



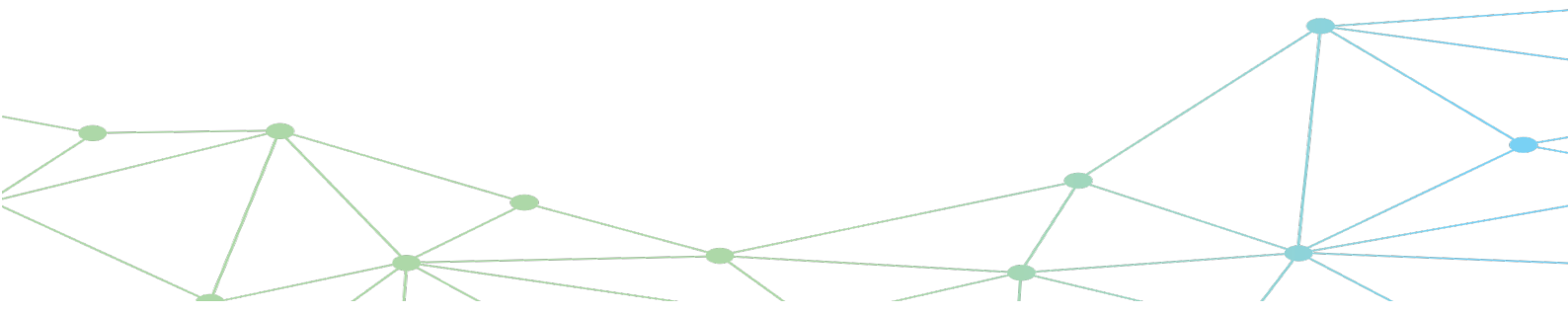
Australian Government

**Department of Infrastructure, Transport,
Regional Development, Communications and the Arts**

Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2023

Guidance Note

June 2023



Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Disclaimer

The material contained in this publication is made available on the understanding that the Commonwealth is not providing professional advice, and that users exercise their own skill and care with respect to its use, and seek independent advice if necessary.

The Commonwealth makes no representations or warranties as to the contents or accuracy of the information contained in this publication. To the extent permitted by law, the Commonwealth disclaims liability to any person or organisation in respect of anything done, or omitted to be done, in reliance upon information contained in this publication.

Use of the Coat of Arms

The Department of the Prime Minister and Cabinet sets the terms under which the Coat of Arms is used. Please refer to the Commonwealth Coat of Arms - Information and Guidelines publication available at <http://www.pmc.gov.au>.

Creative Commons licence

With the exception of (a) the Coat of Arms; and (b) the Department of Infrastructure, Transport, Regional Development, Communications and the Arts photos and graphics, copyright in this publication is licensed under a Creative Commons Attribution 4.0 Australia Licence.

Creative Commons Attribution 4.0 Australia Licence is a standard form licence agreement that allows you to copy, communicate and adapt this publication provided that you attribute the work to the Commonwealth and abide by the other licence terms.

Further information on the licence terms is available from <https://creativecommons.org/licenses/by/4.0/>

This publication should be attributed in the following way: © Commonwealth of Australia 2023

Contact us

This publication is available in PDF and Word format. All other rights are reserved, including in relation to any departmental logos or trademarks which may exist. For enquiries regarding the licence and any use of this publication, please contact:

Director – Internal Comms and Creative Services
Communication Branch
Department of Infrastructure, Transport, Regional Development, Communications and the Arts
GPO Box 594
Canberra ACT 2601
Australia

Email: publishing@infrastructure.gov.au

Website: www.infrastructure.gov.au



Table of contents

1. Overview	5
1.1 Purpose	5
1.2 Context of the reforms	5
1.3 We seek your views on the Exposure Draft Bill	6
1.4 Structure of the Exposure Draft Bill	7
Schedule 2: Consequential amendments and transitional provisions	8
1.5 Consultation process on the Exposure Draft Bill	8
2. Part 1 of Schedule 9 – Introduction	9
2.1 Definitions and key terms	9
2.1.1 Defining the services to be covered under the new ACMA powers	9
2.1.2 Misinformation, disinformation and serious harm	10
2.1.3 Private messages (Clause 2)	12
2.1.4 Excluded content for misinformation purposes (Clause 2)	12
3. Part 2 of Schedule 9 – Information	13
3.1 Division 1 – Scope	13
3.1.1 Electoral and referendum content is in scope of the information powers	14
3.1.2 The contents of private messages are out of scope	14
3.2 Division 2 – Record keeping and reporting	14
3.2.1 The ACMA may make digital platform rules in relation to records (Clause 14)	14
3.3 Division 3 – Information gathering	15
3.3.1 The ACMA may obtain information and documents from digital platform providers and other persons (Clauses 18 and 19)	15
3.3.2 Self-incrimination (Clause 21)	16
3.4 Division 4 – Publishing information	17
4. Part 3 of Schedule 9 – Misinformation codes and standards	17
4.1 Division 1 – Scope	17
4.2 Division 2 – Interpretation	17
4.2.1 Sections of the digital platform industry (Clause 30)	17
4.3 Division 3 – General principles relating to misinformation codes and standards	18
4.3.1 Matters that may be dealt with in a code and standard (Clause 33)	18
4.3.2 Limitations (Clauses 34 and 36)	18
4.3.3 Limitation – electoral and referendum matters with the exception of disinformation from an unauthorised source (Clause 35)	19
4.4 Division 4 – Misinformation codes	19
4.4.1 The ACMA may register codes (Clause 37)	19
4.4.2 The ACMA may request misinformation codes (Clause 38)	19
4.4.3 When no industry body or association exists (Clause 39)	20
4.4.4 Variation of misinformation codes (Clause 40)	20
4.4.5 Replacement of misinformation codes and deregistration (Clauses 41 and 42)	20
4.5 Division 5 – Misinformation standards	21
4.5.1 General requirement – consideration of freedom of political communication (Clause 45)	22
4.5.2 The ACMA may determine standards when a request for a code is not complied with or no industry body or association has been formed (Clauses 46 and 47)	22
4.5.3 The ACMA may determine standards when an existing code fails (Clauses 48 and 49)	22
4.5.4 The ACMA may determine standards due to emerging circumstances (Clause 50)	22
4.5.5 Variation of standards and revocation of standards (Clauses 51 and 52)	22
4.6 Division 6 – Register of misinformation codes and standards	22
5. Additional information – Enforcement	23
5.1 Graduated approach to enforcement	23
5.2 Compliance with the record keeping rules (Clauses 15 and 16)	23
5.3 Compliance with information-gathering powers (Subclauses 18(5) and 19(5))	24
5.4 False or misleading information or evidence under the record keeping rules and information-gathering powers (Clauses 17 and 22)	24

5.5	Compliance with Misinformation codes and standards (Clauses 43, 44, 53 and 54).....	25
5.6	Comparison with fines in the European Union and Australia	25
6. Part 4 of Schedule 9 – Miscellaneous		26
6.1	Service of summons, process or notice on corporations incorporated outside Australia (Clause 58)	26
6.2	Relationship with other laws (Clause 59)	26
6.3	Implied freedom of political communication (Clause 60)	26
6.4	Concurrent operation of State and Territory laws (Clause 62)	26
6.5	Schedule not to affect performance of State or Territory functions (Clause 63).....	26
6.6	Digital platform rules (Clause 64).....	27
7. Consequential amendments and transitional provisions		27
7.1	Australian Communications and Media Authority Act 2005.....	27
7.2	Broadcasting Services Act 1992.....	27
7.2.1	Regulatory Intent.....	27
7.2.2	Decisions appealable to the Administrative Appeals Tribunal	27
7.2.3	Other key changes	27
8. Attachment 1: Graduated application of the ACMA powers		28
9. Attachment 2: What is in scope of the ACMA powers		29

List of figures and tables

Figure 1: Graduated application of the ACMA powers to combat misinformation and disinformation....	6
Figure 2: Defining digital platform services for the new ACMA powers	9
Table 1: Harms	11
Table 2: Enforcement	23
Table 3: Maximum penalties on non-compliance with a registered code or standard.....	25
Table 4: Key examples of what is in scope of the ACMA powers	29

1. Overview

1.1 Purpose

The purpose of this Guidance Note is to outline and briefly explain the key parts of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 (the Bill).

This is also an opportunity for stakeholders, experts and the community to provide feedback on the draft Bill, which the Australian Government will seek to finalise and introduce in the Parliament in the second half of 2023.

1.2 Context of the reforms

In January 2023, the Minister for Communications announced that the Australian Government will introduce new laws to provide the independent regulator, the Australian Communications and Media Authority (ACMA), with powers to combat online misinformation and disinformation.

