details.</p>
2.	<p>Does the service have policies that manage (but do not prohibit) disinformation content? If yes, include relevant information including links to relevant documentation, where available.</p>
3.	<p>Does the service have policies that prohibit misinformation content? If yes, include relevant information including links to relevant documentation, where available.</p>
4.	<p>Does the service have policies that manage (but do not prohibit) misinformation content? If yes, include relevant information including links to relevant documentation, where available.</p>
5.	<p>How is the 'reach' of content and accounts defined/measured by the Signatory on the service for content/conduct that the Signatory deems to be misinformation or disinformation?</p>
6.	<p>How are the 'impressions' on content or accounts defined/measured by the Signatory on the service for content/conduct that the Signatory deems to be misinformation or disinformation?</p>
7.	<p>How is user 'engagement' defined/measured by the Signatory for content/accounts that the Signatory deems to be misinformation or disinformation?</p>

Objective 1: Provide safeguards against harms that may arise from disinformation and misinformation

Code Outcome 1a: Signatories contribute to reducing the risk of harms that may arise from the propagation of disinformation and misinformation on digital platforms by adopting a range of scalable measures (MANDATORY)

No.	Information sought for relevant reporting period
8.	Does the Signatory employ human review of user behaviours or content that is available to Australian end-users on the service (including review processes that are conducted in partnership with fact-checking organisations)? If yes, include relevant information including links to relevant documentation, where available.
9.	Does the Signatory have dedicated resources (e.g., Trust and Safety teams) based in Australia to review content available to active Australian end-users on the service? If yes, include relevant information including links to relevant documentation, where available.
10.	Does the Signatory label disinformation and misinformation content on the service or provide trust indicators of content to active Australian end-users of the service? If yes, include relevant information including links to relevant documentation, where available.
11.	Does the Signatory demote, lower or use other interventions (however described) to affect the ranking or recommendation of content that may expose active Australian end-users to disinformation and misinformation on the service? If yes, include relevant information including links to relevant documentation, where available.
12.	Does the service have policies that allow for removal of disinformation and misinformation content that violates the service's terms of service (including community guidelines that prohibits or manages disinformation and misinformation other than content that is propagated by inauthentic behaviours)? If yes, include relevant information including links to relevant documentation, where available.
13.	Does the service have policies that allow for removal or permanent suspension of end-users/accounts that violate the service's terms of service (including community guidelines that prohibit or manage disinformation and misinformation)? If yes, include relevant information including links to relevant documentation, where available.
14.	Does the service have policies that allow for action other than permanent suspension to be taken against end-users/accounts that violate the service's policies that prohibit or manage disinformation and misinformation? If yes, include relevant information including links to relevant documentation, where available.

Examples of action include, but are not limited to:

- Temporary suspension
- Warnings
- Removal of trusted/verified status

- Shadowbanning
- Limitations on account privileges/functionalities

Code Outcome 1B: Users will be informed about the types of behaviours and types of content that will be prohibited and/or managed by Signatories under this Code.

No.	Information sought for relevant reporting period
15.	Has the Signatory informed all active Australian end-users of the service, either on an individual or collective basis, about the types of behaviours and types of content that will be prohibited and/or managed by the Signatory under the Code? If yes, include relevant information including links to relevant documentation, where available.
16.	Was that information offered in any language other than English? If yes, please list the languages offered.
17.	Are active Australian end-users of the service informed when action is taken against their account, or content they publish on the service, for violating the service's policies that prohibit or manage disinformation and misinformation? If yes, include relevant information including links to relevant documentation, where available.
18.	Can active Australian end-users of the service appeal action taken by the Signatory related to the violation of the service's policies that prohibit or manage disinformation and misinformation including whether appeals mechanisms are provided in-service or by other means? If yes, include relevant information including links to relevant documentation, where available.

Code Outcome 1C: Users can report content or behaviours to Signatories that violate their policies.

No.	Information sought for relevant reporting period
19.	Can all Australian users of the service report content/or on-platform activity for violating the service's policies? If yes, include relevant information including links to relevant documentation, where available.
20.	Can all Australian users of the service report content/ or behaviours for violating the service's policies that prohibit or manage disinformation and misinformation? If yes, include relevant information including links to relevant documentation, where available.
21.	Do reporting options available to active-Australian end-users cover all content available of the service?

Code Outcome 1D: Users will be able to access general information about Signatories' actions in response to reports.

No.	Information sought for relevant reporting period
22.	Has the Signatory given active Australian end-users access to general information about the Signatory's actions in response to reports about the service? If yes, include relevant information including links to relevant documentation, where available.

Code Outcome 1E: Users will be able to access general information about Signatories' use of recommender systems and have options relating to content suggested by recommender systems.

