2022-2023-2024

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024

EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Communications, the Hon Michelle Rowland MP)

COMMUNICATIONS LEGISLATION AMENDMENT (COMBATTING MISINFORMATION AND DISINFORMATION) BILL 2024

OUTLINE

Overview of the Bill

The *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* (the Bill) amends the *Broadcasting Services Act 1992* (the BSA), and other Acts as relevant for consequential amendments and transitional provisions. It has three key objectives:

- to empower the Australian Communications and Media Authority (ACMA) to require digital communications platform providers take steps to manage the risk that misinformation and disinformation on digital communications platforms poses in Australia
- to increase transparency regarding the way in which digital communications platform providers manage misinformation and disinformation
- to empower users of digital communications platforms to identify and respond to misinformation and disinformation on digital communications platforms.

The Bill adds a new Schedule 9 to the BSA. It imposes core obligations on digital communications platform providers to:

- assess risks relating to misinformation and disinformation on their platforms, and publish a report of the outcomes of that assessment
- publish their policy or policy approach in relation to managing misinformation and disinformation
- publish a media literacy plan setting out the measures the provider will take to enable end-users of the platform to better identify misinformation and disinformation.

New Schedule 9 also empowers the ACMA to:

- obtain information and documents relating to misinformation and disinformation from digital communications platform providers
- make rules (disallowable by Parliament) requiring digital communications platform providers to make and retain records relating to misinformation and disinformation, and to prepare reports consisting of information contained in those records
- approve and register enforceable misinformation codes (disallowable by Parliament) that have been developed by sections of the digital platforms industry, setting out the measures those sections of the industry will take to reduce the risk of misinformation and disinformation
- in certain circumstances – for example, if misinformation codes do not adequately protect the Australian community from misinformation and disinformation, determine misinformation standards (disallowable by Parliament) for sections of the digital platforms industry
- make rules requiring digital communications platform providers to implement and maintain a process for handling complaints and resolving disputes about misinformation and disinformation

- publish information relating to misinformation and disinformation.

Digital communications platform providers will continue to be responsible for the content they host and promote to users. The definitions of misinformation, disinformation and serious harm set out the types of societal harms the powers are designed to address, and ensure that the ACMA's use of its powers, and the platforms' systems and processes, are targeted at serious harms with significant and far-reaching implications for the Australian community or a segment thereof, or severe consequences for an individual in Australia. The types of harm are: harm to the operation or integrity of an electoral or referendum process in Australia; harm to public health in Australia including the efficacy of preventative health measures; vilification of a group in Australian society; intentionally inflicted physical injury to an individual; imminent damage to critical infrastructure or disruption of emergency services in Australia; and imminent harm to the Australian economy.

The intent of the Bill is to set a high and targeted threshold for the definition of misinformation and disinformation. It does not intend to cover *all* dissemination of content that may be considered false, but rather, dissemination of content that is verifiably false, misleading or deceptive, and causing or contributing to serious harm.

Context for the Bill

The rapid spread of seriously harmful misinformation and disinformation poses a major challenge to the proper functioning of societies across the world. In democratic countries such as Australia which rely on the free flow of information to inform public debate, the integrity, diversity and reliability of information is fundamental to our democratic way of life.

Digital communications platforms enable online users in Australia to connect with family, friends and those with common interests, without regard for geographic distance. Although this has brought significant benefits, it can also serve as a vehicle for the widespread dissemination of misleading or false information that is seriously harmful to Australians.

Given the increasing reliance on digital communications platforms for information, and the benefits that platform providers derive from this reliance, these providers bear considerable responsibility for information circulating in the information environment. Providers have a responsibility to help their users more easily discern the quality of information, provide reporting tools, and reduce exposure to and the impact of seriously harmful misinformation and disinformation on Australians.

Four in five Australians say the spread of misinformation on social media needs to be addressed in Australia, according to the Australian Media Literacy Alliance's Adult Media Literacy 2024 report. This was an increase of 6 per cent over the 2021 report.[1]

In Australia, some steps have been taken by the digital platform industry to address the challenge of misinformation and disinformation. In December 2019, as part of the Government's response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry, the ACMA was asked to oversee the development of a voluntary code by

[1] Tanya Notley et al, *Adult Media Literacy in 2024: Australian Attitudes, Experiences and Needs* (Australian Media Literacy Alliance, August 2024) <https://medialiteracy.org.au/wp-content/uploads/2024/08/AML2024_report_final-compressed.pdf>.

industry on disinformation and news quality. In February 2021, the Digital Industry Group Inc (DIGI) launched the *Australian Code of Practice on Disinformation and Misinformation* (the voluntary code), which requires its signatories to commit to a number of measures to address misinformation and disinformation on their services.[2] The voluntary code currently has nine signatories: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok, Twitch and Legitimate. A number of other major digital communications platform providers are not signatories to the voluntary code.

The signatory status of X (formerly Twitter) was withdrawn in November 2023 by the voluntary code's independent Complaints Sub-Committee following X's refusal to take remedial action or cooperate in an investigation into a complaint about X closing, and leaving closed, accessible channels for the public to report misinformation and disinformation on the platform during the Australian Voice to Parliament referendum.[3]

The voluntary code has been an important first step in combatting the propagation of misinformation and disinformation online. However, as outlined in the ACMA's June 2021 and July 2023 reports to the Australian Government, there are a number of shortcomings with the existing self-regulatory arrangements. These include a lack of consistent and trended data available from digital communications platform providers on their measures and actions taken to address misinformation and disinformation in the Australian context, as well as issues associated with the effectiveness of the administration of the voluntary code.[4] An independent assessment of the 2024 annual transparency reports from the voluntary code signatories also raised concerns about the lack of 'trended data and associated commentary' specific to the Australian context and noted that recent improvements in the quality of the reports had stalled compared to previous years.[5]

The ACMA is engaging with the industry to develop a measurement framework to bolster the reporting framework under the voluntary code. This is aimed at establishing metrics to measure the effectiveness of and provide greater transparency on the systems and processes signatories have in place to meet code outcomes. The measurement framework would be enhanced by the Bill, which provides the ACMA with powers to make rules requiring digital communications platform providers to keep records and provide reports to the ACMA on key metrics that measure the effectiveness of their activities to combat misinformation and disinformation.

The ACMA's powers are directed to digital communications platform providers and not individual end-users. The Bill aims to incentivise digital communications platform providers to have robust systems and measures in place to address misinformation and disinformation

---

[2] Digital Industry Group Inc (DIGI), *Australian Code of Practice on Disinformation and Misinformation* (22 December 2022) ('*DIGI Code'*) <DISINFORMATION CODE | DIGI>.
[3] DIGI, 'Complaint by Reset Australia Against X (FKA Twitter) Upheld by Australian Code of Practice on Disinformation and Misinformation Independent Complaints Sub-Committee' (Media Release, 27 November 2023) <Complaint by Reset Australia against X (f.k.a Twitter) upheld by Australian Code of Practice on Disinformation and Misinformation independent Complaints Sub-Committee | DIGI>.
[4] ACMA, *Digital Platforms' Efforts Under the Australian Code of Practice on Disinformation and Misinformation* (Second Report to Government, July 2023) <Digital platforms' efforts under the Australian Code of Practice on Disinformation and Misinformation, second report to government (acma.gov.au)>; ACMA, *A Report to Government on the Adequacy of Digital Platforms' Disinformation and News Quality Measures* (June 2021) <Adequacy of digital platforms disinformation and news quality measures.pdf (acma.gov.au)>.
[5] DIGI, *Australian Code of Practice on Disinformation and Misinformation: Annual Report* (31 May 2024) <https://digi.org.au/wp-content/uploads/2024/05/ACPDM-_-Annual-Report-_-May-2024-FINAL.pdf> 9.

on their services. It does not provide the ACMA with powers to directly regulate content on digital communications platforms itself. Nor does it empower the ACMA to require digital communications platform providers to remove content or block end-users from their services, except in the case of content that involves inauthentic behaviour (for example, coordinated bots, troll farms or fake accounts). The ACMA would not have a direct takedown power for individual content or particular accounts.

The Bill does not apply to professional news, content that would reasonably be regarded as parody or satire, nor the reasonable dissemination of content for any academic, artistic, scientific or religious purpose. Additionally, the Bill contains significant protections for freedom of expression generally explained further in this Explanatory Memorandum.

It is expected that the ACMA will use a graduated, proportionate and risk-based approach to non-compliance and enforcement, including by issuing formal warnings, remedial directions and infringement notices, through to applying for injunctions and civil penalties, depending on the particular provision. The Bill provides scope for key decisions by the ACMA to be reviewed in the Administrative Review Tribunal (ART) and the amount of civil penalties payable by digital communications platform providers for breaches of approved misinformation codes and misinformation standards would be determined by the courts (up to the maximum amounts specified in the Bill).

Financial impact statement

The measures in the Bill are expected to have a minor financial impact on Commonwealth expenditure. Funding for the ACMA to administer provisions in this Bill was considered in the 2023-24 Budget.

Impact Analysis

An Impact Analysis for this Bill has been prepared in consultation with the Office of Impact Analysis. A copy of this Impact Analysis is attached at the end of this Explanatory Memorandum.

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024

This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

The *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* (the Bill) amends the *Broadcasting Services Act 1992* (the BSA), and other Acts as relevant for consequential amendments and transitional provisions. It has three key objectives:

- to empower the Australian Communications and Media Authority (ACMA) to require digital communications platform providers take steps to manage the risk that misinformation and disinformation on digital communications platforms poses in Australia
- to increase transparency regarding the way in which digital communications platform providers manage misinformation and disinformation
- to empower users of digital communications platforms to identify and respond to misinformation and disinformation on digital communications platforms.

The Bill adds a new Schedule 9 to the BSA. It imposes core obligations on digital communications platform providers to:

- assess risks relating to misinformation and disinformation on their platforms, and publish a report of the outcomes of that assessment
- publish their policy or policy approach in relation to managing misinformation and disinformation
- publish a media literacy plan setting out the measures the provider will take to enable end-users of the platform to better identify misinformation and disinformation.

New Schedule 9 also empowers the ACMA to:

- obtain information and documents relating to misinformation and disinformation from digital communications platform providers
- make rules requiring digital communications platform providers to make and retain records relating to misinformation and disinformation, and to prepare reports consisting of information contained in those records
- approve and register enforceable misinformation codes that have been developed by sections of the digital platforms industry, setting out the measures those sections of the industry will take to reduce the risk of misinformation and disinformation

- in certain circumstances – for example, if misinformation codes do not adequately protect the Australian community from misinformation and disinformation, determine misinformation standards for sections of the digital platforms industry
- make rules requiring digital communications platform providers to implement and maintain a process for handling complaints and resolving disputes about misinformation and disinformation
- publish information relating to misinformation and disinformation.

Schedule 9 to the BSA defines misinformation and disinformation as the dissemination of content on a digital communications platform that, among other criteria, contains information that is reasonably verifiable as false, misleading or deceptive, and is reasonably likely to cause or contribute to serious harm of a specified type, with significant and far-reaching consequences for the Australian community (or a segment thereof) or severe consequences for an individual in Australia. The types of serious harm are:

- harm to the operation or integrity of an Australian electoral process
- harm to public health in Australia
- vilification of a group in Australian society distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin, or vilification of an individual because of a belief that the individual is a member of such a group
- intentionally inflicted physical injury to an individual in Australia
- imminent damage to critical infrastructure or disruption of emergency services in Australia
- imminent harm to the Australian economy.

The effect of misinformation and disinformation being defined in this way is that the entirety of Schedule 9 to the BSA – including the ACMA's regulatory powers and the core transparency obligations imposed on digital communications platform providers – is aimed specifically at addressing the risk that verifiably false, misleading or deceptive content disseminated on digital communications platforms will cause or contribute to one of these types of harm. These harms align with the purposes for which international human rights law allows restrictions to be placed on the freedom of expression.

The measures provided for in Schedule 9 focus on systems and processes, rather than the regulation of individual pieces of content. In line with this intent, there is an explicit statement in Schedule 9 to the BSA that nothing therein – or in any rule, code or standard made, approved or determined pursuant to Schedule 9 to the BSA – can require digital communications platform providers to remove content or ban an account, except in the case of disinformation that involves inauthentic behaviour.

Schedule 9 to the BSA empowers the ACMA to enforce compliance with digital platform rules, approved misinformation codes or misinformation standards, and core transparency obligations. Enforcement mechanisms available to the ACMA include formal warnings, remedial directions, infringement notices and civil penalties.

Human rights implications

Schedule 9 to the BSA assists to ensure the enjoyment by all Australians of the following rights:

- the right to security of the person, enshrined in Article 9 of the *International Covenant on Civil and Political Rights* (ICCPR)[6]
- the right to participate in public affairs, and to vote and be elected at genuine periodic elections, enshrined in Article 25 of the ICCPR
- the right to be protected against discrimination, enshrined in Articles 2 and 26 of the ICCPR, Article 2(b) of the *Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW)[7] and Article 2 of the *International Convention on the Elimination of All Forms of Racial Discrimination* (CERD)[8]
- the right to the highest attainable standard of physical and mental health, enshrined in Article 12 of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR).[9]

The Bill limits the following rights:

- the right to privacy, enshrined in Article 17 of the ICCPR
- the right to freedom of expression, enshrined in Article 19 of the ICCPR.

The context of Schedule 9's positive contributions to and limitations on human rights is explained in detail in the following sections.

Schedule 9 to the BSA seeks to reduce the risk of certain content being disseminated online, thereby protecting the human rights of Australians.

Human rights positively affected by the Bill

Right to security of the person

Article 9 of the ICCPR provides that 'everyone has the right to liberty and security of person'. The United Nations (UN) Human Rights Committee has said that this right protects individuals against the 'intentional infliction of bodily or mental injury'. This obliges States Parties to, for example, 'take appropriate measures in response to death threats against persons in the public sphere, and more generally to protect individuals from foreseeable threats to life or bodily integrity proceeding from any governmental or private actors'.[10]

The dissemination of content on a digital service will be considered misinformation or disinformation if, in addition to meeting the other criteria specified in clauses 13 and 14 of Schedule 9 to the BSA, it is reasonably likely to cause or contribute to the intentional infliction of physical injury to an individual in Australia. The inclusion of this type of harm in

[6] Opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) ('ICCPR').
[7] Opened for signature 18 December 1979, 1249 UNTS 1 (entered into force 3 September 1981) ('CEDAW').
[8] Opened for signature 7 March 1966, 660 UNTS 1 (entered into force 4 January 1969) ('CERD').
[9] Opened for signature 16 December 1966, 993 UNTS 3 (entered into force 3 January 1976) ('ICESCR').
[10] Human Rights Committee (HRC), *General Comment No 35: Article 9: Liberty and Security of Person*, UN Doc CCPR/C/GC/35 (16 December 2014) para 9; see also HRC, *Views: Communication No 1958/2010*, UN Doc CCPR/C/111/D/1958/2010 ('*El Hojouj Jum'a et al v Libya')* para 6.5.

clause 14 means that digital communications platform providers have a responsibility to be transparent about the way in which they handle that type of content, and that the ACMA has regulatory powers in relation to such content.