In 2019, the Australian Competition and Consumer Commission (ACCC) released its Digital Platforms Inquiry Final Report. As part of its response to the report, the former Government requested online platforms in Australia develop a voluntary code of practice to address online misinformation, disinformation, and news quality, and that the ACMA will have oversight of the codes and report to Government on the adequacy of platforms' measures and the broader impacts of disinformation.

The Australian Code of Practice on Disinformation and Misinformation (the voluntary code) was launched on 22 February 2021 by Digital Industry Group Inc (DIGI). The code has eight signatories – Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitter.

In March 2022, the ACMA released its report to government on the adequacy of digital platforms' disinformation and news quality measures, which made five recommendations and 48 findings. These covered the voluntary code, its development process, signatory performance and the Australian misinformation and disinformation environment more generally.

Recommendations 3 and 4 of the report proposed that the ACMA be given the following powers to combat harmful misinformation and disinformation online:

- Information-gathering powers, including the power to obtain Australia-specific data on measures platforms are taking to address misinformation;
- the power to make record keeping rules, requiring platforms to maintain and provide the ACMA with records of locally relevant data on measures to address misinformation and disinformation;
- reserve powers to register and enforce industry codes; and
- reserve powers to make industry standards.

The Bill will amend the *Broadcasting Services Act 1992* (the Act), and other Acts as relevant for consequential amendments, to enact these recommendations.

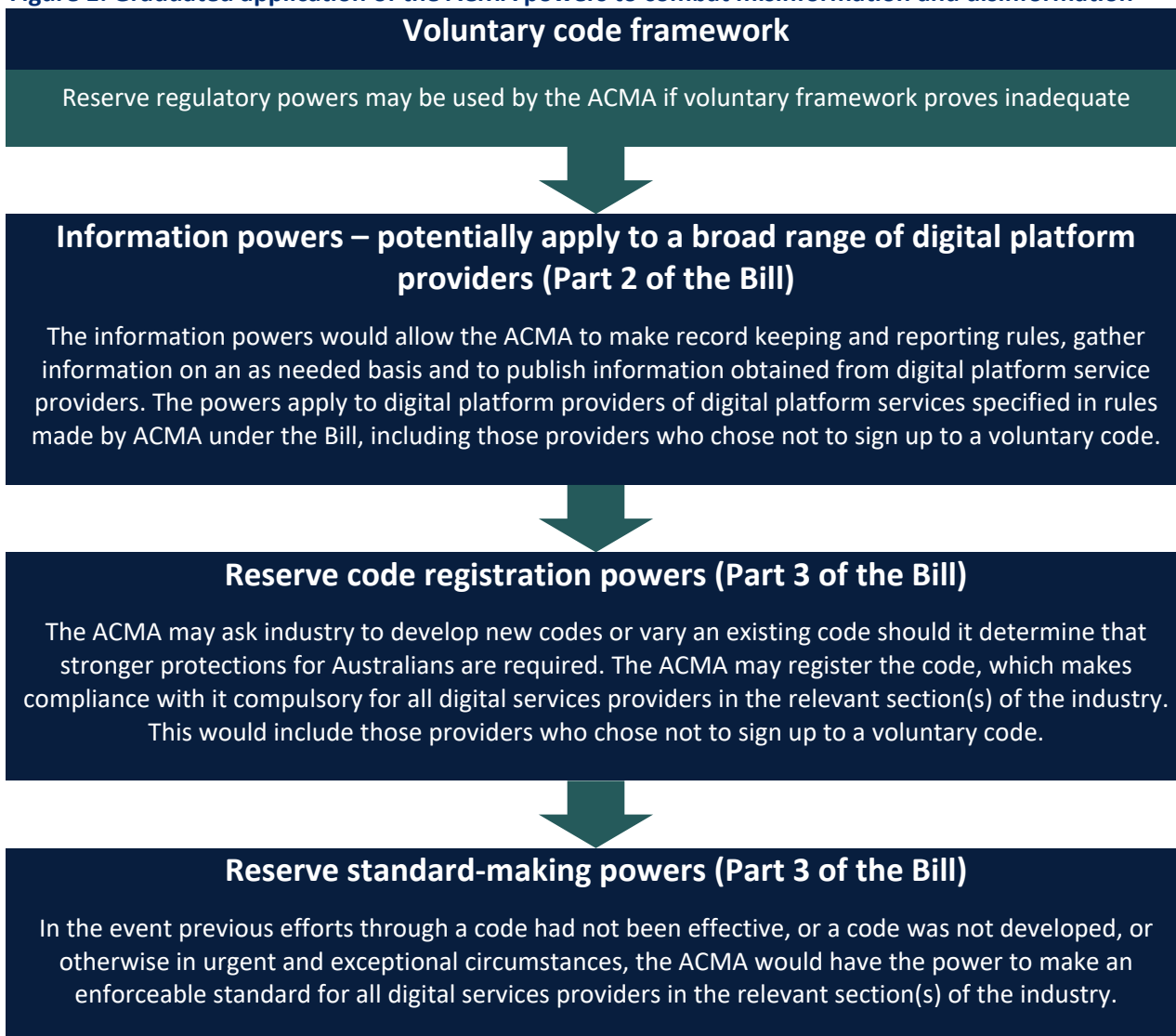
An effective self-regulatory scheme is the preferred approach. However, the Bill provides a graduated set of powers that allows the ACMA to act if voluntary efforts are inadequate.

Where voluntary efforts provide inadequate protection and the ACMA is satisfied that it is necessary to address systemic issues in relation to misinformation or disinformation on digital platform services, the ACMA will be able to request the industry make a new code. That code will become mandatory and enforceable following registration.

In the event of industry failing to develop a code, or if a code is failing to protect Australians, the ACMA could make a standard as a last resort. Standards will have stronger enforcement mechanisms through higher penalties for non-compliance.

This will be supported with new information-gathering and record keeping powers to provide greater transparency on the effectiveness of platform efforts in combatting misinformation and disinformation. Refer to Attachment 1 for a diagram of the graduated powers.

Figure 1: Graduated application of the ACMA powers to combat misinformation and disinformation



1.3 We seek your views on the Exposure Draft Bill

We seek your views on the exposure draft (ED) Bill and whether the proposed legislation strikes an appropriate balance of a range of issues such as freedom of expression, the complexity for platforms to operationalise various content exemptions (e.g. professional news and authorised electoral content), the scope of the private message exemption, the size of the civil penalties and any other relevant issues.

The proposed powers seek to strike a balance between the public interest in combatting the serious harms that can arise from the propagation of misinformation and disinformation, with freedom of speech.

The Bill aims to incentivise digital platform providers to have robust systems and measures in place to address misinformation and disinformation on their services, rather than the ACMA directly regulating

individual pieces of content. The Bill does not seek to curtail freedom of speech, nor is it intended that powers will be used to remove individual pieces of content on a platform. The proposed definition of misinformation and disinformation is intended to provide guidance on the types of harms the powers are designed to address. The concept of ‘serious harm’ is intended to ensure that the ACMA’s use of its powers, and the platforms’ systems and processes, are targeted at harms with significant implications for the community.

Digital platform providers will continue to be responsible for the content they host and promote to users. In balancing freedom of expression with the need to address online harm, the code and standard-making powers will not apply to professional news and authorised electoral content, nor will the ACMA have a role in determining what is considered truthful.

The information powers under the proposed framework will help bring greater transparency to the actions taken by online platforms to counter misinformation and disinformation. It will enable the ACMA to obtain information to more clearly understand and identify the circumstances in which platforms act against misinformation and disinformation, what tools they are using, and how effective and regularly they are used.

We are seeking your views on the Exposure Draft Bill, particularly:

- **the definitions of misinformation and disinformation**
- **the definition of digital platform services and the types of services we propose be subject to the new framework**
- **how instant messaging services will be brought within the scope of the framework while safeguarding privacy**
- **the scope of the information-gathering and recording keeping powers, which includes the prevalence of false, misleading or deceptive information on digital platform services**
- **the preconditions that must be met before the ACMA can require a new code, register a code and make an industry standard**
- **how the digital platforms industry may be able to operationalise the Bill and various content exemptions (e.g. professional news, satire, authorised electoral content)**
- **appropriate civil penalties and enforcement mechanisms for non-compliance.**

1.4 Structure of the Exposure Draft Bill

The key elements of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 include:

Schedule 1: Main Amendments

This part of the Bill introduces the main amendment – new Schedule 9 – Digital platform services, into the *Broadcasting Services Act 1992* (BSA).