No.	Information sought for relevant reporting period
23.	Has the Signatory given active Australian end-users access to general information about the Signatory's use of recommender systems? If yes, include relevant information including links to relevant documentation, where available.
24.	Does the Signatory provide active Australian end-users with in-service options to control and otherwise determine the appearance of content suggested by recommender systems? If yes, include relevant information including links to relevant documentation, where available.
25.	Does the Signatory provide active Australian end-users with in-service options to control content suggested by recommender systems used by the service? If yes, include relevant information including links to relevant documentation, where available.
26.	Does the Signatory provide active Australian end-users with options (other than in-service options) to control content suggested by recommender systems used by the service? If yes, include relevant information including links to relevant documentation, where available.
27.	Can the options the Signatory offers active Australian end-users in relation to content suggested by recommender systems be used for individual pieces of content? If yes, include relevant information including links to relevant documentation, where available.
28.	Can the options the Signatory offers active Australian end-users in relation to content suggested by recommender systems be used by end-users to restrict content suggestions related to specific other end-users/accounts? If yes, include relevant information including links to relevant documentation, where available.
29.	Can the options the Signatory offers active Australian end-users in relation to content suggested by recommender systems be used by end-users to block or mute content posted by other accounts on the service? If yes, include relevant information including links to relevant documentation, where available.

No.	Information sought for relevant reporting period
30.	Can the options the Signatory offers active Australian end-users in relation to content suggested by recommender systems be used to make changes based on topics, themes or narratives suggested by recommender systems used by the service? If yes, include relevant information including links to relevant documentation, where available.

Objective 3: Work to ensure the integrity and security of services and products delivered by digital platforms

Code Outcome 3: The risk that Inauthentic User Behaviours undermine the integrity and security of services and products is reduced.

No.	Information sought for relevant reporting period
31.	Does the Signatory have measures in place on the service which prohibit or manage the types of user behaviours that are designed to undermine the integrity and security of the service (inauthentic user behaviour), for example, the use of inauthentic accounts or automated bots that are designed to propagate disinformation? If yes, include relevant information including links to relevant documentation, where available and any additional detail, particularly how often systems scan for inauthentic behaviour.
32.	<p>List the types of inauthentic user behaviours the Signatory acts against in Australia such as:</p> <ul style="list-style-type: none"> • creating and propagating disinformation • creation and use of inauthentic accounts, account takeovers and bot-driven amplification, • Hack-and-leak operations • Impersonation • Malicious deep fakes • The purchase of inauthentic engagements • The creation and use of accounts that participate in coordinated inauthentic behaviour • User conduct aimed at artificially amplifying the reach or perceived public support for disinformation <p>Provide relevant information including links to relevant document, where available, including the types of inauthentic user behaviours not listed above.</p>
33.	What actions does the Signatory take against content or end-users/accounts that violates their policies such as removal of content, temporary or permanent suspensions of end-users/accounts? Include relevant information including links to relevant documentation, where available.

Part 1a: Measures - Unique signatories

This part only applies to unique signatories that provide support and offer solutions to the issue of misinformation and disinformation.

Additional guidance: Unique signatories refers to signatories who offer services that are not directly responsible or at-risk of disseminating of misinformation and disinformation. The purpose of this Part is to recognise the wide range of efforts signatories undertake to contribute to society's efforts to address the issue of misinformation and disinformation. This Part recognises the importance of services that may contribute solutions or work collaboratively with at-risk platforms and contribute to society's efforts to address the issue of misinformation and disinformation.

No.	Information sought for relevant reporting period
1.	As a signatory to the code, how do you contribute to reducing the impact of misinformation and disinformation? Provide links to relevant information, including links to relevant documentation, where available.
2.	Does the signatory utilise information-sharing mechanisms, or other methods of collaboration with industry and civil society, to address the impacts of misinformation and disinformation? If so, provide relevant information, including links to relevant documentation, where available.
3.	Does the signatory quantify the impact of your efforts to address the impact of misinformation and disinformation? If so, provide relevant information.