False, misleading or deceptive information that is likely to result in physical injury to individuals might include the incitement of violence, or smear campaigns targeting prominent individuals for political or personal reasons, or content incorrectly framing an individual or individuals for wrongdoing, provoking public outrage. The misinformation campaign that followed the attacks in Bondi, Sydney in April 2024, wrongly identifying a Jewish Australian as responsible for the attacks and resulting in death threats to that individual, provides an example,[11] as does the misinformation campaign that targeted a Gold Coast doctor in February 2022, which also included death threats, following claims on social media that two girls died after being vaccinated for COVID-19 at his practice.[12] Other examples from around the world include false reports about child abductions spread on social media and messaging apps in France in 2019, which prompted vigilante attacks against Roma people;[13] and a video that went viral in India in 2018, falsely identifying five individuals as child kidnappers, prompting a mob attack on those individuals.[14]

Schedule 9 to the BSA seeks to reduce the risk of this type of content being disseminated online, and in this way assists to protect the right of Australians to security of the person.

The right to participate in public affairs, and to vote and be elected

Article 25 of the ICCPR provides, *inter alia*, that 'every citizen shall have the right and the opportunity, … without unreasonable restrictions: (a) to take part in the conduct of public affairs, directly or through freely chosen representatives; [and] (b) to vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors'.

Misinformation and disinformation can undermine the right of Australians to participate in the conduct of public affairs, or to vote and be elected at genuine periodic elections, if it is disseminated at such a scale that it harms the operation or integrity of an Australian electoral process. To guard against this risk, pursuant to the regulatory scheme set out in Schedule 9 to the BSA, the dissemination of content on a digital service is considered misinformation or disinformation if, in addition to meeting other criteria specified in clauses 13 and 14, it is reasonably likely to cause or contribute to serious 'harm to the operation or integrity of a Commonwealth, State, Territory or local government electoral or referendum process'. The

[11] See Joseph Olbrycht Palmer, 'Social Media Users Incorrectly Name Killer in Sydney Mall Attack', *AFP Fact Check* (18 April 2024) <https://factcheck.afp.com/doc.afp.com.34PH9YM>; Kevin Nguyen and Michael Workman, 'Benjamin Cohen was falsely accused of the Bondi Junction stabbings. Here's how the lie spread around the world' (*ABC Investigations*, 16 April 2024) <Benjamin Cohen was falsely accused of the Bondi Junction stabbings. Here's how the lie spread around the world - ABC News>.

[12] Anastasia Tsirtsakis, 'RACGP calls for anti-vaxxer crackdown after GP receives death threats', *The Age* (online, 1 February 2022) <https://www1.racgp.org.au/newsgp/professional/racgp-calls-for-crackdown-on-anti-vaxxers-after-gp>.

[13] Agence France-Presse (AFP), 'Roma attacked in Paris after fake news reports', *The Guardian* (28 March 2019) <Roma attacked in Paris after fake news reports | Roma, Gypsies and Travellers | The Guardian>; Judit Szakacs and Eva Bognar, *The Impact of Disinformation Campaigns about Migrants and Minority Groups in the EU* (European Parliament, Directorate-General for External Policies) <The impact of disinformation campaigns about migrants and minority groups (europa.eu)> 14.

[14] Elyse Samuels, 'How misinformation on WhatsApp led to mob killings in India', *The Washington Post* (21 February 2020) <How misinformation on WhatsApp led to a mob killing in India - The Washington Post>.

inclusion of this type of harm in clause 14 means that digital communications platform providers have a responsibility to be transparent about the way in which they handle that type of content, and that the ACMA has regulatory powers in relation to such content.

Content that might cause or contribute to this type of harm could include baseless claims that an election process is rigged, or false information about how, when and where to vote, both of which could deny Australians the right to make an informed choice about whether to participate in an election. Other content falling within this category might include false, misleading or deceptive information about electoral candidates or referendum proposals, which – if disseminated at scale – could have the effect of denying Australians the right to have a say in the conduct of public affairs based on informed choice.

Some of the digital content that would undermine the right of Australians to vote and be elected, and to participate in the conduct of public affairs, would also in certain circumstances give rise to an offence under existing Australian legislation. For example, it is an offence under the *Commonwealth Electoral Act 1918* to publish or distribute anything likely to mislead or deceive an elector in relation to the casting of a vote, during the election period,[15] and there is an equivalent offence in the *Referendum (Machinery Provisions) Act 1984* in relation to referendums.[16] However, in Australian legislation there is currently no obligation imposed on digital communications platform providers to themselves take steps in relation to the risk of this type of content being disseminated on their platforms.

The Australian Electoral Commission (AEC)'s disinformation register provides examples of disinformation that the AEC has previously identified in the lead up to elections that could affect the right to vote, to be elected and to participate in the conduct of public affairs. These examples include claims that voting software used by the AEC will result in rigged elections, and claims that the AEC is providing incorrect and illegal instructions regarding how to vote.[17]

So far, the spread of misinformation and disinformation has not significantly damaged the Australian electoral process, and thus has not undermined the right of Australians to vote, to be elected and to participate in the conduct of public affairs. However, experience from around the world suggests that misinformation and disinformation of this nature can influence public opinion and sway voter behaviour to such an extent that the outcome of an electoral process can no longer be said to represent the free will of the electorate.[18] The World Economic Forum's 2024 Global Risks Report warns that 'misinformation and disinformation may radically disrupt electoral processes in several economies over the next two years'.[19]

---

[15] *Commonwealth Electoral Act 1918* (Cth) s 329(1).
[16] *Referendum (Machinery Provisions) Act 1984* (Cth) s 122(1).
[17] See Australian Electoral Commission (AEC), 'Disinformation Register, 2022 Federal Election' (10 January 2023) <Disinformation register - Australian Electoral Commission (aec.gov.au)>.
[18] E.g., Michele Cantarella et al, 'Does Fake News Affect Voting Behaviour?' (2023) 52(1) *Research Policy* 104628; Fabian Zimmerman and Matthias Kohring, 'Mistrust, Disinforming News, and Vote Choice: A Panel Survey on the Origins and Consequences of Believing Disinformation in the 2017 German Parliamentary Election' (2020) 37(2) *Political Communication* 215; Irene Khan, *Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HRC/47/25 (13 April 2021) para 24.
[19] World Economic Forum (WEF), *The Global Risks Report 2024* (January 2024) <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf> 18.

Schedule 9 to the BSA seeks to address the risk that misinformation and disinformation will radically disrupt an electoral process in Australia, and in doing so, seeks to safeguard the right of all Australians to participate in the conduct of public affairs and to vote and be elected at genuine periodic elections.

The right to be protected against discrimination

International human rights law provides for the right to be protected against discrimination on various grounds, including race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth and 'other status'. This right is enshrined in numerous international human rights instruments. Article 2 of the ICCPR, for example, provides that States Parties shall ensure to individuals within their territory and subject to their jurisdiction, the rights recognised in the ICCPR 'without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status'. Article 26 of the ICCPR provides that the law shall 'guarantee to all persons equal and effective protection against discrimination'. The CERD provides that States Parties undertake to pursue a policy of eliminating racial discrimination in all its forms,[20] and the CEDAW provides similarly that States shall adopt 'appropriate legislative and other measures … prohibiting all discrimination against women'.[21]

The ICCPR does not define discrimination. The CERD, however, defines discrimination as:

> any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life.[22]

The Human Rights Committee has said that for the purposes of the ICCPR, discrimination should be understood to have a similar meaning to that provided in the CERD.[23] The CEDAW defines discrimination in similar terms to the CERD, the key aspects of both definitions being that individuals have the right to be protected against:

- any distinction, exclusion or restriction
- made on the basis of a protected ground
- with the effect or purpose of impairing or nullifying the enjoyment of their human rights and fundamental freedoms, on an equal footing with others.[24]

UN human rights bodies have taken the view that vilification can constitute discrimination, if it has the effect of nullifying or impairing the exercise by one person or group of their human rights and fundamental freedoms, on an equal footing with others. For example, in relation to a complaint made against Canada by a school teacher regarding his dismissal from a teaching position, the Human Rights Committee found that the teacher had discriminated against Jewish children by disseminating anti-Semitic beliefs. The Committee said that the dissemination of anti-Semitic material contributed to the creation of a 'poisoned environment'

[20] CERD (n 8) art 2(1).
[21] CEDAW (n 7) art 2(b).
[22] CERD (n 8) art 1(1).
[23] HRC, *General Comment No 18: Non-discrimination*, UN Doc HRI/GEN/1/Rev.1 (10 November 1989) para 7.
[24] CEDAW (n 7) art 1.

that interfered with the provision of education for Jewish children.[25] In a similar vein, in its observations on a report by Russia to the Human Rights Committee in 2009, the Committee expressed concern about 'the systematic discrimination against individuals on the basis of their sexual orientation …, including hate speech and manifestations of intolerance and prejudice'.[26] Again, the Human Rights Committee regarded hate speech as a form of discrimination. The Committee on the Elimination of Discrimination against Women has similarly taken the view that discrimination includes 'acts that inflict physical, mental or sexual harm or suffering, [and] threats of such acts' that affect women disproportionately and that impair or nullify the enjoyment by women of human rights and fundamental freedoms.[27]

Thus, the right to be protected against discrimination on various grounds, enshrined in various international human rights instruments, includes the right to be protected against vilification on those same grounds, if the vilification nullifies or impairs (or could be expected to nullify or impair) the exercise by the targeted person or group of their human rights and fundamental freedoms on an equal footing with others.

Pursuant to the regulatory regime set out in Schedule 9 to the BSA, the dissemination of content on a digital service will be considered misinformation or disinformation if, in addition to meeting other criteria specified in clauses 13 and 14, it is reasonably likely to cause or contribute to the vilification of a group in Australian society distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin, or vilification of an individual because of a belief that the individual is a member of such a group. The inclusion of vilification as a type of serious harm as defined in clause 14 means that digital communications platform providers have a responsibility to be transparent about how they will handle the dissemination of false, misleading or deceptive information that is likely to cause or contribute to the vilification of a person or group on one of the listed grounds, and that the ACMA has regulatory powers in relation to such content.

Experience internationally as well as in Australia attests to the way in which misinformation and disinformation can amplify racial, ethnic, religious or other identity-based vilification. A 2021 study by the European Parliament on disinformation about migrants and minority groups found that disinformation could contribute to a 'climate of hostility or a "sphere of hate"', which could 'reinforce prejudices and negative attitudes'.[28] That study reviewed content in the EUvsDisinfo database from 2018 and 2021, and found that 'a large number of articles report on migrants and/or Muslims as a threat to European culture and identity', or as a criminal threat or a threat to health.[29]

In a recent example, following a stabbing attack in northwest England in July 2024 which killed three young girls, a false (Muslim) name of an alleged suspect – said to be a recently arrived asylum seeker – was circulated on social media. The rumours prompted widespread

[25] HRC, *Views: Communication No 736/97*, UN Doc CCPR/C/780/D/736/1997 ('*Ross v Canada'*) para 11.5.
[26] HRC, *Concluding Observations of the Human Rights Committee: Russian Federation*, UN Doc CCPR/C/RUS/CO/6 (24 November 2009) para 27.
[27] Committee on the Elimination of Discrimination against Women, *General Recommendation No 19: Violence against Women* UN Doc A/47/38 (1992) 1; see also Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (Oxford University Press 2013) 764.
[28] Szakacs and Bognar (n 13) 23.
[29] Ibid 13.

violence targeting asylum seekers and Muslims, including attacks on mosques.[30] In earlier examples: in the context of the COVID-19 pandemic, content linking the Roma people to the spread of the virus led to stigmatisation and discrimination against the Roma in several European States;[31] and in 2015 a disinformation campaign created fake accounts purportedly owned by Muslim extremists, and posted messages about 'taking over Denmark' and killing and raping non-Muslim Danish people – thus stoking anti-Muslim sentiment.[32]

Disinformation can also amplify pre-existing harmful gender stereotypes, which can result in gender-based vilification. A 2021 US-based study found that gendered disinformation can 'make use of existing gender narratives, language, and ultimately discrimination to achieve certain social and political goals'; for example, by characterising female politicians as 'not being qualified for the position, lacking the requisite knowledge, intelligence, or experience for the role; or as persons who lie, are too emotional for the task, prone to aggression, or lacking sanity'.[33] The 2023 report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression stated similarly that 'gendered disinformation … uses highly emotive and value-laden content, tailored to local contexts, that undermines women's credibility and competence, stigmatizes them and isolates them', and that 'gender narratives have been invoked against women journalists, sexualising them and attacking their character, integrity, appearance and intelligence as a way of discrediting their reporting and discouraging them from continuing their work'. That report stated further that 'forms of harm emanating from gendered disinformation are varied and deeply consequential to both individuals and society at large', and that targeted individuals pay a 'heavy price psychologically, physically, socially and economically'.[34]

Australian research has similarly found a link between disinformation online and vilification based on race, ethnicity and other characteristics. Research by the Australian Human Rights Commission in 2021, for example, identified a 'correlation between negative media and political narratives about Muslims and Islam and an increase in aggression and violence towards Australian Muslims', and identified 'the perpetuation of stereotypes and the inclusion of misinformation about Muslim people and Islam … as particularly damaging aspects of these narratives'.[35]

In 2023, UN human rights experts recognised that the spread of hatred and hate speech against marginalised groups undermines their rights, and called upon 'social media companies

---

[30] Jill Lawless, 'Online misinformation fuelled tensions over the stabbing attack in Britain that killed 3 children' (*Associated Press*, 2 August 2024) <Misinformation fuels tension over UK stabbing attack that killed 3 children | AP News>; Al Jazeera, 'Agitators accused of Islamophobia for linking Southport attack to Muslims' (31 July 2024) <Agitators accused of Islamophobia for linking Southport attack to Muslims | Crime News | Al Jazeera>.
[31] Szakacs and Bognar (n 13) 15.
[32] Ibid 10.
[33] Dhanaraj Thakur and DeVan L Hankerson, *Facts and their Discontents: A Research Agenda for Online Disinformation, Race and Gender* (Centre for Democracy and Technology, 2021) <2021-02-10-CDT-Research-Report-on-Disinfo-Race-and-Gender-FINAL.pdf> 25; see also Nina Jankowicz et al, *Malign Creativity: How Gender, Sex and Lies are Weaponised against Women Online* (Wilson Centre, January 2021) <Report Malign Creativity How Gender, Sex, and Lies are Weaponized Against Women Online_0.pdf (wilsoncenter.org)>.
[34] Irene Khan, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (7 August 2023) UN Doc A/78/288, paras 45-46.
[35] Australian Human Rights Commission (AHRC), *Sharing the Stories of Australian Muslims* (2021) <ahrc_sharing_stories_australian_muslims_2021.pdf (humanrights.gov.au)> 11.

[to] urgently address posts and activities that advocate hatred and constitute incitement to discrimination, in line with international standards for freedom of expression'.[36]

Schedule 9 to the BSA seeks to reduce the risk of this type of content being disseminated online, and in this way assists to assure the right of all Australians to be protected against vilification (as an aspect of the right to be protected against discrimination) on the basis of the grounds listed in paragraph 14(c).