Proposed new Schedule 9 will consist of the following parts:

- *Part 1 of Schedule 9 – Introduction:* provides the simplified outline of the purpose of the Bill, includes definitions of key terms in Schedule 9, such as disinformation, misinformation, digital platform services, excluded digital services and excluded content.
- *Part 2 of Schedule 9 – Information:* has four divisions which sets the scope of the information powers and provides the ACMA with powers that allow it to make record keeping and reporting

rules, gather information on an as needed basis and to publish information obtained from platforms.

- *Part 3 of Schedule 9 – Misinformation codes and standards:* has seven divisions which sets the scope of the misinformation codes and standards powers, the sections of the industry to which the powers apply, matters that may be dealt with in a code or standard, limitations of the powers, and details relating to the code and standard-making powers. The ACMA will be required to maintain a register of the codes and standards, and make it available for inspection on the internet.
- *Part 4 of Schedule 9 – Miscellaneous:* consists of miscellaneous provisions, including provisions which explain the interaction of the Schedule with other Commonwealth, State and Territory laws.

Schedule 2: Consequential amendments and transitional provisions

This part of the Bill makes consequential amendments to the *Australian Communications and Media Authority Act 2005* (the ACMA Act), the BSA, the *Online Safety Act 2021* and the *Telecommunications Act 1997*, as well as sets out transitional provisions.

- It confers several new functions on the ACMA including to enable it to assist with industry code development, to develop standards, to monitor compliance with misinformation codes and standards, advise the Minister about online misinformation, and make available to the public information relating to misinformation and disinformation on digital platform services.
- It makes changes to the BSA, including the addition of a new object to the BSA – to encourage digital platform providers to protect the community against harm caused, or contributed to, by misinformation and disinformation on digital platform services. Amendments to the BSA also include outlining the Parliament’s intention that digital platform services be able to be regulated in order to prevent and respond to misinformation and disinformation on the services; provisions that enable certain decisions by the ACMA to be subject to merits review; and details around the new civil penalty provisions, such as the maximum penalty unit amounts.

1.5 Consultation process on the Exposure Draft Bill

The Department invites submissions **by 11:59pm AEST, Sunday, 6 August 2023**. Submissions may be lodged in the following ways:

Website: <https://www.infrastructure.gov.au/have-your-say/acma-powers>

Email: Information.Integrity@infrastructure.gov.au

Post: Information Integrity Section
Department of Infrastructure, Transport, Regional Development, Communications and the Arts
GPO Box 2154
CANBERRA ACT 2601

Submissions should include your name, organisation (if relevant) and contact details. Submissions will be treated as non-confidential information, and will be made publicly available on the Department’s website unless you specifically request that your submission, or a part of a submission, be kept confidential.

2. Part 1 of Schedule 9 – Introduction

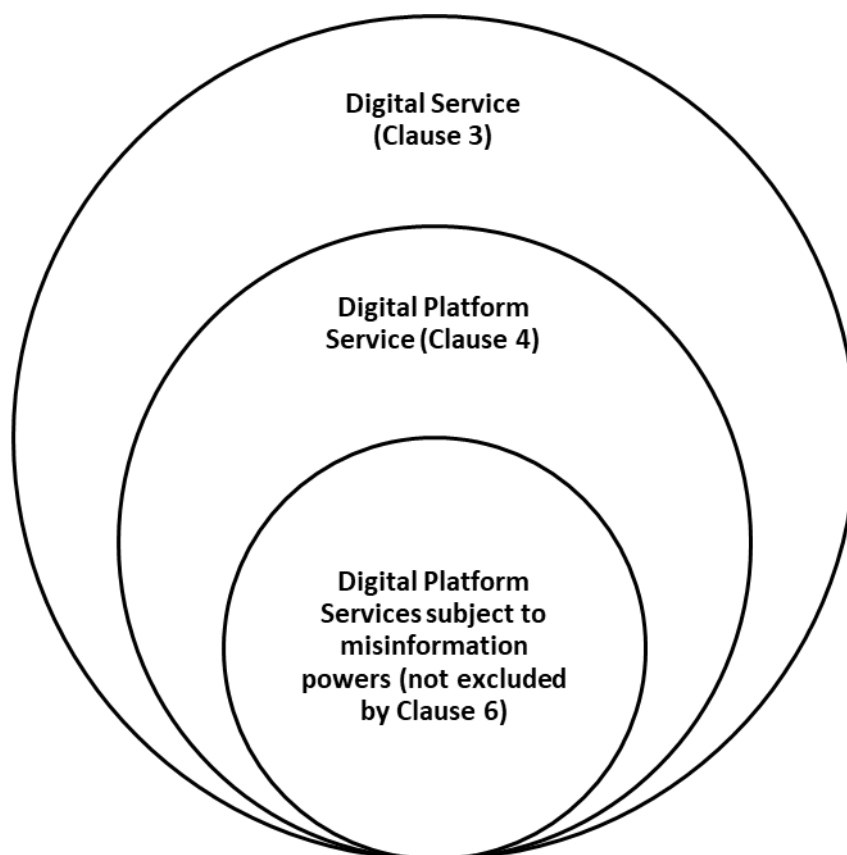
2.1 Definitions and key terms

2.1.1 Defining the services to be covered under the new ACMA powers

The Bill has a three-layered approach to defining the ‘digital platform services’ that are within scope of the powers, which allows for any potential future legislative reform related to digital platforms.

Definitions of services are based upon how information is delivered, presented or interacted with, the type of information on the service, or whether the information is public is not a factor in how a service is defined.

Figure 2: Defining digital platform services for the new ACMA powers



This is the highest level of definition. It is deliberately broad and is intended to capture any service available in Australia that uses the internet to deliver content (content being very broadly described), or any service that enables persons to access content using an internet carriage service. This includes any and all websites, streaming services, social media, email services and other networks available in Australia.

The ACMA powers will not apply to all digital services.

Digital Platform Services (Clause 4)

The second level is digital platform services which has the following three subcategories:

- **Content Aggregation Services:** those whose primary function is to collate and present content from a range of online sources to end-users. This includes search engines and news aggregators.

- **Connective Media Services:** those whose primary function is to allow end-users to interact with each other online. A majority of digital platform services will fall into this category. Several examples are instant messaging services, social media, web-forums, dating sites, and online peer-to-peer marketplaces.
- **Media Sharing Services:** those whose primary function is to provide audio, audio-visual, or moving visual content to end-users. These include podcasting services.

All media sharing services must have an interactive feature as specified in clause 5 of the Bill (see clause 6 further below) to be within scope of the powers. If the service has any of the following apply, then it has an interactive feature:

- allows end-users to post content on the digital service;
- allows end-users to share other users' content with another end-user of the digital service;
- allows end-users to comment on or engage with other users' content (including via 'likes' or other reactions made available by the service).

Each of these three subcategories of digital platform services are defined based on distinct primary functions of the digital platform industry. These functions are further used in determining sections of the digital platform industry, as discussed in Part 3 of this Guidance Note and outlined in clause 30 of the Bill.

The Minister may also by legislative instrument specify the addition of a new subcategory of digital platform service to the list above as different types of services emerge over time and risks of misinformation and disinformation evolve on certain services.

Digital Platform Services excluded by the ACMA powers (Clause 6)

The new powers will cover all digital platform services highlighted above with some exclusions.

The services carved out from the new laws are email services and media sharing services that do not have an interactive feature, such as Broadcast Video On Demand Services (BVODS) and Subscription Video On Demand Services (SVODS). The Minister may also by legislative instrument specify a digital platform service to be exempt from the ACMA powers. These services are **excluded services for misinformation purposes**.

FAQ: What are SMS, MMS and instant messaging services defined as?

SMS and MMS (text messages) for the purposes of this Bill are **not considered a digital service** as they do not use the internet to deliver content. SMS and MMS will not be captured by the powers.

Instant messaging services (WhatsApp, Facebook Messenger, Signal etc.) for the purpose of this Bill are considered to be a **Connective Media Service**. These digital platform services use the internet to deliver content, and the primary function allows end-users to interact with each other.

Some mobile phones will have apps that have the ability to send messages through SMS and IM protocols. For the purpose of this Bill, only messages sent through the internet will be covered. However, the content of the private messages and encryption will not be covered by the powers.

2.1.2 Misinformation, disinformation and serious harm

Misinformation in the Bill is intended to capture content that is disseminated on a digital service, where that content is false, misleading or deceptive, and where the provision of that content on the service is reasonably likely to cause or contribute to serious harm.

The key distinguishing feature between misinformation and disinformation in the Bill is intent.