Part 2: List of pilot metrics

No.	Information sought for relevant reporting period
1.	Total number of active Australian end-users each month during the relevant reporting period
2.	Total number of pieces of content from active Australian end-users which were determined to be: prohibited, and subject to moderation/other action as violating the service's policies relating to disinformation and misinformation
3.	Total number of accounts which were identified as violating the service's policies that prohibit or manage disinformation and misinformation
4.	Total number of active Australian end-users of the service reached by content which violated the service's policies that prohibit or manage disinformation and misinformation
5.	Total number of pieces of content available to active Australian end-users that violated the service's policies that prohibit or manage disinformation and misinformation that had action taken against it, broken down by nature of the action that the Signatory took (e.g. removal pre- and post-publication, downranking, trust indicator)
6.	Total active Australian end-user engagement with content that violated the service's policies that prohibit or manage disinformation and misinformation
7.	Total number of Australian end-user reports about content allegedly violating the service's misinformation and disinformation policies
8.	Total number of Australian end-user reports about accounts allegedly violating the service's misinformation and disinformation policies
9.	Total active Australian end-user reach of content published by inauthentic users/accounts
10.	Total active Australian end-user reach of content published by inauthentic user/accounts before removal
11.	Number of foreign CIB operations identified by the signatory targeting Australia or Australians, including: <ul style="list-style-type: none"> Country of origin of foreign CIB network Timeframe CIB was operating
12.	If any CIB operation(s), what was the: <ul style="list-style-type: none"> total Australian active end-user reach of the operation (s)? total Australian active end-user engagement with the operation (s)? total Australian active end-user impressions with the operation (s)?

Part 3: Key performance indicators (KPIs)

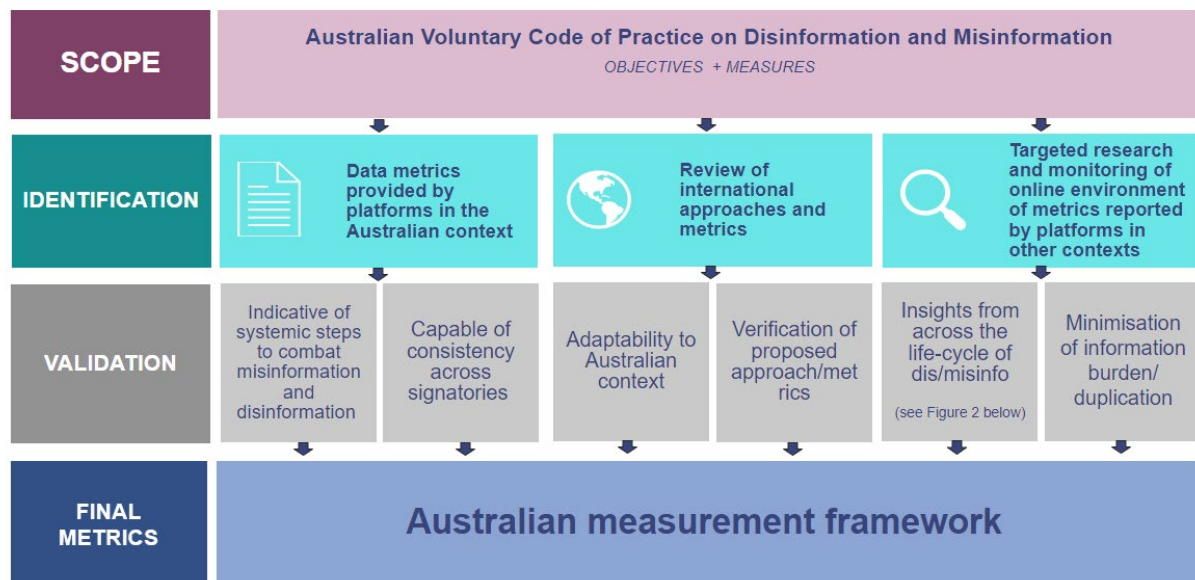
The examples below are illustrative.

Code outcome	Key performance indicator (KPI)	Has KPI been achieved?	Has this data been provided previously?
Outcome 1a	<i>Take action (e.g. downranking, labelling) on violating misinformation content within 48 hours of detection</i>	<i>If the answer is no, provide information about why the KPI hasn't been achieved.</i>	<i>If the answer is yes, please list the time periods it was provided previously.</i>
Outcome 1c	<i>Respond to user complaints against content allegedly violating misinformation and disinformation policies within 24 hours of report</i>		
Outcome 3	<i>Remove 95% of fake accounts at registration</i>		

Appendix B: Process to develop framework

To develop our draft framework, we undertook a three-stage process as summarised in the diagram below.

Figure 5 1: ACMA approach to developing pilot framework



Following this process, the ACMA undertook a consultation process with the following stakeholders:

- Members of the Digital Platforms Regulators Forum (DP-REG)
- Australian government agencies with an interest in misinformation and disinformation including our portfolio Department, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- International government agencies
- Signatories to the voluntary code
- Digital Industry Group Inc. (DIGI)
- Hal Crawford, the then independent reviewer of the annual transparency reports.

We also worked with an external consultant, Moonshot, to independently review and validate the metrics outlined in the draft measurement framework¹⁹.

¹⁹ [Third report on digital platforms' efforts under voluntary arrangements to address disinformation and misinformation | ACMA](#), accessed 22 October 2025.