The right to the highest attainable standard of physical and mental health

Article 12 of the ICESCR provides that everyone has the right to the 'highest attainable standard of physical and mental health'. That Article provides that States Parties shall take steps necessary to achieve the full realisation of that right, including steps necessary for the 'prevention, treatment and control of epidemic, endemic, occupational and other diseases'. The reference to disease control includes 'the implementation or enhancement of immunization programs and other strategies of infectious disease control'.37

The UN Committee on Economic, Social and Cultural Rights has said that this obligation requires States to 'undertake actions that create, maintain and restore the health of the population'. This includes: 'fostering recognition of factors favouring positive health results', including through the 'provision of information'; 'the dissemination of appropriate information relating to healthy lifestyles and nutrition, harmful traditional practices and the availability of services'; and 'supporting people in making informed choices about their health'.38 The Committee has said that in order to fulfil this obligation, States are required to adopt appropriate legislative measures.39

Pursuant to the regulatory scheme set out in Schedule 9 to the BSA, the dissemination of content on a digital service is considered misinformation or disinformation if, in addition to meeting other criteria specified in clauses 13 and 14, it is reasonably likely to cause or contribute to harm to public health in Australia, including to the efficacy of preventative health measures in Australia (paragraph 14(b)). The reference here to public health is intended to include the government system for providing for the health needs and services of all Australians, including preventative health measures, on the understanding that, if this system and these measures are undermined, the health of Australians will consequentially be undermined. The inclusion of this type of harm in clause 14 means that digital communications platform providers have a responsibility to be transparent about the way in which they handle the dissemination of false, misleading or deceptive information that is reasonably likely to harm public health (or contribute to such harm), and that the ACMA has regulatory powers in relation to such content.

The potential for health-related misinformation and disinformation to undermine the right to the highest attainable standard of health has been firmly established since the COVID-19 pandemic. Misinformation and disinformation that might have this effect could relate to how a disease is spread, the safety and effectiveness of vaccines or other preventive health measures, or health treatment options not supported by clinical data. Many studies have found that misinformation and disinformation of this nature can undermine public trust in expert

[36] Catherine Namakula et al, *Freedom of Speech is not Freedom to Spread Racial Hatred on Social Media: UN Experts* (6 January 2023) <https://www.ohchr.org/en/statements/2023/01/freedom-speech-not-freedom-spread-racial-hatred-social-media-un-experts>.
[37] UN Committee on Economic, Social and Cultural Rights, *General Comment No 14: The Right to the Highest Attainable Standard of Health*, UN Doc E/C.12/2000/3 (11 August 2000) para 9.
[38] Ibid para 37.
[39] Ibid para 33.

guidance and government-led public health interventions, and consequently influence peoples' behaviour in a way that negatively impacts public health outcomes.[40]

In 2021, an Australian study found that one in five adults aged between 18–49 years agreed with some forms of misinformation about COVID-19 vaccines. [41] Misperceptions about COVID-19 vaccines were found to be associated with lower health literacy, less knowledge about vaccines, lower perceived personal risk of COVID-19, greater endorsement of non-COVID conspiracy beliefs, lower confidence in government, and lower trust in scientific institutions. Another study the following year found that 4 in 5 Australians had seen misinformation about COVID-19, and that those who believed misinformation had 'lower levels of trust in doctors, health officials and other authoritative sources'.[42]

Health-related misinformation and disinformation online is particularly pernicious. Research during the COVID-19 pandemic found that in the first 11 months of 2020, 5 health and lifestyle websites promoting false health information received 10 times more interactions on social media (comments, likes and shares) than the World Health Organisation and the Centre for Disease Control combined.[43] One study in the US found that it took only '5 to 10 minutes on an anti-vaccine site to increase perceptions of vaccination risks and decrease perceptions of the risks of vaccine omission'.[44]

Misinformation and disinformation also pose a risk to public health in contexts other than pandemics. One study of health information available online prior to 2019 found health misinformation on social media associated with: vaccines; diets and eating disorders; drugs and new tobacco products; pandemics and communicable diseases; noncommunicable diseases; and medical treatments and health interventions.[45] In 2022, a study of the most popular articles on social media in 2018–2019 about the four most common types of cancer found that one in three of the articles contained false, inaccurate or misleading information, and that most of that information was harmful – for example, by promoting unproven

---

[40] Israel Jnr Borges do Nascimento et al, 'Infodemics and Health Misinformation: A Systematic Review of Reviews' (2022) 100(9) *Bulletin of the World Health Organisation* 544; Muhammad Saiful Islam et al, 'COVID-19–Related Infodemic and its Impact on Public Health: A Global Social Media Analysis' (2020) 103(4) *The American Journal of Tropical Medicine and Hygiene* 1621; MA Gisondi et al, 'A Deadly Infodemic: Social Media and the Power of COVID-19 Misinformation' (2022) 24(2) *Journal of Medical Internet Research* 35552; K Pickles et al, 'COVID-19 Vaccine Misperceptions in a Community Sample of Adults Aged 18-49 Years in Australia' (2022) 19(11) *International Journal on Environmental Research and Public Health* 6883; V Suarez-Lledo and J Alvarez-Galvez, 'Prevalence of Health Misinformation on Social Media: Systematic Review' (2021) 23(1) *Journal of Medical Internet Research* 17187; World Health Organization (WHO), *Ebola Virus Disease – Democratic Republic of the Congo* (28 November 2019) <Ebola virus disease – Democratic Republic of the Congo (who.int)>; Ira Rubenstein and Tomer Kenneth, 'Taming Online Public Health Misinformation' (2023) 60 *Harvard Journal on Legislation* 219.

[41] Pickles et al (n 40).

[42] ACMA, *ACMA Misinformation Report: Fact Sheet 1: Key Research Findings* (2022) <https://www.acma.gov.au/sites/default/files/2022-03/ACMA misinformation report_Fact sheet 1 - key research findings.pdf> 1; Sora Park et al, *COVID-19: Australian News and Misinformation Longitudinal Study* (News and Media Research Centre, 2022) <https://apo.org.au/node/316582> 48.

[43] Cat Zakrzewski, 'The Technology 202: Facebook Removes Some Pages Appearing to Coordinate to Push Health Misinformation' (*The Washington Post*, 9 December 2020) <The Technology 202: Facebook removes some pages appearing to coordinate to push health misinformation - The Washington Post>.

[44] Elizabeth Benecke and Sarah Elizabeth De Young, 'Anti-Vaccine Decision-Making and Measles Resurgence in the United States' (2019) 6 *Global Pediatric Health* 1, 2; see also Rubenstein and Kenneth (n 40).

[45] Suarez-Lledo and Alvarez-Galvez (n 40).

treatments as alternatives to those that rigorous studies had found to be beneficial.[46] Other studies have suggested that companies have employed 'social bots' to promote falsified health information to promote their products (such as e-cigarettes).[47]

Schedule 9 to the BSA seeks to reduce the risk of this type of content being disseminated on digital communications platforms, and in this way, seeks to safeguard the right of all Australians to the highest attainable standard of physical and mental health.

Human rights potentially affected by the Bill

The right to privacy

Schedule 9 to the BSA engages Australia's obligations in relation to the right to privacy, enshrined in Article 17 of the ICCPR. Article 17 provides that no one shall be subjected to 'arbitrary or unlawful' interference with their privacy.

The requirement that interferences with privacy must not be 'unlawful' means that they must be provided by law. The Human Rights Committee has interpreted this to mean that 'relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted.'[48] The Committee has interpreted the term 'arbitrary' – in relation to the right to privacy – to mean that 'even interference provided for by law should be in accordance with the provisions, aims and objectives of the [ICCPR] and should be, in any event, reasonable in the particular circumstances'.[49]

The Human Rights Committee has not explicitly elaborated what types of restrictions on the right to privacy will be considered non-arbitrary for the purposes of the test stated above, other than that such restrictions should accord with the provisions, aims and objectives of the ICCPR and be reasonable in the circumstances. In relation to other ICCPR rights, however, the Committee has said that for restrictions not to be arbitrary, they must be imposed in pursuit of a legitimate objective, and must be 'necessary and proportionate' to the achievement of that objective.[50]

Thus, the right to privacy may be restricted to the extent that such restrictions are prescribed by law, reasonable, necessary, and proportionate to the achievement of a legitimate objective.

The UN High Commissioner for Human Rights has considered that any form of systematic monitoring and analysis of public online discourse is a form of surveillance, and thus, interferes with the right to privacy. This includes the collection and analysis of social media

[46] Skyler Johnson et al, 'Cancer Misinformation and Harmful Information on Facebook and Other Social Media: A Brief Report' (2022) 114(7) *Journal of the National Cancer Institute* 1036.
[47] Jon-Patrick Allem and Emilio Ferrara, 'Could Social Bots Pose a Threat to Public Health?' (2018) 108 *American Journal of Public Health* 1005.
[48] HRC, *General Comment No 16: Article 17 (Right to Privacy)*, contained in *Report of the Human Rights Committee*, Annex VI, UN Doc A/43/40 (8 April 1988) 181, para 8.
[49] Ibid para 4.
[50] HRC, *Views: Communication No 633/1995*, UN Doc CCPR/C/65/D/633/1995, Annex ('*Gauthier v Canada*') para 13.6 (interpreting the term 'arbitrary' in relation to the right to freedom of expression). The UN High Commissioner for Human Rights has affirmed the relevance of this test to an assessment of restrictions on the right to privacy: UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/51/17 (4 October 2022) para 48.

posts, even on publicly accessible communications platforms. This is because even though these posts may be in the public domain, 'individuals should have a space free from systematic observation and intrusion, particularly by government entities'.[51] The Bill's regulatory regime therefore burdens the right to privacy, to the extent that it imposes obligations on digital communications platform providers (and provides the ACMA with regulatory powers) that pertain to information disseminated on digital communications platforms.

Three aspects of the Bill, in particular, engage Australia's obligations in relation to the right to privacy:

The conferral of power on the ACMA to make digital platform rules requiring digital communications platform providers to make and retain records relating to misinformation and disinformation on their platforms (subclause 30(1) of Schedule 9). In exercising this power, the ACMA could require digital communications platform providers to make and retain records relating to misinformation or disinformation posted by individual end-users, or relating to complaints made by end-users about misinformation or disinformation. It is possible that in making such a rule, the ACMA could effectively require digital communications platform providers to make and retain records that include personal information.
The conferral of power on the ACMA to require digital communications platform providers and other persons to provide it with information or documents relating to misinformation or disinformation on a digital communications platform (clauses 33 and 34 of Schedule 9). Again, it is possible that this information could include personal information.

- More broadly, the ACMA's power to request, approve, or approve variations to, misinformation codes, and to determine or vary misinformation standards. It is possible that these codes or standards may include provisions relating to the use, storage or disclosure of the personal information of individual end-users by digital communications platform providers.

The ACMA's powers to require digital communications platform providers to make and retain records, and to gather information, are aimed at a legitimate objective. The immediate objective is to enable the ACMA to collect data regarding the spread of misinformation and disinformation, so as to enable it to assess the steps being taken by digital communications platform providers to manage the risk of misinformation and disinformation on their platforms. The ACMA's powers to require digital communications platform providers to make and retain records, and to gather information, are also aimed at enabling the ACMA to publish information about the prevalence and nature of misinformation and disinformation on digital communications platforms, and about the steps being taken by digital communications platform providers to prevent and respond to misinformation and disinformation. This in turn is aimed at empowering end-users to identify misinformation and disinformation on digital communications platforms.

Providing the ACMA with the ability to assess and raise awareness regarding the prevalence of misinformation and disinformation on digital communications platforms, and the efforts being taken by digital communications platform providers to manage the risk of misinformation and disinformation, is aimed ultimately at reducing the risk that false,

[51] UN High Commissioner for Human Rights (n 50) para 43.

misleading or deceptive information disseminated on digital communications platforms will cause or contribute to serious harm impacting Australians, of a type and threshold set out at clause 14 of Schedule 9.

The powers conferred on the ACMA by Schedule 9 to the BSA are necessary for the achievement of this objective. This is because much of the misinformation and disinformation on digital communications platforms is posted by individual end-users, and moreover, any complaints mechanisms relating to misinformation or disinformation will also be aimed at individual end-users. Thus, the ACMA would not be able to effectively regulate the risk of misinformation and disinformation on digital communications platforms if it were unable to require digital communications platform providers to collect and retain information regarding posts and complaints by individual end-users, and – where necessary to monitor the operations of a provider – collect such information itself.

Schedule 9 to the BSA provides important protections for the right to privacy. These protections ensure that the restrictions on the right to privacy are proportionate to the aim of enabling the ACMA to require digital communications platform providers to be transparent about, and manage the risk of misinformation and disinformation their platforms. Specifically:

- Subclause 30(2), regarding the ACMA's power to make rules requiring digital communications platform providers to make and retain records relating to misinformation and disinformation, provides that before making a digital platform rule for this purpose, the ACMA must consider the privacy of end-users and whether the rule is required for the performance of the ACMA's functions. Subclause 30(3) provides moreover that digital platform rules relating to records must not require digital communications platform providers to make or retain records of the content of private messages or Voice over Internet Protocol (VoIP) communications.

Subclause 33(3) provides that in exercising its powers to obtain information from digital communications platform providers, the ACMA must not require a person to provide information or documents that would reveal the content of a private message or VoIP communication.[52]

- Subclause 34(2) provides that in exercising its powers to obtain information from other persons, the ACMA must not require a person to provide information or documents relating to content posted by that person on a digital communications platform, other than in the person's capacity as a fact-checker, content moderator, an employee of the provider of the platform, or person providing services to the provider of the platform. Subclause 34(4) provides moreover that the ACMA cannot require a person to reveal the content of a private message or VoIP communication.
- Clauses 45 and 46 provide that the ACMA must not approve a code (or part of a code) or determine a standard that contains requirements related to, respectively, the content or encryption of private messages or VoIP communications.

These protections for personal information reflect the fact that the ACMA's regulatory powers are not designed to address the behaviour of individual end-users, but rather, the way in which digital communications platform providers manage the risk of misinformation and disinformation on their platforms. The protections described above ensure that to the extent that the ACMA's new regulatory powers restrict the right to privacy, such restrictions are reasonable, necessary and proportionate to the achievement of a legitimate objective.

[52] Except for a private message or VoIP communication relating to the internal operations of the platform sent by an employee of, or person providing services to, the provider: cl 33(3).

In addition to the protection for privacy provided in Schedule 9 to the BSA, the ACMA is also bound by the requirements in the *Privacy Act 1988* regarding the collection, use and disclosure of personal information.

The right to freedom of expression

The Bill engages Australia's obligations in relation to the right to freedom of expression, enshrined in Article 19 of the ICCPR. The right to freedom of expression includes 'freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media' of one's choice.

It extends to 'the expression and receipt of communications of every form of idea and opinion capable of transmission to others', subject to the provisions in Article 19(3) (permitting certain restrictions, as outlined below) and Article 20 (which requires States Parties to prohibit hate speech).[53] The Australian Attorney-General's Department has recognised that the right to freedom of expression extends to 'any medium, including written and oral communications, the media, public broadcast, broadcasting, artistic works and commercial advertising'.[54]

The Human Rights Committee has said that the right to freedom of expression enshrined in Article 19 of the ICCPR protects expression on any 'internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines'.[55] It includes the right to seek, receive and impart information that may be 'deeply offensive',[56] and the right to seek, receive and impart information irrespective of the truth or falsehood of the content (subject to the restrictions permitted by Articles 19(3) and 20 of the ICCPR).[57]

Schedule 9 to the BSA requires digital communications platform providers to be more transparent about the way in which they manage the risk of misinformation and disinformation on their platforms, and empowers the ACMA to require providers to take steps in relation to the risk. These measures could feasibly incentivise digital communications platform providers to take an overly cautious approach to the regulation of content that could be regarded as misinformation and disinformation – or in other words, they could have a 'chilling effect.' Thus, these measures could burden the freedom of expression.