Disinformation is intended to capture 'misinformation that has been disseminated with the intention of deceiving another person'. The definition of misinformation and disinformation excludes certain types of content (refer to section 2.1.4).

The use of the terms ‘misinformation’ and ‘disinformation’ are used interchangeably in the remainder of this Guidance Note, and are intended to refer to both misinformation and disinformation, unless otherwise specified, or clear from its context that the reference is meant to refer to just one concept or the other.

Serious harm (Subclause 7(3))

For misinformation to be covered by the powers, it must be reasonably likely that it would cause or contribute to serious harm. For harm to be serious, it is intended that it must have severe and wide-reaching impacts on Australians. Subclause 7(3) outlines the matters that are relevant to determining whether the content could cause or contribute to serious harm:

- the circumstances in which the content is disseminated
- the subject matter of the false, misleading or deceptive information in the content
- the potential reach and speed of the dissemination
- the severity of the potential impacts of the dissemination
- the author of the information
- the purpose of the dissemination
- whether the information has been attributed to a source and, if so, the authority of the source and whether the attribution is correct
- other related false, misleading or deceptive information disseminated
- any other relevant matter.

Clause 2 of the Bill contains a definition of ‘harm’ and outlines types of harm that would be considered. The Table below gives some examples of what could be ‘serious harm’.

Table 1: Harms

Type of harm	Example of serious harm
Hatred against a group in Australian society on the basis of ethnicity, nationality, race, gender, sexual orientation, age, religion or physical or mental disability	Misinformation about a group of Australians inciting other persons to commit hate crimes against that group
Disruption of public order or society in Australia	Misinformation that encouraged or caused people to vandalise critical communications infrastructure
Harm to the integrity of Australian democratic processes or of Commonwealth, State, Territory or local government institutions	Misinformation undermining the impartiality of an Australian electoral management body ahead of an election or a referendum
Harm to the health of Australians	Misinformation that caused people to ingest or inject bleach products to treat a viral infection
Harm to the Australian environment	Misinformation about water saving measures during a prolonged drought period in a major town or city
Economic or financial harm to Australians, the Australian economy or a sector of the Australian economy	Disinformation by a foreign actor targeting local producers in favour of imported goods

Automated dissemination and artificial intelligence

Bad actors can take advantage of bots to automate the process of posting and spreading disinformation on digital services. The spreading of misinformation and disinformation by bots and other artificial intelligence services on a digital platform service is within scope of the powers.

It can be difficult to attribute an anonymous piece of content to a person or a bot, and the powers will treat misinformation the same way no matter how it was created. The definition of dissemination in the Bill includes using automated means (clause 2). Therefore, if a person were to program a bot to start spreading false or misleading information, it would be interpreted that the person who generated the bot

was the originator. Content generated using artificial intelligence such as deepfakes would be within scope of the powers.

A registered code or standard, may for example, include requirements for platforms to crack down on endemic bots or AI spreading false information.

2.1.3 Private messages (Clause 2)

The contents and encryption of private messages will not be within scope of the powers. The definition of private message in the Bill is: an instant message sent using a digital platform service from one end-user of the service (the sender) to one or more other end-users of the service (the recipients) where the message is only observable to end-users of the service selected by the sender or any of the recipients. This is intended to capture interpersonal communications sent to a finite number of users. If a person is sending a message in a group conversation, it will be taken that they have selected all members of that group to receive the message. Examples include:

- a direct message (DM) sent from one user to another user on a social media platform
- the contents of a family group conversation on a messaging service
- messages sent between users on a dating app.

Posts in a forum or message board hosted by a digital platform service are not considered instant messages and are therefore not intended to be covered by the private messages exemption, even if access to this content is limited to certain users. Examples of services intended to be outside the scope of the private messages exemption include:

- messages in a publicly open conversation sent using an instant messaging service
- a social media group for a particular interest or hobby
- a local community marketplace on a social media platform
- a forum or message board on a blogging site where its members post content to facilitate group engagement that is visible only to its members, and may involve user registration to join.

2.1.4 Excluded content for misinformation purposes (Clause 2)

The Bill excludes certain content from the definition of misinformation to strike a balance between the public interest in combatting misinformation, with the right to freedom of expression. Digital platform providers will be responsible for determining whether pieces of content are excluded for misinformation purposes.

Satire

Content produced in good faith for the purposes of entertainment, parody or satire will be excluded, even if the content is at surface value, misinformation.

Professional news

Professional news content will not be within the scope of the new powers. This means we do not expect or envisage platforms to determine if professional news content is misinformation or disinformation. The Australian Government does not seek to influence the editorialisation and reporting by the free press. Professional news content, which is defined as ‘news content’ produced by a ‘news source’ who is subject to certain rules and has editorial independence from the subjects of the news source’s news coverage, will be exempt from the powers. Content produced by a person or organisation that purports to be a professional news organisation, but that does not adhere to such recognised editorial standards, will not be exempt.

In order for their content to be excluded for the purposes of misinformation, content produced by Australian professional news organisations must satisfy certain criteria that is the same as the professional standards test in the *Treasury Laws Amendment (News Media and Digital Platforms*

*Mandatory Bargaining Code) Act 2021 (NMBC)*¹. Content produced by international professional news providers will need to be subject to analogous rules or internal editorial standards to be exempt from the scope of the misinformation powers. A key element of the definition is that news providers have editorial independence from the subjects of the news source’s coverage.

Educational content

Educational content produced by or for accredited educational providers will not be within the scope of the new powers.

Australian educational providers will need to be accredited by a Commonwealth, State or Territory Government, or by a body recognised by the Commonwealth, a State or a Territory as an accreditor of educational institutions.

International educational providers will need to be accredited by a foreign government or body recognised by a foreign government as an accreditor of educational institutions. To be exempt, foreign accreditations should have substantially equivalent standards to Australian educational institutions.

Authorised government content in Australia

Content authorised by the government of the Commonwealth, a State, a Territory or a local government area will be exempt from the powers. For example, this could be social media post from a State’s transport department about an upcoming road project or health campaign.

3. Part 2 of Schedule 9 – Information

The Bill provides the ACMA with information powers that will apply to the digital platform industry. The information powers will allow the ACMA to make record keeping and reporting rules, gather information on an as needed basis and to publish information obtained from digital platforms.

These new powers will provide greater transparency and insights on the effectiveness of platform measures to combat misinformation on their services. Information gathered by these powers may be used to inform investigations into potential breaches of misinformation codes and/or standards. The ACMA may take, and retain for as long as is necessary, possession of a document produced.

Additionally, the ACMA may disclose information to other persons and agencies should the information be relevant for efforts to combat misinformation and disinformation. This is enabled through consequential amendments to the definition of ‘authorised disclosure information’ in the ACMA Act made by this Bill, and correspondingly by Part 7A of the regime in that Act. There are protections for privacy and commercially sensitive information.

3.1 Division 1 – Scope

The information powers in Part 2 of Schedule 9 – to be inserted by the Bill, do not apply in relation to **excluded services for misinformation purposes** or **excluded content for misinformation purposes** – see sections 2.1.1 and 2.1.4 above.

Certain **limitations** also apply – see section 3.1.2 below.

All other digital platform services and content on these services will be within scope.

¹A minor change in the text is required to accommodate the specific requirements of the Bill. However, the intention of the test is identical for both. For example, section subparagraph (v) of the definition of **professional news content** in this Bill refers to digital platform rules. The equivalent is section 52P(1)(a)(vi) in the NMBC which refers to other regulations.

The ACMA could exercise its information powers regardless of whether or not the digital platform services are already signatories to an existing voluntary code of practice.

The ACMA will be able to use its information powers (record keeping and reporting, information-gathering and publication) in relation to:

- misinformation or disinformation on a digital platform service
- measures implemented by the digital platform provider to prevent or respond to such information on the service, including the effectiveness of the measures
- the prevalence of false, misleading or deceptive information provided on the digital platform service.

3.1.1 Electoral and referendum content is in scope of the information powers

The ACMA will be able to use its information powers in relation to election and referendum matters. For example, the ACMA would be able to request information on the length of time it takes for platforms to respond to complaints about misinformation about an electoral matter during a federal election. This will help to inform policy decision-making by government agencies on strengthening the integrity of Australian democratic processes and government institutions.

Note: Authorised electoral communications and electoral and referendum content will be out of scope of the **code and standard-making powers**, with the exception of disinformation from an unauthorised source as per clause 35 of the Bill.

3.1.2 The contents of private messages are out of scope

To protect the right to privacy, the ACMA will not be able to use its powers to require a person to produce information, evidence or documents that would reveal the contents of private messages (subclause 18(4)).