Article 19(3) of the ICCPR provides that the right to freedom of expression may be subject to restrictions 'as are provided by law and are necessary: (a) for respect of the rights or reputations of others; [and] (b) for the protection of national security or of 'public order (*ordre public*), or of public health or morals'.

---

[53] HRC, *General Comment No 34: Article 19: Freedom of Expression*, UN Doc CCPR/C/GC/34 (12 September 2011) para 11.
[54] Australian Government Attorney-General's Department (AGD), *Right to Freedom of Opinion and Expression* (Public Sector Guidance Sheet) <Right to freedom of opinion and expression | Attorney-General's Department (ag.gov.au)>.
[55] HRC, *General Comment No 34* (n 53) paras 12, 43.
[56] Ibid para 11; HRC, *Ross v Canada* (n 25).
[57] *Handyside v United Kingdom* (European Court of Human Rights, Application No 5493/72, 7 December 1976) para 49.

Commentary on this provision has established that for a restriction on the freedom of expression to be permissible, it has to fulfil three conditions.

> It must be provided by law. This may be in formal legislation, or in an enactment of lower rank than a statute'.[58] Either way, it must be 'formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly', and it must be accessible to the public.[59]
> It must pursue a legitimate aim, namely, one of the aims listed in Article 19(3) of the ICCPR (respect for the rights or reputations of others, national security, public order, or public health or morals).
> It must be necessary for attaining that legitimate aim. This means that it should be the 'least intrusive instrument amongst those which might achieve their protective function', and 'proportionate to the interest to be protected'.[60]

To the extent that Schedule 9 to the BSA restricts the freedom of expression, the first limb of this test (requiring that restrictions be provided by law) is satisfied, because the measures set out in Schedule 9 are either prescribed in the Schedule itself, or will be prescribed in digital platform rules, approved misinformation codes or misinformation standards.

The restrictions on the freedom of expression also satisfy the second limb of the test, because they pursue a legitimate aim. Schedule 9 to the BSA defines misinformation and disinformation as the dissemination of false, misleading or deceptive content that, among other criteria, is reasonably likely to cause or contribute to one of the types of harm covered by clause 14. The measures set out in Schedule 9 that burden the freedom of expression are aimed specifically at addressing the risk posed by misinformation and disinformation; thus, they aim to reduce the risk that content disseminated on digital communications platforms will cause or contribute to one of the harms listed in clause 14. These harms align with the purposes for which, pursuant to Article 19(3) of the ICCPR, the freedom of expression may be restricted, as follows:

Clause 14: Type of harm	**Aligned purpose for which freedom of expression may be restricted, pursuant to Article 19(3)**
(a) Harm to the operation or integrity of a Commonwealth, State, Territory or local government electoral or referendum process	The rights of others. Specifically, the right to take part in the conduct of public affairs, and to vote and be elected at genuine periodic elections, enshrined in Article 25 of the ICCPR. See discussion above, pages 8 to 10.
(b) Harm to public health in Australia	Public health. See discussion above, pages 13 to 15.
(c) Vilification of a group in Australian society distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability,	The rights of others. Specifically, the right to be protected against discrimination, enshrined in numerous international human rights instruments. See discussion above, pages 10 to 13.

[58] Nicola Wenzel, 'International Protection of Freedom of Opinion and Expression', in Anne Peters and Rüdiger Wolfrum (eds), *Max Planck Encyclopedias of International Law* (Oxford University Press, 2014) para 30.
[59] HRC, *General Comment No 34* (n 53) para 25.
[60] Ibid paras 22-34. See also Wenzel (n 58); Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HRC/17/27 (16 May 2011).

nationality or national or ethnic origin, or vilification of an individual because of a belief that the individual is a member of such a group	
(d) Intentionally inflicted physical injury to an individual in Australia	The rights of others. Specifically, the right to security of the person, enshrined in Article 9 of the ICCPR. See discussion above, pages 7 to 8.
(e) Imminent damage to critical infrastructure or disruption of emergency services in Australia	Public order. The Human Rights Committee has not explicitly defined public order for the purposes of Article 19(3) of the ICCPR; however, in relation to a similar clause describing permissible restrictions on the right of peaceful assembly, the Committee has said that 'public order' refers to 'the sum of the rules that ensure the proper functioning of society, or the set of fundamental principles on which society is founded'.[61] The protection of critical infrastructure and emergency services are necessary to 'ensure the proper functioning of society'.
(f) Imminent harm to the Australian economy	Public order. See preceding comment. Protection against imminent harm to the Australian economy, such as the destabilisation of the banking system or financial markets, is necessary to 'ensure the proper functioning of society'.

The restrictions imposed by Schedule 9 to the BSA on the freedom of expression are necessary and proportionate to protect against the risk that the dissemination of false, misleading or deceptive information on digital communications platforms will cause or contribute to one of the above-listed harms. This is achieved in two ways. First, the measures provided for in Schedule 9 – including both the core transparency obligations on digital communications platform providers, and the ACMA's regulatory powers – are focused on systems and processes, rather than the regulation of actual content. This is ensured by clause 67 of Schedule 9, which provides that nothing in Part 2 of Schedule 9, or in a rule, approved code or standard made, approved or determined pursuant thereto, can require a digital communications platform provider to remove content from a platform or prevent an end-user from using the platform, except in the case of disinformation that involves inauthentic behaviour.[62] And second, proportionality is achieved through a series of important protections, provided throughout Schedule 9 to the BSA, for the freedom of expression. These protections assist to ensure that the measures will not have a 'chilling effect' on the freedom of expression online, or on the way in which digital communications platform providers manage content on their platforms. These protections are as follows:

[61] HRC, *General Comment No 37 on Article 21 (Right of Peaceful Assembly)*, UN Doc CCPR/C/GC/37 (17 September 2020) para 44. See also UN Economic and Social Council (ECOSOC), *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1985/4, Annex (1995) para 22; AGD (n 54).

[62] Dissemination of content involving inauthentic behaviour is defined in clause 15 of Schedule 9 as dissemination that – among other criteria – uses an automated system in a way that is reasonably likely to mislead an end-user about: the identity, purpose or origin of the person disseminating the content; the popularity of the content on the digital service; the motive or intention of an end-user; or the source or origin of the content.

- Clause 16 provides exemptions for: the dissemination of content that would reasonably be regarded as parody or satire; the dissemination of professional news content; and the reasonable dissemination of content for any academic, artistic, scientific or religious purpose.
- Subclauses 33(3), 34(4) and 30(3), and clauses 45 and 46, provide that the ACMA must not exercise its information-gathering powers, powers to require digital communications platform providers to make and retain records, or powers to approve a code or determine a standard, in relation to private messages or VoIP communications.
  Subclause 34(2) provides that in exercising its information-gathering powers, the ACMA must not require a person to provide information or documents relating to content posted by that person on a digital communications platform, other than in the person's capacity as a fact-checker, a content moderator, an employee of the provider of the platform, or a person providing services to the provider of the platform.
- In exercising its power to approve, or approve variations of, misinformation codes or determine or vary misinformation standards, the ACMA must be satisfied that: the code or standard is reasonably appropriate and adapted to achieving the purpose of providing adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on the platforms; and goes no further than reasonably necessary to provide that protection (subparagraphs 47(1)(d)(iii) and (iv), subparagraphs 50(1)(d)(iii) and (iv), clause 54, and subclause 60(2)).

Notwithstanding these precautions, it is nevertheless important that the impact of Schedule 9 to the BSA on the freedom of expression be assessed, so as to ensure that the measures provided for – not only as prescribed in Schedule 9 itself, but also in their implementation – are necessary and proportionate to the achievement of the legitimate aims identified. For this reason, clause 70 provides that as soon as possible after the third anniversary of the commencement of Schedule 9, and every three years thereafter, the operation of Part 2 of Schedule 9 will be reviewed, with such review to include an assessment of the impact on freedom of expression and whether Part 2 of Schedule 9 should be amended.

Conclusion

The Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*. To the extent that it engages the rights to privacy and freedom of expression in Articles 17 and 19(2) of the ICCPR, any limitation on those rights is reasonable, necessary and proportionate to the objective of protecting Australia and Australians from serious harm caused or contributed to by the dissemination of false, misleading or deceptive information on digital communications platforms.

NOTES ON CLAUSES

Abbreviations used in Notes on Clauses

Term	Meaning
ACMA	Australian Communications and Media Authority
ACMA Act	*Australian Communications and Media Authority Act 2005*
Acts Interpretation Act	*Acts Interpretation Act 1901*
ART	Administrative Review Tribunal
Bill	Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024
BSA	*Broadcasting Services Act 1992*
Competition and Consumer Act	*Competition and Consumer Act 2010*
Criminal Code	*Criminal Code Act 1995*
Human Rights (Parliamentary Scrutiny) Act	*Human Rights (Parliamentary Scrutiny) Act 2011*
Legislation Act	*Legislation Act 2003*
Online Safety Act	*Online Safety Act 2021*
Privacy Act	*Privacy Act 1988*
Telecommunications Act	*Telecommunications Act 1997*

Clause 1—Short Title

Clause 1 provides that the Bill, when enacted, may be cited as the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Act 2024.*

The title reflects that the primary objective of the Bill is to establish a new framework to safeguard against serious harms caused by misinformation or disinformation.

Clause 2—Commencement

Clause 2 provides for the commencement of each provision of the Bill, when enacted, as set out in the table in subclause 2(1).

Sections 1 to 3, and anything in the Act not elsewhere covered by the table set out in subclause 2(1), commence on the day the Act receives the Royal Assent. Schedule 1, and Part 1 of Schedule 2, to the Act commence on the day after the Act receives the Royal Assent. Part 2 of Schedule 2 to the Act commences immediately after either the commencement of Part 1 of Schedule 2 to the Act, or the commencement of the *Administrative Review Tribunal Act 2024*, whichever is later.

Subclause 2(2) is a standard provision for commencement clauses. It allows for the dates of commencement of provisions to be inserted into the table in subclause 2(1) in any published version of the Act. The subclause also provides that any such information inserted into the table is not a part of the Act.

Clause 3—Schedules

Clause 3 provides that, following enactment of the Bill and on the commencement of the relevant items in each Schedule to the Bill, legislation that is specified in the Schedules is amended or repealed as set out in those items, and any other item in the Schedules has effect according to its terms. This is a standard provision which removes any doubt that the Schedules to the Act have effect as indicated in those Schedules.

There are two Schedules to the Bill. Schedule 1 to the Bill contains the main amendments to the BSA. Schedule 2 sets out the consequential and transitional provisions, amending the ACMA Act, the BSA, the Online Safety Act and the Telecommunications Act.

SCHEDULE 1—MAIN AMENDMENTS

Broadcasting Services Act 1992

Item 1—After section 216E

Item 1 inserts a new section 216F into the BSA. This section provides that Schedule 9 to the BSA, as added by item 2, has effect.

Item 2—At the end of the Act

Item 2 adds a new Schedule 9 to the BSA, relating to digital communications platforms.

SCHEDULE 9—DIGITAL COMMUNICATIONS PLATFORMS

The title of Schedule 9 reflects that it relates to digital communications platforms.

The new Schedule 9 contains provisions in relation to misinformation and disinformation, which enable the ACMA to:

- obtain information and documents relating to misinformation and disinformation from digital communications platform providers
- make rules requiring digital communications platform providers to make and retain records relating to misinformation and disinformation, and to prepare reports consisting of information contained in those records
- approve and register enforceable misinformation codes developed by sections of the digital platforms industry, setting out the measures those sections of the industry will take to reduce the risk of misinformation and disinformation
- in certain circumstances – for example, if misinformation codes do not adequately protect the Australian community from misinformation and disinformation, determine misinformation standards for sections of the digital platforms industry
- make rules requiring digital communications platform providers to implement and maintain a process for handling complaints and resolving disputes about misinformation and disinformation
- publish information relating to misinformation and disinformation.

Schedule 9 also places core obligations on digital communications platform providers in relation to misinformation and disinformation. These core obligations are to:

- assess risks relating to misinformation and disinformation on their platforms, and publish a report of the outcomes of that assessment
- publish their policy or policy approach in relation to misinformation and disinformation
- publish a media literacy plan setting out the measures the provider will take to enable end-users of their platforms to better identify misinformation and disinformation.

The ACMA will be able to enforce compliance with approved industry codes, industry standards, digital platform rules and obligations in Schedule 9 on digital communications platform providers, including obligations to provide information to the ACMA. Enforcement mechanisms include civil penalties, remedial directions, infringement notices and formal warnings, depending on the particular provision.

The purpose of these new powers is to promote transparency and hold digital communications platform providers to account for the effectiveness of actions taken by them to counter the spread of misinformation and disinformation on their services.

PART 1—INTRODUCTION

Part 1 of Schedule 9 provides for introductory matters.

DIVISION 1—PRELIMINARY

Division 1 of Part 1 of Schedule 9 provides for preliminary matters. It includes a simplified outline of the Schedule and definitions of terms used throughout it, and explains the extraterritorial operation of the Schedule.

Clause 1—Simplified outline of this Schedule

Clause 1 provides a simplified outline of Schedule 9 to broadly explain its purpose and scope.

Clause 2—Definitions

Clause 2 defines terms used in Schedule 9. Many of these terms have definitions which are self-explanatory, but where they are not, they are explained further below:

access has the same definition in Schedule 9 as when it is used in Schedules 7 and 8 to the BSA. To avoid doubt and to avoid the term being given an unduly narrow meaning, access includes access subject to a pre-condition (such as use of a password) by way of push technology, or by way of a standing request (for example, where a customer requests a digital communications platform provider to provide them with material on a regular basis, such as through a subscription to a podcast with interactive features).

Australia has been included in clause 2 to clarify that when used in a geographical sense, it includes all the external Territories.

connective media service (see subclause 5(2)).

content means any content whether in the form of: text; data; speech, music or other sounds; visual images (animated or otherwise); any other form; or any combination of forms.

This is the same definition given to the term in Schedules 7 and 8 to the BSA.

content aggregation service (see subclause 5(3)).

digital communications platform (see subclause 5(1)).

digital communications platform provider (see subclause 7(1)).

digital platform rules (see subclause 82(1)).

digital service (see clause 4).

disinformation (see subclause 13(2)).

dissemination is to have its ordinary meaning. To avoid doubt and to avoid the term being given an unduly narrow meaning, paragraphs (a) and (b) provide that dissemination includes using automated means and dissemination to one person or more than one person.

In paragraph (a) automated refers to a process (or processes) which can function with little to no human action. This is intended to capture circumstances such as where a person has programmed an artificial intelligence bot to automatically produce, post and disseminate content containing misinformation and/or disinformation, or content that is wholly generated and disseminated through artificial intelligence without direct instruction from a person. Dissemination is still taken to have occurred even if it is a bot (and not a person) that is actively producing and posting that content.