The ACMA will also not be able to make rules that require digital platform providers to make or retain records of the content of private messages (subclause 14(3)).

While private messages are a key feature of instant messaging services, it is envisaged that the ACMA would use its information-gathering and record keeping powers to understand more about platform measures to combat misinformation and how user complaints are addressed.

The registered codes and standards could have requirements that instant messaging services have measures in place that help address the harm of misinformation on their service without revealing the content of private messages. For example, this could include a range of educative measures that platforms provide to assist their users to critically assess information.

3.2 Division 2 – Record keeping and reporting

3.2.1 The ACMA may make digital platform rules in relation to records (Clause 14)

The ACMA will be provided with the power to make rules to require digital platform providers to make and retain records relating to:

- misinformation or disinformation on the digital platform service
- measures implemented by the digital platform provider to prevent or respond to misinformation or disinformation on the service, including the effectiveness of the measures

- the prevalence of false, misleading or deceptive information² provided on the digital platform service.

The ACMA may require digital platform providers prepare reports consisting of information contained in the records, and require providers to give any or all of these periodically to the ACMA. This will enhance transparency and allow tracking of digital platforms' progress in addressing misinformation. For instance, digital platform providers of certain services specified in the rules may be required to keep records of complaints and reports related to misinformation, and the measures taken in response, and provide this information in the form of a regular report to the ACMA.

The ACMA has consistently encouraged industry to establish a framework of key performance metrics aimed at measuring the effectiveness of digital platform measures to combat misinformation on their services. One potential use of these powers could be to get digital platform providers to keep and provide records on metrics in the framework. This would enable comparison of metrics and key indicators across the digital platforms industry, leading to increased transparency and greater comparability.

The ACMA would consult with industry in developing the record keeping rules and measurement framework as part of the usual consultation processes under the *Legislation Act 2003*.

Scenario 1: Record keeping rules

Signatories to a voluntary code have committed to report annually about the volume and nature of content that is being reported and complained about on their platforms. This is considered an important indicator of user confidence and can help inform policy development and response on a range of issues across government.

Signatories commit to meet this obligation through the release of annual transparency reports on their measures to combat misinformation. However, the ACMA's review of successive reports finds that this qualitative and quantitative data is not included, or is only provided at a global – and not national – level. Multiple platforms advise the ACMA that they do not currently report on this information, and do not provide it, despite the ACMA requesting it voluntarily.

The ACMA is also concerned about the lack of this data from platforms who are non-signatories of the voluntary code. The ACMA publicly consults on the draft record keeping rules which will apply to signatories and non-signatories. Under the proposed rule, platforms will need to regularly collect and report on Australia-specific data about reports and complaints, broken down by subject matter categories outlined in the rule. This information will be an important input to monitoring the effectiveness of the industry code and confidence in the process.

3.3 Division 3 – Information gathering

3.3.1 The ACMA may obtain information and documents from digital platform providers and other persons (Clauses 18 and 19)

The ACMA will have information-gathering powers that could be used to compel digital platform providers to give information, documents and evidence relevant to the same matters as the record keeping rules in section 3.2.1. These powers may be exercised on an as needed basis.

The ACMA may also request information from other persons on the same matters. These persons could include fact-checkers or other third-party contractors to digital platform providers, to assist the ACMA monitor compliance with misinformation codes, misinformation standards and digital platform rules.

² False, misleading or deceptive information has been included separate to misinformation and disinformation. False, misleading or deceptive information may not necessarily be seriously harmful, however to make complete assessments, the ACMA will be empowered to gather a wider range of information.

3.3.2 Self-incrimination (Clause 21)

This section of the Bill only applies to individual natural persons who own and operate a digital platform service. The vast majority of providers of digital platform services are body corporates, which have no privilege against self-incrimination.

The common law privilege against self-incrimination entitles an individual to refuse to answer any question, or produce any document, if the answer or the production would tend to incriminate that person – broadly referred to as the privilege against self-incrimination.

The Bill provides that a person is not excused from answering a question or providing information or a document on the ground that the answer to the question, or the information or document, may tend to incriminate the person or expose the person to a penalty. This abrogation of the privilege is necessary to avoid undermining the regulatory regime and the intention and purpose of the Bill. Enabling the ACMA to have the information necessary for it to undertake work to encourage digital platform services to protect the community against the harms from misinformation and disinformation is an important objective necessitating abrogation of this privilege.

However, any information or evidence or producing document cannot be used against the individual in criminal proceedings other than proceedings for an offence for giving false or misleading information under the *Criminal Code* and subclause 22(1) of this Bill.

This part of the Bill does not intend to abrogate legal professional privilege.

Scenario 2: Information-gathering powers

Over recent months, false and misleading claims have circulated on three platforms that a new telecommunications technology causes significant health issues leading to widespread concern and an increase in vandalism of telecommunications infrastructure. Independent technical research has found these claims are demonstratively false and the Chief Scientist has also refuted these claims.

The ACMA uses its information-gathering powers to request all three platforms to provide information about the measures taken by the platforms regarding this material (including takedowns, content demotion and the promotion of authoritative content), the reach of this information to Australian users on their platform and metrics going to the effectiveness of these measures (slowed traffic and sharing etc).

Scenario 3: Information-gathering powers

Platforms A, B and C are social media services, each with a significant Australian user base. Platforms A and B are signatories to a voluntary code, while Platform C is a non-signatory.

As part of public reporting under the code, Platforms A and B both report seeing an increase and amplification of objectively false user-generated material relating to an ongoing geopolitical conflict, that appears like it may be part of a co-ordinated disinformation campaign. Platforms A and B outline the steps they have taken to identify, review and moderate this content on their services, according to their respective community guidelines.

The ACMA has reason to believe that similar false content is being amplified on Platform C, however despite being asked, Platform C is unwilling to voluntarily provide information about its moderation activities.

In order to understand the scale of this potential disinformation campaign, the ACMA exercises its information-gathering powers to request information from Platform C about whether it has similarly seen an increase in false statements regarding the conflict, and what steps, if any, it has taken in response to this content.

3.4 Division 4 – Publishing information

To promote transparency, the ACMA would have the ability to publish the information collected under the information-gathering and record keeping powers on its website, including the identity of the platform to which the information relates.

The ACMA will **not be permitted to publish information** that is personal information within the meaning of the *Privacy Act 1988*. The ACMA will be required to consult with impacted providers to give them an opportunity to identify information that they consider if published could be expected to materially prejudice the commercial interests of a person and if so to provide reasons. The ACMA is required to take these reasons into account before publishing any information.

4. Part 3 of Schedule 9 – Misinformation codes and standards

This Part provides the framework for the graduated approach to codes and standards, as described in section 1.2 of this Guidance Note.

Note: This Part of the Bill does not deal with voluntary codes, unless industry requests and the ACMA agrees to register the voluntary code – in which case it will become a code that must be complied with by industry, and will be enforceable through civil penalties and other mechanisms through this Bill.

4.1 Division 1 – Scope

This term ‘misinformation’ in the context of misinformation codes and standards is referenced in this part as an umbrella term covering both misinformation and disinformation (i.e. disinformation is a subset of misinformation).

The misinformation code and standard-making powers in Part 3 of the Bill do not extend to **excluded services for misinformation purposes** or **excluded content for misinformation purposes** - see sections 2.1.1 and 2.1.4 above.

Certain **limitations** also apply – see sections 4.3.2 and 4.3.3 below.

All other digital platform services and content on these services will be within scope.

4.2 Division 2 – Interpretation

4.2.1 Sections of the digital platform industry (Clause 30)

The misinformation code and standard-making powers could apply to one or more sections of the digital platform industry, comprising content aggregation services, connective media services, and media sharing services.

The Minister under subclause 4(6) would have the power to specify new kinds of digital platform services, which would then fall within scope of the misinformation codes and standard powers.

The sections of the digital platform industry may not necessarily be mutually exclusive and may consist of the aggregate of any two or more sections or may be subsets of a section of the industry noted above.

In practice, a single industry body could make a single industry code that covers all three segments of the industry. This is similar to the current self-regulatory arrangements where DIGI has developed a single voluntary code that a range of platforms have signed up to. This approach may be optimal when platforms operate several digital platforms services. For example, Company Z is a provider of various digital platforms services such as news aggregation, search engine, social media platform and podcast.

Alternatively, an industry body representing one section of the industry could develop a code only relating to their segment (see scenario below).