Paragraph (b) is included so that the act of dissemination is not limited by the number of people who receive the misinformation and/or disinformation.

excluded dissemination (see subclause 16(1)).

inauthentic behaviour (see clause 15).

interactive feature (see clause 6).

internet carriage service has the same meaning as in the Online Safety Act.

internet search engine service (see subclause 5(4)).

media literacy plan means a plan setting out the measures a digital communications platform provider will take to enable end-users of the platform to better identify misinformation and disinformation on the platform, including to enable end-users to identify the provenance of content disseminated on the platform (particularly content that purports to be authoritative or factual). This is the plan that digital communications platform providers are required to make available to the public, pursuant to paragraph 17(1)(c). Pursuant to clause 22, the ACMA may make digital platform rules relating to media literacy plans

The term 'media literacy' is used in Schedule 9 in a narrower sense, as compared to the way in which the term is used in some other contexts. For the purposes of Schedule 9, as encapsulated in the definition of 'media literacy plan', it refers to the ability of end-users to identify misinformation and disinformation on digital communications platforms, including the ability to identify the source of content, particularly content that purports to be authoritative or factual. This contrasts with, for example, the broader definition used by the Australian Media Literacy Alliance, which refers to media literacy as 'the ability to critically engage with media in all aspects of life'.[63] It also contrasts with the term 'media information literacy', as used by the European Commission's High-Level Group on Fake News and Online Disinformation, defined as 'the capacity to exert critical thinking as to the productions, representations, languages (visuals, texts, sounds), audiences and communities characteristic of mainstream and social media'.[64] This narrow use of the term 'media literacy' for the purposes of Schedule 9 reflects the limited scope of the term in the Schedule.

media sharing service (see subclause 5(5)).

misinformation (see subclause 13(1)).

misinformation code means a code developed under Division 4 of Part 2.

misinformation complaint means a complaint regarding misinformation or disinformation (or potential misinformation or disinformation) on a digital communications platform or content removed from a digital communications platform on the basis that its dissemination using the platform is misinformation or disinformation on the platform.

misinformation standard means a standard determined under Division 4 of Part 2.

news content (see subclause 16(3)).

participant (see clause 43).

post is explained by reference to posted – content is ***posted*** on a digital service by an end-user if the end-user causes the content to be accessible to, or delivered to, one or more other end-users using the digital service.

private message means a message sent using a digital communications platform from an end-user to another end-user; or at the same time to a number of end-users that does not exceed the number specified in the digital platform rules or, if no number is specified in the digital platform rules, 1,000.

For the purposes of Schedule 9, a message could be in any digital format. It could be in the form of an instant message, or something else, so long as only the selected recipients are able to view the content.

---

[63] Australian Media Literacy Alliance et al, 'A Media Literacy Framework for Australia' (2020) <https://medialiteracy.org.au/media-literacy-framework/>.

[64] Directorate-General for Communication Networks, Content and Technology, European Commission, *A Multi-Dimensional Approach to Disinformation: Report of the independent High Level Group on Fake News and Online Disinformation* (European Union, 2018) <A multi-dimensional approach to disinformation - Publications Office of the EU (europa.eu)> 25.

A message will be considered private only if it has been sent to another end-user, or a number of end-users that does not exceed 1,000 or another number specified in the digital platform rules. End-users do not 'receive' a message for the purposes of this definition unless the sender has directed that the message be sent to them. In other words, content that would be accessible by all end-users of the platform (for example, public posts) would not be considered a private message.

The number 1,000 has been chosen as a conservative threshold that exceeds any scientifically accepted limits on the number of meaningful relationships humans can maintain at a time. Although this is an ongoing area of study in psychology, the most cited number, known as Dunbar's Number, is 150. Dunbar observes that groups with more than 150 members start to become unstable and can fragment.[65]

Therefore, when a person sends a message to over 1,000 recipients (or other number specified in the digital platform rules), even on a so-called 'private' social media page or instant message group for example, it can be reasonably assumed that there is a significant potential for the content to be re-disseminated without the explicit consent of the original creator of the message. These messages cannot reasonably be considered private and are not intended to be captured as private messages for the purposes of Schedule 9.

Allowing the maximum number of end-users to whom a private message may be sent to be specified in the digital platform rules, as opposed to in Schedule 9, allows the determination of this number to be informed by information made available to the ACMA pursuant to the operation of other provisions in Schedule 9. It would be expected, for example, that the determination of the maximum number of recipients that may receive a private message – with the result that such messages would not be subject to record keeping and reporting obligations (clause 30), the ACMA's information gathering powers (clauses 33 and 34) or misinformation codes or standards – may be informed by information on misinformation complaints, made available by digital communications platform providers pursuant to any digital platform rules made under paragraph 25(2)(c) and any additional information regarding misinformation and disinformation on digital communications platforms obtained by the ACMA pursuant to clauses 33 and 34.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that the rules would be subject to parliamentary scrutiny and potential disallowance and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

professional news content (see subclause 16(2)).

protected information means: (a) a trade secret; or (b) other information that has a commercial value that would be, or could reasonably be expected to be, destroyed if the information were publicly disclosed.

[65] RIM Dunbar, 'Neocortex Size as a Constraint on Group Size in Primates' (1992) 22(6) *Journal of Human Evolution* 469.

This definition of protected information is broadly similar to that contained in subsection 145(3) of the *Public Health (Tobacco and Other Products) Act 2023* and section 47 of the *Freedom of Information Act 1982*, and other provisions in Australian legislation directed to preventing the disclosure of particular kinds of commercially valuable information.[66]

In *Searle Australia Pty Ltd v Public Interest Advocacy Centre*, the Full Court of the Federal Court of Australia considered the meaning of 'trade secret' and 'other information having a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if the information were disclosed', for the purposes of the *Freedom of Information Act 1982*. The Court considered that in order for information to constitute a trade secret, the information must be: secret (noting that information 'may lose its secret character as time passes'); used or useable in the trade; and advantageous for trade rivals to obtain. Regarding the meaning of 'commercial value', the Court said that 'there would ordinarily be material before the decision-maker which would show whether or not the commercial value of the information would be or could be expected to be destroyed or diminished if the information were disclosed.'[67]

The intention is that this understanding should inform the understanding of the clause 2 definition of 'protected information'.

Such information could include, for example, information of a technical nature ('know-how'), or business information, such as client lists and marketing plans. It would also generally include source code.

This definition of protected information is *not* expected to capture information obtained by the ACMA from a digital communications platform provider, regarding that provider's performance in preventing and responding to misinformation and disinformation, merely on the basis that if disclosed, that information would cause the provider reputational damage (and consequently, financial loss). It would not include information of a general nature in order to determine the spread of misinformation or disinformation on the platform. Thus, information such as the number of misinformation complaints received by a provider, or the time taken by the provider to respond to those complaints, or a provider's failure to take steps to minimise the spread of misinformation and disinformation on its platform, would not generally be 'protected information' – unless the value of *that information* would be destroyed (or be expected to be destroyed) if publicly disclosed.

provided on a digital service (see clause 8).

provided to the public (see clause 9).

section of the digital platform industry (see clause 42).

serious harm (see clause 14).

service includes a website.

using (see clause 10).

[66] See also the similar wording in s 185(1) of the *Gene Technology Act 2000* and the definition of 'confidential commercial information' in s 4(1) of the *Food Standards Australia New Zealand Act 1991*.
[67] *Searle Australia Pty Ltd v Public Interest Advocacy Centre* (1992) 36 FCR 111, 120-21.

VoIP communication means a communication by voice over internet protocol. This covers any real time audio communication carried via the internet. It does not cover any saved recordings of audio content (including recordings that are only available for a limited amount of time).

Common examples of VoIP communication include call services that allow for phone calls using the internet or real time voice communication between players in an online video game.

Clause 3—Extra-territorial operation

Clause 3 extends the operation of Schedule 9 to acts, omissions, matters and things outside Australia.

As Schedule 9 is intended to apply to digital communications platform providers domiciled both within and outside Australia, the purpose of this clause is to ensure that regulatory provisions will not be interpreted so as to be applied only to acts, omissions, matters and things done or situated within Australia. This provision displaces the common law presumption that statutes do not apply extraterritorially.

This provision is to be read together with other provisions in Schedule 9 which establish the requisite connection between Australia and the subject matter that Schedule 9 seeks to regulate. Specifically:

- clause 4 defines a 'digital service' as a service that, among other things, is 'offered in Australia'
- clause 13 defines misinformation and disinformation as the dissemination of content containing information that is reasonably verifiable as false, misleading or deceptive and, among other things, is provided to one or more end-users in Australia
- clause 14 defines 'serious harm' as one of six types of harm in Australia, which have either significant and far-reaching consequences for the Australian community or a segment thereof, or severe consequences for an individual in Australia
- clauses 54 and 60 provide that the ACMA may only determine or vary a misinformation standard if it is satisfied that it is reasonably appropriate and adapted to, and goes no further than reasonably necessary to, provide adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on the digital communications platforms in question.

The combined effect of these provisions is that while clause 3 extends the operation of Schedule 9 to acts, omissions, matters and things outside Australia (and thus, seeks to regulate the conduct of foreign digital communications platform providers outside Australia), the Bill's regulatory scheme applies specifically and exclusively to content that is provided to end-users in Australia, on digital services offered in Australia, that would be reasonably likely to cause or contribute to serious harm in Australia.

DIVISION 2—KEY CONCEPTS

Division 2 introduces key concepts used in the Schedule. These concepts define the services, and set out the uses of them, that are to be covered by obligations contained in subsequent provisions of Schedule 9.

Clause 4—Digital service

Clause 4 defines a ***digital service*** for the purposes of Schedule 9. A service delivered by, or accessible by means of, an internet carriage service is a digital service if it satisfies all the criteria listed in paragraphs 4(a) to (d) and does not satisfy either of the criteria in paragraphs 4(e) and (f). The criteria in paragraphs 4(a) to (d) capture almost all services that are currently offered in Australia via the internet.

Paragraph 4(d) provides that the digital service must be 'offered in' Australia. A digital service is 'offered in' Australia if the provider of that service, or a person acting on behalf of the provider, makes it available to end-users in Australia. A service may be considered offered in Australia even if the content is delivered from outside Australia. A service does not need to be exclusively offered to end-users in Australia to be considered offered in Australia.

Generally, a digital service would be considered offered in Australia if the service is accessible by an end-user with an Australian IP address. However, there may be circumstances in which a service might be accessible via an Australian IP address, but is nevertheless inaccessible to end-users in Australia. This would be the case, for example, if a service could not be accessed without an end-user account, and such an account could not be created without a phone number of a country other than Australia. In such a scenario, the service would not be considered 'offered in' Australia. In this scenario, the provider has taken steps to make the service *inaccessible* in Australia.

A digital service would not be considered 'offered in' Australia if the service provider blocked end-users with Australian IP addresses from accessing the service (geo-blocking). In this scenario, the provider has again taken steps to make the service inaccessible in Australia. However, if a service provider were to block end-users with Australian IP addresses from accessing the service, but also instruct end-users regarding how to circumvent that restriction (for example by accessing the content via virtual private network (VPN)), the service *would* be considered 'offered in' Australia.

To avoid doubt, paragraphs 4(e) and (f) exclude services from being a digital service to the extent they are a 'broadcasting service' or a 'datacasting service'. These terms are defined in section 6 of the BSA.[68]

The reason why Schedule 9 focuses on digital services rather than broadcasting and datacasting services is because broadcasting and datacasting services are already subject to an extensive regulatory framework under the BSA. This framework makes use of measures such as licence conditions, standards and codes of practice relating to the content which may be transmitted. Moreover, broadcasting and datacasting services generally are not provided by means of an internet carriage service. These factors greatly reduce the likelihood, volume and speed of misinformation and disinformation potentially being disseminated on those services.

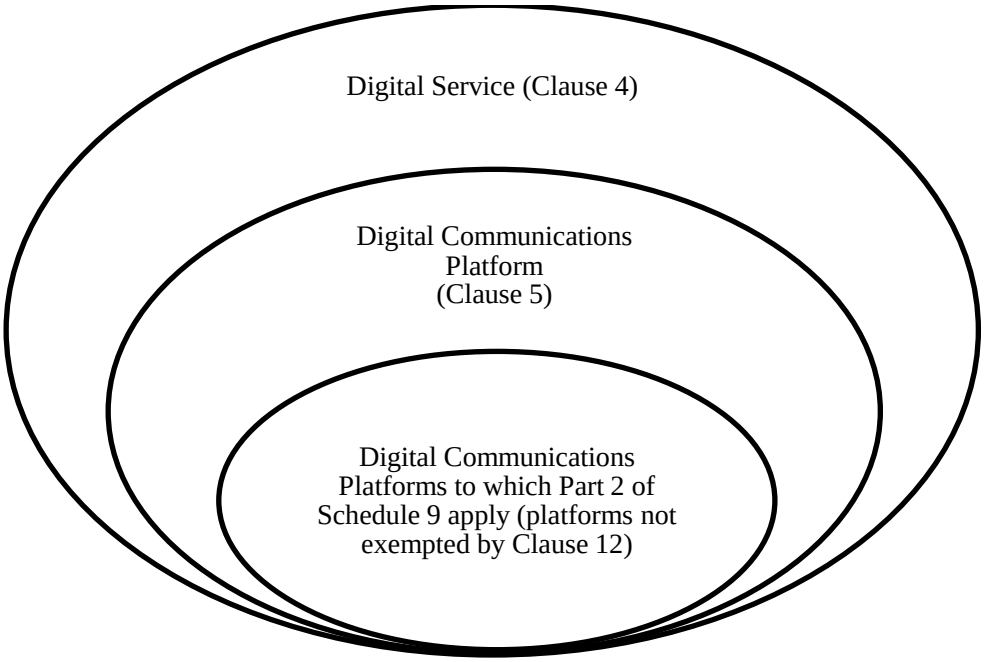
On the other hand, digital services are not currently subject to a regulatory framework which has the ability to reduce the potential dissemination of misinformation and disinformation. For instance, a person seeking to use a digital service to disseminate content is not subject to the licensing regime which applies to the various categories of 'broadcasting' service

[68] See also the *Broadcasting Services ("Broadcasting Service" Definition — Exclusion) Determination 2022*.

regulated under the BSA. Also, while the Online Safety Act provides for some regulation of harmful online content, it does not seek to regulate the dissemination of misinformation and disinformation.

Figure 1 illustrates the different digital service and platform categories in Schedule 9, including the types of services within scope of the ACMA's misinformation and disinformation powers.

Figure 1: Digital communications platforms defined in the Bill



Further information on the definition of digital communications platform and exemptions for certain digital communications platforms is provided in the explanation for clauses 5 and 12 respectively.

Clause 5—Digital communications platform

Clause 5 defines ***digital communications platform*** for the purposes of Schedule 9.

Paragraphs 5(1)(a) to (e) list types of digital communications platforms. These are:

- a connective media service (see subclause 5(2)); or
- a content aggregation service (see subclause 5(3)); or
- an internet search engine service (see subclause 5(4)); or
- a media sharing service (see subclause 5(5)); or
- a kind of digital service determined by the Minister under subclause 5(7).

Whether a digital service is a digital communications platform generally will depend on whether the primary function of the digital service is as described in paragraph 5(2)(a), 5(3)(a), 5(4)(b) or 5(5)(a), disregarding functions listed in subclause 5(6).

The primary function of a digital service should be determined by considering the experience of end-users of the service, rather than how its functions might be characterised by the service provider or through characterisation of how the digital service operates in a technical sense.

It is possible for a digital service to have additional functions alongside the primary function. However, only the primary function would be used to assess which section (if any) of the digital communications platform industry any given digital service should belong to.

If a digital service's primary function is not described in subclauses 5(2) to (5) then (subject to any determination by the Minister under subclause 5(7)) the digital service is not a digital communications platform.

A digital service will also not be a digital communications platform to the extent to which it is:

- an internet carriage service (paragraph 5(1)(f))
- an SMS service (that is, a short message service) (paragraph 5(1)(g)), or
- an MMS service (that is, a multimedia message service) (paragraph 5(1)(h)).

The exclusion at paragraph 5(1)(f) indicates a distinction Schedule 9 draws between a service which is itself an internet carriage service and a service that is provided by means of an internet carriage service (as described in either paragraph (a) or (b) of the definition of digital service in clause 4).

The exclusions of SMS and MMS services should be read in a technical sense and are included to avoid doubt. These services are already excluded from being a digital service under Schedule 9, as they do not use the internet. They have been expressly excluded here, as their functionality can appear similar to instant messaging.

The conditions that must be satisfied in order for a digital service to be considered a connective media service, content aggregation service, internet search engine service or media sharing service are set out in subclauses 5(2), 5(3), 5(4) and 5(5), respectively. Each of these subclauses states that additional conditions – that must also be met in order for a digital service to be considered a digital communications platform of the type described – may be set out in the digital platform rules.

Allowing additional conditions to be set out in digital platform rules, rather than having the conditions pertaining to the listed types of digital communications platforms exhaustively and definitively set out in subclauses 5(2), 5(3), 5(4) and 5(5) allows flexibility for the definitions of those platforms to be adapted as necessary to keep pace with evolving technologies. It also enables the ACMA to adapt the definitions of these types of digital communications platforms if necessary in response to information made available to the ACMA pursuant to the operation of other provisions in Schedule 9 – for example, based on information on misinformation complaints, made available by digital communications platform providers pursuant to digital platform rules made under clause 25, and additional information regarding misinformation and disinformation on digital communications platforms obtained by the ACMA pursuant to clauses 33 and 34.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on the ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that the rules would be subject to parliamentary

disallowance and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

Connective media service

Subclause 5(2) defines a ***connective media service*** as a digital service that satisfies all of the criteria in paragraphs 5(2)(a) to (d).

Paragraph 5(2)(a) requires that the digital service have the primary function of enabling online interaction between two or more end-users. This is intended to emphasise that the primary function must be about enabling online interactions with a social element. Examples of digital services that are intended to be captured by the definition of connective media service include social media, instant messaging services and web-forums. Collaborative platforms that allow online group work and social communications would also be captured, as their *primary function* is to enable online interaction between two or more end-users. However, it is not intended that platforms such as ridesharing applications and eCommerce marketplaces be covered given that the primary function of these services is not for the purpose of enabling online interaction, but rather for other purposes such as transport or commercial transactions.

The criterion in paragraph 5(2)(c) requires the digital service to have an ***interactive feature*** as defined in clause 6.

The ACMA would have the ability to narrow the definition of 'connective media service' through specifying conditions in digital platform rules (paragraph 5(2)(d)).

Whilst the range of digital communications platforms potentially captured under the definition of connective media service in clause 5 is broad, the application of Part 2 (misinformation and disinformation) of Schedule 9 to particular categories of connective media service can be limited through the Minister exercising powers under clause 12 (see further explanation for clause 12). As the features and nature of digital communications platforms are constantly evolving, including through generative artificial intelligence, it is necessary to have the flexibility, through instrument, to carve in and out types of digital communications platforms from the scope of Part 2.

Similarly, the ACMA is able to make digital platform rules, approve codes and determine standards to target particular high-risk digital communications platforms only (see explanation for clause 30 as one example), in order for the operative parts of Schedule 9 to only regulate a narrower group of connective media services.

It would also be open to the ACMA to exempt digital communications platforms from the operation of Subdivisions A to D of Division 2 of Part 2 (Transparency) by rules made under clause 29. If it did so, other provisions in Schedule 9 (such as the Information Gathering powers in Division 3 of Part 2) would remain unaffected and would continue to apply to the connective media service in question.

Content aggregation service

Subclause 5(3) defines a ***content aggregation service*** as a digital service that satisfies all of the criteria in paragraphs 5(3)(a) to (c): the primary function of the digital service is to collate and present to end-users content from a range of online sources including sources other than the digital service; the service is not an internet search engine service, which is a separate category of digital communications platform (see subclause 5(4)); and the service satisfies any conditions that are set out in the digital platform rules.

For example, digital services such as news aggregators would satisfy the criterion in paragraph 5(3)(a) as their primary function is to collate information from across the internet (which could include some content produced by the service itself), and present it to end-users.

Internet search engine service

Subclause 5(4) defines an ***internet search engine service*** as a service that satisfies the criteria in paragraphs 5(4)(a) and (b) (the service collects, indexes or ranks content from a range of online sources, including sources other than the digital service; and the primary function of the digital service is to enable an end-user to search the digital service's collection, index or ranking), plus any conditions set out in the digital platform rules (paragraph 5(4)(c)).

Digital services known as search engines would satisfy the criteria in paragraphs 5(4)(a) and (b).

A digital service known as a search engine that uses artificial intelligence technology in any of its processes would still be considered to be an internet search engine service so long as the primary function was still to enable an end-user to search the digital service's collection, index or ranking.

Media sharing service

Subclause 5(5) defines a ***media sharing service*** as a digital service that satisfies the criterion in paragraph (a) plus any other conditions set out in the digital platform rules (paragraph (b)).

Paragraph 5(5)(a) outlines that the primary function of the service is to provide audio, visual (animated or otherwise) or audio-visual content to end-users. For example, digital services with the primary function being to provide podcasts, or provide platforms for the publication of videos, or video content on demand services would satisfy paragraph 5(5)(a).

Services that allow end-users to publish audio, visual or audio-visual content for social purposes may also be captured in the connective media service category.

However, a media sharing service will not be subject to Part 2 (Misinformation and disinformation) of Schedule 9, including approved misinformation codes or misinformation standards, if it does not have an interactive feature (see paragraph 12(1)(b)). The reason for the requirement that the media sharing service have an interactive feature is because an interactive feature is the mechanism by which misinformation and disinformation can be spread, including at scale, and therefore is the focus of regulation under Schedule 9. For the purposes of Part 2 therefore, this definition is not intended to include podcasts that do not

have an interactive feature, or platforms such as broadcast video on demand or subscription video on demand television.

The ACMA would also have the ability to narrow the definition of 'media sharing service' through specifying conditions in digital platform rules (paragraph 5(b)).

It is intended that the application of Part 2 (misinformation and disinformation) of Schedule 9 can also be limited by the Minister through the operation of other paragraphs and subclauses in clause 12 (see further explanation for clause 12).

Similarly, the ACMA would be able to make digital platform rules, approve codes and determine standards that target particular classes of high-risk digital communications platforms only (see explanation for clause 30 as one example). The ACMA can also target the application of Division 2 of Part 2 of Schedule 9 (the Transparency provisions) to apply to certain digital communications platform providers only, through digital platform rules under clause 29. For example, ACMA could make a rule exempting low-risk digital communications platforms from Division 2 of Part 2. If it did so, other provisions of Schedule 9 (such as the Information Gathering powers in Division 3 of Part 2) would continue to apply in relation to the media sharing service in question.

Functions to disregard

Subclause 5(6) provides that in determining the primary functions of a digital service for the purposes of paragraphs 5(2)(a), 5(3)(a), 5(4)(b) or 5(5)(a), any of the functions in paragraphs 5(6)(a) to (d) should be disregarded. The intent of expressly disregarding these functions is to reiterate that the primary function of a digital service should be determined by considering the experience of end-users on the service, rather than, for example, what the service provider claims the service's functions to be.

Digital services determined by the Minister

Subclause 5(7) allows the Minister to determine that a kind of digital service is a digital communications platform if the Minister is satisfied that it is appropriate to apply provisions of Schedule 9 to the digital service in order to provide adequate protection for the Australian community. Such a determination would be a legislative instrument for the purposes of the Legislation Act.

Subclause 5(7) is intended to allow the Minister to determine, by legislative instrument, that Schedule 9 applies to a new type of digital communications platform which may come into existence in the future. It may also allow high-risk industry sections to quickly fall within scope of the powers in Schedule 9 where there may be ambiguity about whether or not the service is covered by the kinds of services listed in paragraphs 5(1)(a) to (d) but where the functions of the service present a misinformation and/or disinformation risk to Australians.

An example of a new kind of digital service that could be determined to be a digital communications platform is a generative artificial intelligence service. At the time of the drafting of the Bill and this Explanatory Memorandum, the scope and nature of generative artificial intelligence services is still evolving, and it is unclear if there will be a future need to determine generative artificial intelligence services as a distinct kind of digital communications platform for the purposes of Schedule 9 to the BSA. Currently, generative

artificial intelligence is starting to be incorporated into existing digital services. However, should the technology evolve in a manner requiring a distinct definition, the Minister would be empowered to make a determination under subclause 5(7).

Subclause 5(8) requires the Minister to consult with the ACMA before making an instrument under subclause 5(7).

Clause 6—Interactive feature

Clause 6 defines an ***interactive feature*** for the purposes of Schedule 9.

This definition is relevant to the definition of 'connective media service', as a digital service that does not have an interactive feature will not be considered to be a connective media service (paragraph 5(2)(c)). It is also relevant to the definition of 'media sharing services', as a media sharing service will also not be subject to the rules in Divisions 2 to 5 of Part 2 of Schedule 9, or in approved misinformation codes or misinformation standards, if it does not have an interactive feature (see clause 12).

A digital service has an interactive feature if any one or more of the functions listed in paragraphs 6(a) to (c) applies to the digital service.

Paragraph 6(a) provides that an ***interactive feature*** includes features that allow an end-user to post content on the digital service, with the exception of interaction as part of gameplay. See also the definition of ***post*** in clause 2.

Paragraph 6(b) provides that an ***interactive feature*** includes features that allow an end-user to share, within the digital service (other than as part of gameplay), content that is provided on that digital service with another end-user.

This is intended to capture features which enable an end-user who is not the originator of content on a given platform to "share" that content on the same platform with others (other than as part of gameplay).

It is not intended to capture situations where an end-user, on their own volition, chooses to use a *third-party* platform to share or promote content.

For example, if platform provider A publishes content on its platform, and an end-user of platform A decides on his or her own volition to use *platform B* to share a link to the content on platform A, this activity will not result in platform A having an ***interactive feature*** for the purposes of the Bill. Whether this activity occurs is wholly outside platform provider A's control.

Subparagraph 6(c)(i) provides that an ***interactive feature*** is a feature which makes interaction between end-users observable to other end-users, other than as part of gameplay.

This is intended to capture features which enable the *content* of the interactions between two or more end-users to be viewed by third parties. For example, a live-stream where third parties can observe.

Subparagraph 6(c)(ii) provides that an ***interactive feature*** is a feature which makes interaction by end-users with content provided on the digital service observable to other end-users, other than as part of gameplay.

This is intended to capture features which enable a third party to observe another end-user's access to, or changes to, content that is made available on the service. For example, this would cover features which enable third parties to observe whether and how another end-user has accessed media files on a media file sharing service.

Paragraphs 6(a), (b) and (c) apply other than when the relevant activity takes place 'as part of gameplay'.

It is intended that this limitation extends only to 'in game' activities – i.e. activities that take place within the game environment, rather than ancillary chat or similar functions that may be accessed while gaming is taking place or before or after gaming activity.

Clause 7—Digital communications platform provider

Clause 7 sets out the definition of ***digital communications platform provider*** as a person who provides a digital communications platform (see clause 5).

Subclauses 7(2) and (3) provide that a person does not provide a digital communications platform merely because the person supplies an internet carriage service that enables content to be delivered or accessed, or merely because the person provides a billing service, or a fee collection service, in relation to a digital communications platform. This is to clarify that a digital communications platform provider is intended to be the person that controls the content accessible to end-users on a digital communications platform.

Clause 8—When content is provided on a digital service

Subclause 8(1) provides that content is ***provided on*** a digital service if the content is delivered by the digital service, or accessible to end-users using the digital service. Subclause 8(2) provides that content is also provided on a digital service if the content is delivered to the end-user by the digital service, or accessible to the end-user using the digital service.

This definition is relevant to the definition of interactive feature in clause 6. A digital service will have an interactive feature if the digital service provides a means for end-users to share, using the digital service (and other than as part of gameplay), content that is *provided on* the digital service with another end-user. It will also have an interactive feature if the digital service makes interaction by end-users with content *provided on* the digital service observable to other end-users (other than as part of gameplay).

The definition is also relevant to the definition of digital service, which requires the service to be provided to the public (paragraph 4(c)). Subclause 9(2) provides that, for the purposes of Schedule 9, a service that is provided to the public is taken to be different from a service that is not provided to the public, even if the content *provided on* the services is identical.

Additionally, it is also relevant to the definitions of misinformation and disinformation in clause 13, which require content to be *provided on* a digital service to one or more end-users in Australia in order to be in scope of those definitions.

References to content being 'delivered by' the service and 'accessible to' the end-user are intended to cover both a situation where the service may actively deliver content to the end-user (for example, through push-technology), and where the service may not deliver content to any particular end-user, but merely make it available on a service in a form which allows end-users to access it should they wish.

Clause 9—When a service is provided to the public etc.

Clause 9 outlines when a service is ***provided to the public*** for the purposes of Schedule 9.

Subclause 9(1) provides that a service is provided to the public if, and only if, the service is provided to at least one person outside the 'immediate circle' (within the meaning of the Telecommunications Act) of the person who provides the service.

This definition is relevant to the definitions of digital service and digital communications platform. A service will not be a digital service or a digital communications platform covered by Schedule 9 to the BSA if it is not provided to the public (see paragraph 4(c)).

Subclause 9(2) provides that a service that is provided to the public is taken to be different from a service that is not provided to the public, even if the content provided on the services is identical. This subclause has been included because, while some services may have both private and public versions, the intention of this legislation is to only cover services to the extent they are provided to the public.

Clause 10—Extended meaning of *using*

Clause 10 provides that a reference in Schedule 9 to ***using*** a thing is a reference to using the thing either in isolation, or in conjunction with one or more other things. A similar definition is used in section 24 of the Telecommunications Act.

This is intended to overcome potential difficulties in attributing instrumentality to a single element of a system, where the whole system is required to perform an act.

PART 2—MISINFORMATION AND DISINFORMATION

Part 2 of Schedule 9 places new obligations on digital communications platform providers and gives new powers to the ACMA in relation to transparency (Division 2), record keeping, reporting, information gathering and publication of information on the ACMA's website (Division 3), and misinformation codes and misinformation standards (Division 4). Division 1 of Part 2 defines the key concepts of misinformation, disinformation and serious harm.

Part 2 creates obligations on digital communications platform providers designed to enhance transparency and assist Australians to identify misinformation and disinformation on digital communications platforms. It also provides powers for the ACMA to make digital platform rules requiring digital communications platform providers to make and retain records relating to misinformation or disinformation, and/or in relation to measures implemented by digital communications platform providers to prevent or respond to misinformation or disinformation on digital communications platforms, including the effectiveness of the measures.

Part 2 also empowers the ACMA to gather information from digital communications platform providers and relevant other persons. It provides powers for the ACMA to approve a misinformation code or determine a misinformation standard, if necessary, in order to provide adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on digital communications platforms.

DIVISION 1—INTRODUCTION

Clause 11—Objects

Clause 11 sets out the objects of Part 2 of Schedule 9 to the BSA. These are specific objectives for the purposes of Part 2 of Schedule 9, which complement the objectives to be added to the overall objects of the BSA (see paragraphs 3(1)(hc) to (he), inserted by Item 5 of Schedule 2 to the Bill).