Scenario 4: Sections of the digital platform industry

There has been heightened concern in the community about the amount of misinformation on content aggregation services such as search engines and news aggregators. Industry participants have formed a new industry group to tackle this issue and approach the ACMA about making a new code. The new code contains measures specific to search engines and news aggregators that operate in Australia.

The ACMA considers that the new industry body represents the content aggregator section of the digital platform industry, and is satisfied the code meets the conditions outlined in section 4.4.1 of this Guidance Note. The ACMA then registers the code.

4.3 Division 3 – General principles relating to misinformation codes and standards

This Division sets out general principles, including a statement of regulatory policy in relation to the development of codes. The Division states that it is intended that bodies or associations that represent sections of the digital platform industry should develop their own codes requiring participants in those sections of the digital platform industry to implement measures to prevent or respond to misinformation and disinformation on digital platform services.

The ACMA would have the ability to register a single code or multiple codes.

4.3.1 Matters that may be dealt with in a code and standard (Clause 33)

The following are some examples of matters that may be dealt with by misinformation codes and standards:

- preventing or responding to misinformation or disinformation on digital platform services
- using technology to prevent or respond to misinformation or disinformation on digital platform services
- preventing or responding to misinformation or disinformation on digital platform services that constitutes acts of foreign interference (within the meaning of the *Australian Security Intelligence Organisation Act 1979*)
- preventing advertising involving misinformation or disinformation on digital platform services
- preventing monetisation of misinformation or disinformation on digital platform services
- supporting fact checking
- allowing end-users to detect and report misinformation or disinformation on digital platform services
- policies and procedures for receiving and handling reports and complaints from end-users.

4.3.2 Limitations (Clauses 34 and 36)

The ACMA will not be able to register a code (or part of a code), or determine a standard, relating to:

- the content of private messages (clause 34)
- the encryption of private messages (clause 34).

The misinformation codes and standards will have no effect to the extent (if any) to which the matter is dealt with by other instruments, codes and standards referred to in clause 36 of the Bill.

4.3.3 Limitation – electoral and referendum matters with the exception of disinformation from an unauthorised source (Clause 35)

The code and standard-making powers will not apply to electoral and referendum content that is required to be authorised. They would also not apply to any other electoral matter content unless it is disinformation, for example, disinformation spread by a foreign state actor on a digital platform service to influence the outcome of an election in Australia.

This approach seeks to strike a balance between the public interest in combatting the serious harms that can arise from the propagation of misinformation and disinformation, with freedom of speech and political communication.

4.4 Division 4 – Misinformation codes

4.4.1 The ACMA may register codes (Clause 37)

The ACMA would have the ability to register industry developed codes which govern the arrangements of the digital platform industry.

The ACMA would need to be satisfied of a number of factors before registering an industry code including:

- the body or association proposing the code represents a particular section (or all sections) of the digital platform industry and it has consulted with members of the public and participants in the industry
- the code would provide adequate protection for the community against the harms of misinformation or disinformation on the digital platform services
- the code requires participants in that section of the industry to implement measures to prevent or respond to misinformation or disinformation on the digital platform services
- the code enables assessment of compliance with the measures
- whether the code burdens freedom of political communication, and if so whether this is reasonable and not excessive.

Registration of an industry code would make compliance with its obligations mandatory across a section of the industry (for instance a specific class of a digital platform service) or across the entire industry. Further details on the sections of the digital platform industry are outlined in clause 30 of the Bill.

The ACMA may examine the codes it has previously registered when it considers a code for potential registration to avoid conflict between a new code and existing code.

4.4.2 The ACMA may request misinformation codes (Clause 38)

The ACMA will have the power to request an industry body or association representing a particular section (or sections) of the digital platform industry to develop a new industry code which applies to its participants and deals with matters relating to the operation of digital platform services by those participants.

The ACMA may specify the timeframe in which the new code must be developed and given to the ACMA which must run for at least 120 days. The ACMA may specify indicative targets for achieving progress in the development of the code (for example, a target of 60 days to develop a preliminary draft of the code).

The ACMA cannot make such a request unless it is satisfied that the development of a code is necessary or convenient in order to prevent or respond to misinformation or disinformation on digital platform services of participants in that industry, or to address systemic issues. The ACMA must also be satisfied that in the absence of such a request, it is unlikely that the code would be developed within a reasonable period.

4.4.3 When no industry body or association exists (Clause 39)

If ACMA is satisfied that an industry body or association does not exist for a particular section of the digital platform industry, it may publish a notice on its website inviting industry to form such a body or association in order to develop a code. If the ACMA publishes such a notice, it must give industry at least 60 days to form a representative body or association. The ACMA may decide to do this, for example, if it determines that an industry code is necessary to protect Australians from misinformation or disinformation in a particular section of the digital platform industry.

Alternatively, the ACMA may choose to make an industry standard using its standard-making powers.

4.4.4 Variation of misinformation codes (Clause 40)

Given the codes are likely to cover a range of different measures that may need to change over time, the ACMA has the ability to consider variations and impacted parts, rather than the code as a whole. This is intended to allow variations to be considered and registered more quickly, allowing safeguards to come into force in a timelier manner.

Industry bodies may propose to vary a registered code by their own volition. The ACMA may also request a code be amended in the case of a partial failure (clause 49).

The ACMA may, by written notice given to the body or association, approve the draft variation. Except in the case where the variation is of a minor nature, the body or association must have published the draft variation on its website and given members of the public and participants in the industry at least 30 days to make submissions.

4.4.5 Replacement of misinformation codes and deregistration (Clauses 41 and 42)

Any changes to a code may be achieved by replacing the code instead of varying the code.

The ACMA would also have the ability to deregister a code or part of a code. Deregistration may be appropriate in circumstances where obligations in a code are no longer relevant or operational because they have, for example, been replaced by a subsequent code or a standard. A code could also be deregistered if an industry body no longer existed to maintain and update the code. Deregistration would mean that compliance with the code is no longer mandatory nor subject to the ACMA oversight.

Scenario 5: Requiring industry to develop new codes

A voluntary code (Industry Code A) has been in place for about 12 months. Over this period, the ACMA has gathered information from signatories and non-signatories of the voluntary code. The data indicates widespread misinformation on a range of digital platforms, particularly in large and public instant messaging chats. The misinformation falsely claims that specific community groups in Australia are responsible for a range of social issues. The misinformation seeks to undermine social cohesion and foster hatred towards certain groups in Australian society.

The ACMA assesses the effectiveness of the voluntary code and concludes that it has failed to provide adequate protections to the community against false and seriously harmful claims.

The ACMA requests Industry Body B, which represents the relevant section of the industry, connective media services, to develop a new code in order to address the specified deficiencies, including broadening the scope to include large group messaging services. Industry Body B provides the ACMA with a copy of the new code (Industry Code C) for review and registration, following consultation with industry participants and a public consultation process.

The ACMA reviews the new code and is satisfied that it meets the requirements of clause 37. Additionally, Industry Code C does not contain any requirements about the contents of private messages or the encryption of private messages. The ACMA registers the code and its obligations are mandatory for connective media services with an Australian user base. Registration provides the ACMA with the power to enforce compliance with Industry Code C.

Scenario 6: Varying registered codes

Industry Body D updates several provisions in Industry Code E which includes stronger protections for end-users such as support for media literacy initiatives and fact checking. This follows a public consultation period by Industry Body D of over 30 days, which includes the digital platform industry and the public. Industry Body D submits the draft variation to the ACMA, which approves and registers the variation given that it meets the requirements in clause 40, therefore amending Industry Code E.

Scenario 7: Deregistering registered codes

There is a registered code (Industry Code F) in place, which was drafted by Industry Body G. However, Industry Body G ceases to exist after two years of the code's registration. The ACMA publishes a notice under subclause 39(1) inviting the creation of a new body or association, but one is not formed. As such, the ACMA determines a standard under clause 47, the standard supersedes Industry Code F, and the ACMA deregisters Industry Code E.

4.5 Division 5 – Misinformation standards

The ACMA will be able to determine standards for industry through a legislative instrument. This is generally intended to be a last resort and these provisions will have higher penalties reflecting the graduated nature of the powers. A standard made by the ACMA could apply to one or more sections of the industry.

The ACMA would also be required to consult with the relevant body or association (where it exists) before making a standard. The matters that the ACMA can determine standards about as well as the limitations on these powers are the same as codes – also see sections 4.3.1, 4.3.2 and 4.3.3 of this Guidance Note.

4.5.1 General requirement – consideration of freedom of political communication (Clause 45)

The ACMA will be required to be satisfied of the following general factors before determining a standard:

- whether the standard would burden freedom of political communication; and
- if so, whether the burden would be reasonable and not excessive, having regard to any circumstances the ACMA considers relevant.