Paragraph (a)

Paragraph 11(a) explains the object of enabling end-users to better understand the accuracy and credibility of content disseminated using digital communications platforms, particularly content that purports to be factual or authoritative. This object is about empowering end-users to better assess the reliability of the content on digital communications platforms and to respond appropriately to content they identify as misinformation or disinformation.

The following provisions in Part 2 of Schedule 9 promote this object:

- the requirement on digital communications platform providers to publish a media literacy plan for the platform (paragraph 17(1)(c))
- the ability for the ACMA to make digital platform rules in relation to media literacy plans (clause 22).

Paragraph (b)

Paragraph 11(b) explains that an object of Part 2 of Schedule 9 is to ensure digital communications platform providers:

- publish policies, or information on policy approaches, in relation to misinformation and disinformation on digital communications platforms; and
- take other steps to enhance transparency in relation to misinformation and disinformation on digital communications platforms.

This object is promoted by:

- clause 17, which requires digital communications platform providers to publish:
  - a report on the outcomes of an assessment by the provider of risks relating to misinformation and disinformation on their platform (paragraph 17(1)(a));
  - either their current policy or their current policy approach in relation to misinformation and disinformation on their platform (paragraph 17(1)(b));
  - a current media literacy plan for the platform (paragraph 17(1)(c)); and
  - information (other than source code) specified in the digital platform rules (paragraph 17(1)(d))
- clause 25, which allows digital platform rules to require publication, or provision to the ACMA, of information regarding misinformation complaints and dispute handling

clause 30, which allows digital platform rules to require digital communications platform providers to provide reports to the ACMA on misinformation and disinformation on their platforms, and/or measures they have implemented to prevent and respond to misinformation or disinformation
clause 33, which enables the ACMA to require digital communications platform providers to provide information and documents relevant to misinformation or disinformation on their platforms

- clause 38, which enables the ACMA to publish on its website certain information about misinformation and disinformation including statements of reasons for why a provider has not published certain information obtained under paragraph 17(4)(b) and information that ACMA has gathered from digital communications platform providers under clauses 30 and 33.

Paragraph (c)

The object at paragraph 11(c) is to enable sections of the digital platform industry to develop codes that require participants in those sections of the digital platform industry to implement measures to prevent or respond to misinformation and disinformation on digital communications platforms. This object is promoted through Subdivision C (misinformation codes) of Division 4 of Part 2 of Schedule 9.

Paragraph (d)

The object at paragraph 11(d) is to enable the ACMA to approve codes and determine standards that are reasonably appropriate and adapted to protecting the Australian community from serious harm caused or contributed to by misinformation or disinformation on digital communications platforms.

This object makes it clear that one of the purposes of Part 2 of Schedule 9 is the prevention or minimisation of serious harm, and to provide for measures that are reasonably appropriate and adapted to that purpose. The ACMA's substantive powers throughout Part 2 have been designed to promote this object. For example, before approving or varying a misinformation code under clause 47 or 50, or determining or varying a standard under Subdivision D of Division 4, the ACMA must be satisfied that the code, standard or variation is reasonably appropriate and adapted to achieving the purpose of providing adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation (subparagraphs 47(1)(d)(iii) and 50(1)(d)(iii) and paragraphs 54(a) and 60(2)(a)) and that it goes no further than reasonably necessary to provide that protection (subparagraphs 47(1)(d)(iv) and 50(1)(d)(iv) and paragraphs 54(b) and 60(2)(b)). Similarly, when making standards under Subdivision D of Division 4, the ACMA must be satisfied that the standard is necessary in order to provide adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation (see paragraphs 55(1)(c), 56(1)(e), 57(1)(d), 58(1)(e) and 59(1)(a)).

Paragraph (e)

Paragraph 11(e) provides that one of the objects of Part 2 of Schedule 9 is to provide the ACMA with powers, which respect the freedom of expression, to take action for the purposes of Part 2.

The right to freedom of expression in international human rights law includes the 'freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of [one's] choice.'[69] The right to privacy protects the right not to be subjected to 'arbitrary or unlawful' interference with one's privacy.[70] This means that any interferences with the right to privacy must be provided by law, and that they should be 'in accordance with the provisions, aims and objectives of the [ICCPR] and should be, in any event, reasonable in the particular circumstances'.[71]

International human rights law allows the right to freedom of expression and the right to privacy to be restricted, so long as the restrictions are prescribed by law, reasonable, necessary, and proportionate to the achievement of a legitimate objective.72 In the case of restrictions to the freedom of expression, the 'legitimate objective' must be to protect: the rights or reputations of others; national security; public order; or public health or morals.73

Various provisions throughout this Part have been drafted to reflect when any restrictions on the right to freedom of expression and the right to privacy may be permissible under international human rights law. Most importantly, clause 14 ensures that the types of serious harm – that the dissemination of false, misleading or deceptive content must be reasonably likely to contribute to or cause, to be considered misinformation or disinformation – align with the purposes for which the right to freedom of expression may be restricted, under international human rights law. The Human Rights Committee has not explicitly prescribed 'legitimate purposes' in relation to restrictions on the right to privacy, but it is likely that purposes recognised as legitimate reasons for restricting the freedom of expression would also be recognised as legitimate reasons for restricting the right to privacy. In other words, to the extent that measures in this Part impinge upon the right to freedom of expression or the right to privacy, the purpose of that impingement is to reduce the risk of the types of harm identified in clause 14.

This object at paragraph 11(e) is promoted by the checks and balances that have been incorporated into the ACMA's powers in Part 2 to ensure that any restriction on freedom of expression is necessary and proportionate to the objective of preventing serious harm of the kinds described in clause 14. The provisions that promote the object in paragraph 11(d) also promote the object in paragraph 11(e). Namely:

- subparagraphs 47(1)(d)(iii) and (iv) and 50(1)(d)(iii) and (iv) require that before approving or varying a code, the ACMA must be satisfied that it is reasonably appropriate and adapted to achieving the purpose of providing adequate protection for the Australian community from serious harm caused or contributed to by

[69] ICCPR (n 6) art 19.
[70] Ibid art 17.
[71] HRC, *General Comment No 16* (n 48) paras 4, 8.
[72] In relation to the freedom of expression: HRC, *General Comment No 34* (n 53) para 22. The Human Rights Committee has not explicitly elaborated what types of restrictions on the right to privacy will be considered non-arbitrary, for the purposes of the test set out in Article 17 of the ICCPR (which protects the right to privacy), other than that such restrictions should accord with the provisions, aims and objectives of the ICCPR and be reasonable in the circumstances. However, where the ICCPR provides that rights must not be 'arbitrarily' restricted, this has generally been interpreted to mean that restrictions must be in pursuit of a legitimate objective, and 'necessary and proportionate' to the achievement of that objective: see, e.g., *Gauthier v Canada* (n 50) para 13.6. The UN High Commissioner for Human Rights has affirmed the relevance of this test to an assessment of restrictions on the right to privacy: UN High Commissioner for Human Rights (n 50) para 48.
[73] ICCPR (n 6) art 19.

misinformation or disinformation on the platforms, and goes no further than reasonably necessary to provide that protection
- clauses 54 and 60, together with paragraph 55(1)(c), 56(1)(e), 57(1)(d), 58(1)(e) and 59(1)(a) require the ACMA to be satisfied of these same matters when determining or varying a standard.

Additionally, Part 2 of Schedule 9 provides various other safeguards to ensure that to the extent that actions taken pursuant to the Part may burden the freedom of expression and the right to privacy, those actions are necessary and proportionate to the need to address the risk of the harms listed in clause 14. These safeguards are:

- paragraph 17(3)(b), which provides that the obligation of digital communications platform providers to publish information does not apply to personal information
- subclause 30(2), which provides that before making a digital platform rule for the purposes of clause 30, the ACMA must consider the privacy of end-users and whether the rule is required for the performance of the ACMA's functions
- subclauses 30(3), 33(3), and 34(4), and clauses 45 and 46 – which relate to the ACMA's powers to require digital communications platform providers to make and retain records, its information gathering powers, and its powers to approve a code or determine a standard – have limitations in relation to private messages and VoIP communications[74]
  subclause 34(2), which provides that in exercising its powers to obtain information from persons, the ACMA must not require a person to provide information or documents relating to content posted by that person on a digital communications platform, other than in the person's capacity as a fact-checker, content moderator, or employee of, or person providing services to, the provider of the digital communications platform
- subclause 67(1), which provides that nothing in Part 2 of Schedule 9, a digital platform rule made for the purposes of Part 2, or an approved misinformation code or misinformation standard, can require the removal of content from a digital communications platform, or the banning of an account, except in the case of disinformation that involves inauthentic behaviour[75].

Paragraph (f)

The object at paragraph 11(f) is designed to emphasise the purpose of Part 2 of Schedule 9 operating at the systemic level. The object reflects the intention that the ACMA examine systemic issues relating to the conduct of digital communications platform providers in relation to misinformation and disinformation on digital communications platforms. For example, under Subdivision A of Division 3 of Part 2, the ACMA may make digital platform rules requiring digital communications platform providers to make and retain records, and provide reports, relating to measures implemented by digital communications platform providers to prevent or respond to misinformation or disinformation on digital

[74] In the case of the ACMA's power to gather information from digital communications platform providers under clause 33, these limitations do not apply to private messages or VoIP communications relating to the internal operations of the platform sent by an employee of, or person providing services to, the provider: subclause 33(3).
[75] Dissemination of content involving inauthentic behaviour is defined in clause 15 as dissemination that – among other criteria – uses an automated system in a way that is reasonably likely to mislead an end-user about: the identity, purpose or origin of the person disseminating the content; the popularity of the content on the digital service; the motive or intention of an end-user; or the source or origin of the content.

communications platforms, including the effectiveness of the measures. For the avoidance of doubt, this object can be read as a limitation on the ACMA taking specific action against individual end-users for the content they post online.

Clause 12—Exemption for certain digital communications platforms

Clause 12 exempts certain digital communications platforms from the substantive requirements of Part 2 of Schedule 9, from digital platform rules made for the purposes of that Part, and from approved misinformation codes and misinformation standards. Those provisions and instruments would not apply in relation to a digital communications platform to the extent that it is one of the following: an email service, a media sharing service that does not have an interactive feature, or a digital service the Minister determines is an excluded service for misinformation purposes under subclause 12(3).

Email services (paragraphs 12(1)(a) and (2)(a)) have been excluded as email is a protocol enabling communications between servers and is not a platform that has a single provider as such. Although some large email services do exist (such as Gmail) these services are not the sole providers of email, and individuals can host their own private email servers should they wish.

Media sharing services that do not have an interactive feature (paragraphs 12(1)(b) and (2)(b)) are excluded, as the intention is to only capture those services that facilitate the spread of information from end-users to *other* end-users (and therefore potentially enable dissemination of misinformation and disinformation at scale). Media sharing services not intended to be captured by the regulatory scope of Schedule 9 include broadcast video on demand services, subscription video on demand services or podcasts without interactive features.

Paragraphs 12(1)(c) and (2)(c), and subclause 12(3), provide the Minister with the power to determine, by legislative instrument, digital services to be excluded services for misinformation purposes. Subclause 12(3) states that the Minister may, by legislative instrument, determine that a digital service is an excluded service for misinformation purposes.

The purpose of these provisions is to enable the Minister to carve out low-risk digital communication platforms or classes of platforms (through subsection 33(3A) of the Acts Interpretation Act) from all of the operative parts of Schedule 9. As at the time of writing, such platforms could, for example, include ***connective media services*** that enable collaborative work and social connection, which would otherwise meet the definition, but would not (currently) be high-risk services for the spread of misinformation and disinformation. Given the nature and features of digital communications platforms are constantly and rapidly evolving, including through new generative artificial intelligence technology, it is necessary to have flexibility for the Minister to carve out (and back in if necessary through subsection 33(3A) of the Acts Interpretation Act), digital communications platforms, through disallowable instruments. The determination power is intended to avoid imposing an unnecessary regulatory burden on low-risk digital services inadvertently captured by the definitions. The determination power is also necessary given the fast-changing nature of technology. New technologies could be created that technically meet the definitions but that are not intended to be captured. (This could include, for example, in a scenario where obligations in Schedule 9 to the BSA may conflict with obligations placed on new or

emerging models of artificial intelligence by other legislation in future to combat misinformation and disinformation.)

Clause 13—Meanings of *misinformation* and *disinformation*

Clause 13 defines ***misinformation*** and ***disinformation*** for the purposes of Schedule 9.

Subclause 13(1) provides that dissemination of content using a digital service is ***misinformation*** on the digital service if it meets all four of the following elements:

- the content contains information that is reasonably verifiable as false, misleading or deceptive. 'Information' is intended to include opinions, claims, commentary and invective
- the content is provided on the digital service to one or more end-users in Australia
- the provision of the content on the digital service is reasonably likely to cause or contribute to serious harm (see subclause 13(3) and clause 14), and
- the dissemination is not excluded dissemination (see clause 16).

This definition is relevant to a broad number of provisions of Schedule 9 to the BSA which either:

- define the duties of regulated entities (for example, the duty under subparagraph 17(1)(b)(ii) for digital communications platform providers to provide information on the provider's 'current policy approach in relation to misinformation and disinformation on the platform'), or
- define the powers of the ACMA to make instruments by reference to which legal duties may be imposed on regulated entities, for example, the power of the ACMA conferred by clause 47 to approve a code containing measures to prevent or respond to misinformation or disinformation on the platforms (see subparagraph 47(1)(d)(i)).

In practical terms, digital communications platform providers will need to identify misinformation or disinformation themselves, including identifying content on their digital communications platforms that contains information that is reasonably verifiable as false, misleading or deceptive, pursuant to such duties or relevant instruments.

Some matters that could be considered when determining if content is reasonably verifiable as false, misleading or deceptive include:

- whether the information has been fact-checked by a third-party organisation
- expert opinions or advice, for example public health experts could provide advice supported by scientific evidence
- verifying claims against multiple reliable and independent sources
- if previous complaints have been made about identical or similar material and this material has been assessed as false, misleading or deceptive
- if the material or similar material has previously been considered and assessed in the context of a platform provider's risk assessment plan for a platform.

Subclause 13(2) provides that dissemination of content using a digital service is ***disinformation*** on the digital service if it meets the same four elements as misinformation and one further element (paragraph 13(2)(e)). For the dissemination of content to be covered by paragraph (e) of the definition of disinformation, there needs to be grounds to suspect that the person disseminating, or causing the dissemination of, the content intends to deceive another

person (subparagraph 13(2)(e)(i)), or there needs to be dissemination involving inauthentic behaviour (see subparagraph 13(2)(e)(ii)).

For there to be 'grounds to suspect', there would need to be sufficient objective facts, evidence or circumstances that would induce a reasonable person to form a real and genuine *suspicion* that the person intends to deceive another person. Those objective facts, evidence or circumstances do not need to rise to the level which would induce a reasonable person to *know or positively believe* that the person intends to deceive another.

Such grounds for suspecting an intention to deceive another person (subparagraph 13(2)(e)(i)) could arise, for example, where complaints have previously been made to the provider on content that has been disseminated by the disseminator, the platform has verified that it is false, and the disseminator continues to share the same or similar content despite warnings from the platform.

Some other examples of 'grounds to suspect' may involve:

- content that is a doctored image, and is explicitly presented as unaltered by the disseminator; or
- false content that uses logos of trusted sources such as national public broadcasters or other professional news services, where the source or disseminator of that content has been verified by the platform as not the broadcaster or news service.