4.5.2 The ACMA may determine standards when a request for a code is not complied with or no industry body or association has been formed (Clauses 46 and 47)

The ACMA may determine a standard if a request for a code is not complied with, indicative targets for code development were not met or the ACMA otherwise refuses to register a code; and the ACMA is satisfied that it is necessary or convenient to determine a standard in order to provide adequate protection for the community from misinformation or disinformation on the digital platform services.

If no industry body or association exists and none has been formed following the ACMA publishing a notice under clause 39 inviting one to be formed for the purpose of creating a code, the ACMA may determine a standard for the unrepresented section of the digital platform industry.

4.5.3 The ACMA may determine standards when an existing code fails (Clauses 48 and 49)

Should a registered code exist, and the ACMA has determined that it is partially or wholly deficient in protecting Australians from misinformation or disinformation on the services, the ACMA will give a notice to the body that developed the code requesting that the deficiencies be addressed in a specified period. If the body is unable to address the deficiencies to a satisfactory standard, the ACMA may determine a standard that supersedes the deficient code (or parts of it in the case of a partial failure).

4.5.4 The ACMA may determine standards due to emerging circumstances (Clause 50)

There may be exceptional and urgent circumstances where Australians are at significant risk of harm from misinformation or disinformation (e.g. a time of war). If the ACMA determines a code or standard is necessary or convenient to provide protection, and the ACMA considers a code may not be able to made in a reasonable time period, then the ACMA could determine an industry standard.

4.5.5 Variation of standards and revocation of standards (Clauses 51 and 52)

The ACMA will have the ability to vary or revoke a misinformation standard, including by adding or removing sections or amending or strengthening requirements.

4.6 Division 6 – Register of misinformation codes and standards

The ACMA is to maintain an electronic register of codes and standards, and intends to do this on its website to provide transparency and accessibility to the public and industry.

5. Additional information – Enforcement

Note: This section sets out the enforcement mechanisms available in relation to the new powers. Relevant provisions are in proposed new Schedule 9 inserted by Schedule 1 to this Bill, as well as in the Consequential Amendments (Schedule 2 to the Bill).

5.1 Graduated approach to enforcement

The ACMA uses a graduated and strategic risk-based approach to compliance and enforcement. This approach recognises that breaches of laws will be dealt with effectively and efficiently. It also recognises the role of co-regulation set out in the legislation it administers and of engaging with the regulated community to promote compliance.

The ACMA will have access to powers under Part 13 of the BSA to enforce compliance with proposed new Schedule 9 outlined in the Bill. This will include powers to seek information and conduct investigations into any matters relevant to ACMA’s content functions, such as in relation to potential breaches of misinformation codes and standards.

The ACMA will be able to use its investigatory powers to seek information from platforms, or relevant third parties to ensure that codes and standards are being complied with. Where breaches are found, the ACMA will be able to take regulatory action commensurate with the seriousness of the breach and the level of harm. It is intended that it will generally use the minimum power or intervention necessary to achieve compliance.

The regulatory enforcement tools available to the ACMA are summarised below.

Table 2: Enforcement

Type	Details of enforcement
Formal warnings	Notices issued for non-compliance with any obligations, specifying the nature of the breach and steps to remedy the situation
Remedial directions	A legally binding direction to take specific remedial action to remedy a breach
Enforceable undertakings	A voluntary agreement by a person or digital platform service to comply with an obligation
Infringement notices	A penalty notice issued by the ACMA for breaching certain obligations, which carries a lower financial penalty than a civil penalty
Injunctions	The ACMA may seek a court issued injunction to enforce compliance, particularly if repeated breaches occur after a formal warning or remedial direction has been issued
Civil penalties	Financial penalties imposed by a court as a result of a breach of obligations and serve as a deterrent against future non-compliance

5.2 Compliance with the record keeping rules (Clauses 15 and 16)

Digital platform services must comply with record keeping rules.

The ACMA has the power to issue a formal warning to the provider if it is satisfied that a digital platform provider has contravened the record keeping rules. A formal warning can be used to place a provider on notice that the ACMA has identified issues of concern, thereby providing them with an opportunity to address those issues, but also warns them that stronger enforcement action may be taken if the non-compliance is not rectified or it recurs.

The ACMA may also issue an infringement notice to address non-compliance, containing the matters specified in section 205Z of the BSA, including:

- details relating to the alleged contravention of the designated infringement notice provision
- the penalty amount of 60 penalty units (\$16,500 in 2023) for corporations and 10 penalty units (\$2,750 in 2023) for individuals
- the deadline for paying the penalty.

The ACMA will also be empowered to issue remedial directions (clause 16). These are given in writing and direct the person or entity to take specified action aimed at ensuring that the breach is remedied or that it is unlikely to recur in the future.

Digital platform providers that contravene record keeping rules, or who fail to comply with remedial directions, will face civil penalty proceedings and may be fined up to 5,000 penalty units (\$1,375,000 in 2023) for corporations or 1,000 penalty units (\$275,000 in 2023) for individuals. A digital platform provider will commit a separate contravention in respect of each day during which the contravention continues.

5.3 Compliance with information-gathering powers (Subclauses 18(5) and 19(5))

A digital platform provider or other person who has relevant information, documents or evidence must comply with requests for information from the ACMA.

The ACMA may issue a formal warning to the digital platform provider or person if it is satisfied that the person has not complied with the requirements of a written notice issued by it under the information-gathering powers.

The ACMA can also issue an infringement notice to address non-compliance, containing the matters specified in section 205Z of the BSA, including:

- details relating to the alleged contravention of the designated infringement notice provision
- the penalty amount (8 penalty units, being \$2,200 in 2023) for corporations, and 6 penalty units (\$1,650 in 2023) for individuals
- the deadline for paying the penalty.

As a final enforcement option, the ACMA may seek civil penalties of up to 40 penalty units (\$11,000 in 2023) for corporations and 30 penalty units (\$8,250 in 2023) for individuals. This will be a daily amount if the contravention continues.

5.4 False or misleading information or evidence under the record keeping rules and information-gathering powers (Clauses 17 and 22)

It will be an offence of 100 penalty units (\$27,500 in 2023) if a digital platform provider knowingly makes or retains false or misleading records, or omits any matter which makes them misleading, in purported compliance with the digital platform rules.

Providing false or misleading information or evidence in response to an information-gathering request by the ACMA is also an offence which carries a penalty of imprisonment for 12 months. This reflects the approach taken in section 525 of the *Telecommunications Act 1997*. Of course, this penalty does not apply when the digital platform provider or other persons provide the ACMA with information containing false or misleading content for the purposes of complying with the powers (e.g. examples of misinformation removed from the platform).

5.5 Compliance with Misinformation codes and standards (Clauses 43, 44, 53 and 54)

Registered misinformation codes and misinformation standards will be enforceable using the same mechanisms referred to above.

The ACMA may issue a formal warning to the provider if it is satisfied that a digital platform provider has contravened a registered code or standard.

The ACMA will also be empowered to issue remedial directions to platforms that fail to comply with a registered code or standard. These are given in writing and direct the person or entity to take specified action aimed at ensuring that the breach is remedied or that it is unlikely to recur in the future.

The ACMA will be empowered to give an infringement notice for contraventions of the codes or standards. In issuing an infringement notice, the ACMA is alleging that the relevant contravention has occurred. If the recipient of the notice pays the specified penalty, their liability for the alleged contravention is discharged. If the penalty is not paid, it will be the court's role to consider and determine, upon the application of the ACMA, whether in fact the alleged contravention has been established. Should the ACMA issue an infringement notice, it must contain the matters specified in s205Z of the BSA, including:

- details relating to the alleged contravention of the designated infringement notice provision
- the penalty amount (maximum of 60 penalty units (\$16,500 in 2023) for corporations or 10 penalty units (\$2,750 in 2023) for individuals)
- the deadline for paying the penalty.

Digital platform providers can face significant civil penalties under the Bill, and it is expected that the ACMA will actively seek penalty orders against those providers who routinely contravene provisions in a registered code or a standard, or fail to comply with remedial directions in particular.

The maximum amount of civil penalties is intended to deter systemic non-compliance by digital platform services and reflects the serious large scale social, economic and/or environmental harms and consequences that could result from the spread of misinformation or disinformation.

The civil penalties for breaches of standards are greater than breaches of codes as a standard is the highest level of regulatory action in the regulatory framework.

Table 3: Maximum penalties on non-compliance with a registered code or standard

Registered Code – non-compliance	Industry Standard – non-compliance
Maximum of 10,000 penalty units (\$2.75 million in 2023) or 2 per cent of global turnover (whatever is greater) for corporations or 2,000 penalty units (\$0.55 million in 2023) for individuals.	Maximum of 25,000 penalty units (\$6.88 million in 2023) or 5 per cent of global turnover (whatever is greater) for corporations or 5,000 penalty units (\$1.38 million in 2023) for individuals.

5.6 Comparison with fines in the European Union and Australia

The EU's Digital Services Act (DSA) was approved in October 2022 and regulates a range of digital platform services such as social media, online marketplaces, and search engines. It covers a wider range of harmful content than the ACMA powers such as illegal hate speech, child sex abuse material, terrorist content, misinformation and disinformation.

Failure to comply with the DSA may, in serious cases such as systemic failure to comply, result in significant fines for Very Large Online Platforms (VLOPs) of up to six per cent of a digital platform services annual global turnover. Lesser breaches, such as giving incorrect information to the EU regulators, may result in fines of up to one percent of platform annual turnover.

The fines in the EU and the penalties proposed in the Bill as outlined above are intended to give a clear signal that systemic non-compliance with obligations to prevent and respond to misinformation and disinformation is unacceptable and that platforms need to protect end-users.

In Australia, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* created a new offence for content and hosting service providers around the world who fail to expeditiously remove abhorrent violent material capable of being accessed within Australia. The penalty for a corporation that fails to remove content expeditiously under the *Criminal Code* is up to 50,000 penalty units (\$13.75 million in 2023) or 10 per cent of the global annual turnover of the company, whichever is greater. The penalty for a person who fails to remove content expeditiously is up to 10,000 penalty units (\$2.75 million in 2023) or 3 years' imprisonment, or both.

6. Part 4 of Schedule 9 – Miscellaneous

Part 4 of the Bill contains a number of miscellaneous provisions of which some are briefly outlined below.

6.1 Service of summons, process or notice on corporations incorporated outside Australia (Clause 58)

Where a summons, process or notice is required to be served on or given to a body corporate incorporated outside Australia; and the body corporate does not have a registered office or a principal office in Australia; and the body corporate has an agent in Australia, that summons, process or notice may be served on or given to its agent.

6.2 Relationship with other laws (Clause 59)

The new Schedule 9 to be inserted by the Bill does not limit the operation of other laws such as Part 13 or Schedule 8 of the *Broadcasting Services Act 1992*, Part 9 of the *Online Safety Act 2021*, the *Commonwealth Electoral Act 1918*, the *Referendum (Machinery Provisions) Act 1984* or the *Telecommunications Act 1997*.

6.3 Implied freedom of political communication (Clause 60)

The provisions in Schedule 9; the digital platform rules, any misinformation code registered under Part 3 and any misinformation standards will have no effect to the extent (if any) that their operation would infringe any constitutional doctrine of implied freedom of political communication. This provision is to make clear that any such provisions would be invalid to the extent that they have such an effect, however would otherwise continue to operate.

6.4 Concurrent operation of State and Territory laws (Clause 62)

The ACMA powers will not apply to the exclusion of a law of a State or Territory to the extent to which that law is capable of operating concurrently with this Schedule.

6.5 Schedule not to affect performance of State or Territory functions (Clause 63)

The ACMA powers must not be exercised in such a way as to prevent the exercise of the powers, or the performance of the functions, of government of a State, the Northern Territory or the Australian Capital Territory.

6.6 Digital platform rules (Clause 64)

The ACMA may, by legislative instrument, make rules (the digital platform rules) prescribing matters which give effect to the Bill. The rules will be not be able to do a number of things such as create an offence or civil penalty, impose a tax and provide powers of arrest, entry, search or seizure.

7. Consequential amendments and transitional provisions

7.1 Australian Communications and Media Authority Act 2005

References to the new Schedule 9 of the *Broadcasting Services Act 1992* have been added into the ACMA Act.

Several functions have been added to the ACMA's broadcasting, content and datacasting functions list in section 10 of the ACMA Act. These new functions enable the ACMA to assist industry with code development; to develop standards; to monitor compliance with codes, standards and rules; conduct investigations; inform itself and advise the Minister on misinformation on digital platform services and publish information relating to misinformation.

7.2 Broadcasting Services Act 1992

7.2.1 Regulatory Intent

The regulatory intent in section 4 of the BSA has been updated with subsection 4(3AC) outlining the Parliament's intention that the ACMA be able to regulate digital platform services in order to prevent and respond to misinformation and disinformation on the services.

7.2.2 Decisions appealable to the Administrative Appeals Tribunal

The following decisions by the ACMA will be appealable to the Administrative Appeals Tribunal (AAT):

- to give a remedial direction – subclause 16(2), 44(2) or 54(2) of Schedule 9
- variation of a remedial direction – subclause 16(2), 44(2) or 54(2) of Schedule 9
- refusal to revoke a remedial direction – subclause 16(2), 44(2) or 54(2) of Schedule 9
- refusal to register a misinformation code or part of a misinformation code – subclause 37(3) of Schedule 9.

7.2.3 Other key changes

- references to new Schedule 9 and its provisions have been added throughout.
- the long title of the BSA and its objects provision have been amended to reflect that regulation of digital platform services has been brought within the ambit of the BSA.
- the BSA civil penalty provisions have been amended to include penalties in relation to non-compliance with certain provisions in Schedule 9.

8. Attachment 1: Graduated application of the ACMA powers

Voluntary code framework

Platforms continue to fulfil their commitments under the voluntary code, including the publication of annual transparency reports.

Recognising the voluntary nature of the framework, it is intended that the ACMA, in the first instance, would work with digital platforms to voluntarily lift ambition in addressing misinformation and disinformation.

Regulatory levers may be used by the ACMA if the voluntary framework proves inadequate



Information-gathering, record keeping and publishing powers (apply at all times)

The ACMA's information-gathering powers may be used to compel a provider of a digital platform service to provide information or data on how they are complying with their obligations under a voluntary code or any future registered code or standard. The ACMA may also obtain information from other persons (e.g. fact-checkers and third-party contractors of digital platform providers to deal with possible misinformation or disinformation content on their services) to assist the ACMA with its compliance efforts.

The ACMA may also make targeted record keeping rules to improve the data collected by digital platform providers on a periodic basis. To promote transparency, the ACMA would have the ability to publish the information collected under the information-gathering and record keeping powers.

These powers can apply to the full range of digital platform services and digital platform providers, including those providers who chose not to sign up to a voluntary code.



The ACMA could ask industry to make new codes and register industry codes

Should the ACMA determine that stronger action is needed to protect Australians, it could request that a section of the industry put in place a new and more effective code of practice (than the existing DIGI voluntary code of practice, for example).

Once the ACMA is satisfied a draft code presented to it by industry meets a number of criteria, it may register it which makes compliance with it compulsory for all digital platform services providers in the relevant segment of the industry. This would include those providers who chose not to sign up to a voluntary code.



The ACMA could make an industry standard

In the event previous efforts through a code had not been effective, or a code was not developed, or otherwise in urgent and exceptional circumstances, the ACMA would have the power to make an enforceable standard.

A standard would be a determination written by the ACMA that would require providers of digital platform services to combat misinformation and disinformation on their services. Such a standard would have higher penalties than registered codes and would generally reflect a determination that previous efforts had not been effective.

9. Attachment 2: What is in scope of the ACMA powers

Table 4: Key examples of what is in scope of the ACMA powers

Examples	Information powers	Code and standard powers
Misinformation	In scope	In scope
Disinformation	In scope	In scope
Professional news content	Excluded	Excluded
Authorised electoral and referendum content	In scope	Excluded
Unauthorised electoral or referendum content that is misinformation	In scope	Excluded
Unauthorised electoral or referendum content that is disinformation	In scope	In scope
Satire / parody / entertainment – content produced in good faith for these purposes	Excluded	Excluded
Content authorised by an Australian Federal, State, Territory or Local Government	Excluded	Excluded
Educational content produced by or for accredited educational providers	Excluded	Excluded
Private message content	Excluded	Excluded
Digital platform services (excluding services in clause 6) <ul style="list-style-type: none"> - search engines - news aggregators - instant messaging services - social media - web-forums - dating sites - online peer-to-peer marketplaces - podcasting services (with an interactive feature) 	In scope	In scope
Excluded services for misinformation purposes (clause 6 services) <ul style="list-style-type: none"> - email, Broadcast Video On Demand Services (BVODS), Subscription Video On Demand Services (SVODS), podcasts without an interactive feature as defined in clause 5 	Excluded	Excluded