A note is included to explain that disinformation includes disinformation by or on behalf of a foreign power. The purpose of this note is to confirm that disinformation campaigns, whether initiated by foreign powers or by an individual domestic actor with mal-intent, are intended to be captured under this definition.

Subclauses 13(1) and (2) apply in relation to any content disseminated using a digital service, regardless of whether it is disseminated before or after the commencement of the Bill (see subitem 34(1) of Schedule 2 to the Bill).

For dissemination to be misinformation or disinformation, the content provided on a digital service (or considered in combination with content provided on other digital services) must be reasonably likely to cause or contribute to serious harm (see subclause 13(3) and clause 14).

Subclause 13(3) provides a list of matters to consider for the purpose of determining whether content disseminated on a digital service is reasonably likely to cause or contribute to serious harm. This subclause reflects the fact that the likelihood that content on a digital communications platform will cause or contribute to serious harm necessarily depends on the context of the dissemination. As indicated by the inclusion of paragraph 13(3)(i) (requiring that 'any other relevant matter' be considered), the matters listed are not exhaustive. This flexibility is important, because it is possible that future evolutions in technology (and evolutions in the use of such technology) could transform the way in which the provision of verifiably false, misleading or deceptive content on a digital service could cause or contribute to serious harm. Thus, it is not possible to definitively and exhaustively list all matters that may be relevant to this determination.

The factors listed at subclause 13(3) will be particularly important for the purpose of determining whether the dissemination of content on a digital communications platform satisfies the severity threshold for serious harm articulated in paragraphs 14(g) and 14(h).

Some examples of the way in which these factors may assist in determining whether false, misleading or deceptive content disseminated on a digital communications platform can be considered reasonably likely to cause or contribute to serious harm are provided in the explanation to clause 14 (meaning of serious harm).

Subclause 13(4) provides that the Minister may, by legislative instrument, determine a further matter to which regard must be had in determining whether the provision of content on a digital service is reasonably likely to cause or contribute to serious harm as defined in clause 14. While paragraph 13(3)(i) provides that regard should be had to 'any other relevant matter', it is possible that in light of evolutions in technology, the Minister may determine that there is another factor that is so significant that it should be explicitly prescribed as a matter to be considered, for the purpose of determining whether the dissemination of content on a digital service is reasonably likely to cause or contribute to serious harm.

Subclause 13(5) provides that subclause 13(2) does not limit subclause 13(1). This is provided to avoid any question that the definition of *disinformation* by implication limits the scope of the definition of *misinformation*. This is intended to forestall any argument that the two concepts are mutually exclusive: for example, that any conclusion that content was *misinformation* required a positive finding that there was *no* intention to deceive.

Clause 14—Meaning of serious harm

Clause 14 sets out the kinds of ***serious harm*** that content disseminated on a digital communications platform must be reasonably likely to cause or contribute to, in order for that content to be considered misinformation or disinformation for the purposes of Schedule 9. Dissemination of content will not be considered misinformation or disinformation – and thus, will not be within scope of Schedule 9 – unless it is reasonably likely to cause or contribute to serious harm as defined by this clause. The effect of this is that the entire regulatory scheme provided for by Schedule 9 is aimed at addressing the risk of these kinds of harm.

Paragraphs 14(a) to (f) set out 6 discrete categories of harm, which reflect the most serious consequences that the spread of misinformation and disinformation can have for the Australian community. These categories of harm align with the strictly limited purposes for which, pursuant to international human rights law, restrictions may be placed on the freedom of expression.[76] Paragraphs 14(g) and 14(h) describe the required severity of the harm. The combined effect of these provisions is that in order to be considered serious harm for the purposes of Schedule 9, the dissemination of content on a digital service must be one of the types of harm set out in paragraphs 14(a) to (f), and must be of a severity described in paragraph 14(g) and/or 14(h).

Paragraph (a): Harm to an electoral or referendum process

Paragraph 14(a) covers harm to the operation or integrity of a Commonwealth, State, Territory or local government electoral or referendum process. The inclusion of this type of harm is aimed at protecting the right of Australian citizens to take part in the conduct of public affairs, and to vote and be elected in elections that guarantee the free will of the

[76] Art 19(a) of the ICCPR (n 6) provides that the right to freedom of expression may be subject to such restrictions as are provided by law and are necessary: (a) for respect for the rights of others, and (b) for the protection of national security or of public order (ordre public) or of public health or morals.

electors.[77] The mass spread of misinformation and disinformation can undermine the right of Australians to vote for electoral candidates, or for or against a proposal submitted to referendum, or to support or oppose any government, based on informed choice.

Content that might cause or contribute to this type of harm could include false information about how, when and where to vote in an Australian election or referendum, which could effectively prevent Australians from exercising their right to vote; or false, misleading or deceptive information about electoral candidates or referendum proposals, which could have the effect of denying Australians the right to have a say in the conduct of public affairs based on informed choice.

The Australian Electoral Commission (AEC)'s disinformation register provides examples of disinformation that the AEC has previously identified in the lead up to elections. These include: claims that voting machines will be rigged to favour one of the major political parties; claims that voting software used by the AEC will result in rigged elections; and claims that the AEC is providing incorrect and illegal instructions regarding how to vote.[78]

So far, the spread of misinformation and disinformation has not significantly damaged the Australian electoral process. However, experience from around the world suggests that content of this nature, if disseminated at scale, can influence public opinion and sway voter behaviour to such an extent that the outcome of an electoral process can no longer be said to represent the free will of the electorate.[79] For example, a study on the impact of 'disinforming news' in the lead up to the federal election in Germany in 2017 found that 'because of its disruptive, right-leaning nature', this type of content 'apparently alienated voters from the main governing party' and 'drove them into the arms' of the right-wing populist party AfD. That study concluded that 'disinformation beliefs were apparently one of the reasons for electoral success of the right-wing populists'.[80] A study of the general election in Italy in 2018 found similarly that exposure to 'fake news' had a 'significant and positive effect' on populist voting, and 'effectively succeeded in nudging voters towards more populist electoral picks'[81]

The World Economic Forum's 2024 Global Risks Report warns that 'misinformation and disinformation may radically disrupt electoral processes in several economies over the next two years'.[82] That report notes that to combat the growing risk, 'governments are beginning to roll out new and evolving regulations to target both hosts and creators of online

[77] Art 25 of the ICCPR (ibid) provides that 'every citizen shall have the right and the opportunity, … (a) to take part in the conduct of public affairs, directly or through freely chosen representatives; (b) to vote and be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free will of the electors'. For discussion of the content of that right see HRC, *General Comment No 25: Article 25 (Participation in Public Affairs and the Right to Vote)*, UN Doc CCPC/C/21/Rev.1/Add.7 (1996).
[78] See AEC (n 17).
[79] E.g., Cantarella et al (n 18); Zimmerman and Kohring (n 18); Khan, *Disinformation and Freedom of Opinion and Expression* (n 18) para 24; Craig and Gainous, 'To Vote or Not to Vote? Fake News, Voter Fraud, and Support for Postponing the 2020 US Presidential Election' (2024) 52(1) *Politics and Policy* 33; Hunt Allcott and Matthew Gentzkow, 'Social Media and Fake News in the 2016 Election' (2017) 31 *Journal of Economic Perspectives* 211; Lisa Hill et al, *How and Why to Regulate False Political Advertising in Australia* (Springer Nature, 2022) 19-20; Soroush Vosoughi et al, 'The Spread of True and False News Online' (2018) 359 (6380) *Science* 1146.
[80] Zimmerman and Kohring (n 18) 231.
[81] Cantarella et al (n 18) 10.
[82] WEF (n 19) 18.

disinformation and illegal content', but that generally, 'the speed and effectiveness of regulation is unlikely to match the pace of development'.[83]

Some of the digital content that would cause or contribute to this type of harm would also in certain circumstances give rise to an offence under existing Australian legislation. For example, it is an offence under the *Commonwealth Electoral Act 1918* to publish or distribute anything likely to mislead or deceive an elector in relation to the casting of a vote, during the election period,[84] and there is an equivalent offence in the *Referendum (Machinery Provisions) Act 1984* (Cth), in relation to referendums.[85] The inclusion of this type of harm in clause 14 ensures that Schedule 9 complements existing Australian legislation by imposing obligations on digital communications platform providers to manage the risk that this type of content will be disseminated on their platforms, and by providing the ACMA with regulatory powers to require them to address this risk.

Paragraph (b): Harm to public health in Australia

Paragraph 14(b) covers harm to public health in Australia including to the efficacy of preventive health measures in Australia. Public health is defined in the Macquarie Dictionary as 'the health of a community, especially in relation to health issues affecting the whole community, such as water quality, nutrition, communicable diseases, etc.'[86] For the purposes of this type of harm, public health is understood to include the government system for providing for the health needs and services of all Australians, including preventative health measures, on the understanding that if this system and these measures are undermined, the health of Australians will consequentially be undermined.

The potential for health-related misinformation and disinformation to undermine the right to the highest attainable standard of health has been firmly established since the COVID-19 pandemic. Misinformation and disinformation that might have this effect could relate to how a disease is spread, the safety and effectiveness of vaccines or other preventive health measures, or health treatment options not supported by clinical data. Many studies have found that misinformation and disinformation of this nature can undermine public trust in expert guidance and government-led public health interventions, and consequently influence peoples' behaviour in a way that negatively impacts public health outcomes.[87]

A study conducted in Australia in 2021, for example, found that one in five adults aged 18–49 years agreed with some items of misinformation about COVID-19 vaccines. Misperceptions about COVID-19 vaccines were found to be associated with lower health literacy, less knowledge about vaccines, lower perceived personal risk of COVID-19, greater endorsement of non-COVID conspiracy beliefs, lower confidence in government, and lower trust in scientific institutions.[88] Another study the following year found that four in five Australians had seen misinformation about COVID-19, and that those who believed misinformation had 'lower levels of trust in doctors, health officials and other authoritative sources'.[89]

---

[83] Ibid.
[84] *Commonwealth Electoral Act 1918* (Cth) s 329(1).
[85] *Referendum (Machinery Provisions) Act 1984* (Cth) s 122(1).
[86] *Macquarie Dictionary* (online at 7 June 2024) 'public health'.
[87] Borges do Nascimento et al; Saiful Islam et al; Gisondi et al; Pickles et al; Suarez-Lledo and Alvarez-Galvez; WHO, *Ebola Virus Disease*; and Rubenstein and Kenneth (all at n 40).
[88] Pickles et al (n 40).
[89] ACMA, *ACMA Misinformation Report* (n 42) 1; Park et al, *COVID-19* (n 42) 48.

Health-related misinformation and disinformation online is particularly pernicious. Research during the COVID-19 pandemic found that in the first 11 months of 2020, 5 health and lifestyle websites promoting false health information received 10 times more interactions on social media (comments, likes and shares) than the World Health Organisation and the Centre for Disease Control combined.[90] One study in the US found that it took only '5 to 10 minutes on an anti-vaccine site to increase perceptions of vaccination risks and to decrease perceptions of the risks of vaccine omission'.[91]

Misinformation and disinformation also pose a risk to public health in contexts other than pandemics. One study of health information available online prior to 2019 found that health misinformation on social media was associated with: vaccines; diets and eating disorders; drugs and new tobacco products; pandemics and communicable diseases; noncommunicable diseases; and medical treatments and health interventions.[92] In 2022, a study of the most popular articles on social media in 2018-2019 about the 4 most common types of cancer found that one in 3 of the articles contained false, inaccurate or misleading information, and that most of that information was harmful – for example, by promoting unproven treatments as alternatives to those that rigorous studies had found to be beneficial.[93] Other studies have suggested that companies have employed 'social bots' to spread falsified health information to promote their products (such as e-cigarettes).[94]

Under international human rights law, the protection of public health is one of the few purposes for which governments may restrict the right to freedom of expression.[95] The Human Rights Committee has not explicitly defined what is meant by 'public health' for the purposes of justifying restrictions on the freedom of expression, but guidance may be sought from the way in which the Committee has understood 'public health' when interpreting restrictions to other human rights. In relation to the right to peaceful assembly, for example, the Human Rights Committee has said that:

> The protection of public health may exceptionally permit restrictions to be imposed, for example where there is an outbreak of an infectious disease and gatherings are dangerous. This may in extreme cases also be applicable where the sanitary situation during an assembly presents a substantial health risk to the general public or to the participants themselves.[96]

Many studies have affirmed the necessity for governments to manage the spread of misinformation and disinformation in order to protect public health. The World Health Organisation has warned that 'misinformation online has the potential to travel further, faster and sometimes deeper than the truth'.[97] In 2021, the World Health Assembly passed a resolution recognising the 'negative impact of misinformation, disinformation and

---

[90] Zakrzewski (n 43).
[91] Benecke and De Young (n 44).
[92] Suarez-Lledo and Alvarez-Galvez (n 40).
[93] Johnson et al (n 46).
[94] Allem and Ferrara (n 47).
[95] Article 19 of the ICCPR (n 6) provides that the right to freedom of expression may be subject to restrictions 'as are provided by law and are necessary: (a) for respect for the rights or reputations of others; (b) for the protection of national security or of public order (ordre public) or of public health or morals'.
[96] HRC, *General Comment No 37* (n 61) para 45.
[97] WHO, *Combatting Misinformation Online* (2024) available at: <Combatting misinformation online (who.int)>.

stigmatization on preparedness and response to health emergencies and people's physical and mental health, and the need to counter mis- and dis-information … in the context of health emergencies.' That resolution urged Member States to take measures to 'counter misinformation [and] disinformation', and called on 'international actors, partners, civil society and the private sector' to address, in coordination with Member States, 'the proliferation of disinformation and misinformation particularly in the digital sphere'.[98]

Paragraph (c): vilification of a group or member of a group

Paragraph 14(c) covers vilification of a group in Australian society distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin, or vilification of an individual because of a belief that the individual is a member of such a group.

Experience internationally as well as in Australia attests to the way in which misinformation and disinformation can amplify racial, ethnic, religious or other identity-based vilification.

A 2021 study by the European Parliament on disinformation about migrants and minority groups, for example, found that disinformation could contribute to a 'climate of hostility or a "sphere of hate"', which could 'reinforce prejudices and negative attitudes'.[99] That study reviewed content in the EUvsDisinfo database from 2018 and 2021, and found that many articles included in that database reported on migrants and/or Muslims as a threat to 'European culture and identity', or as a criminal threat or a threat to health.[100]

In a recent example, following a stabbing attack in northwest England in July 2024 which killed three young girls, a false (Muslim) name of an alleged suspect – said to be a recently arrived asylum seeker – was circulated on social media. The rumours prompted widespread violence targeting asylum seekers and Muslims, including attacks on mosques.[101] In earlier examples: in the context of the COVID-19 pandemic, content linking the Roma people to the spread of the virus led to stigmatisation and discrimination against the Roma in several European States;[102] and in 2015, a disinformation campaign created fake accounts purportedly owned by Muslim extremists, and posted messages about 'taking over Denmark' and killing and raping non-Muslim Danish people – thus stoking anti-Muslim sentiment.[103]

Disinformation can also amplify pre-existing harmful gender stereotypes, which can result in gender-based vilification. A 2021 US-based study found that gendered disinformation can 'make use of existing gender narratives, language, and ultimately discrimination to achieve certain social and political goals'; for example, by characterising female politicians as 'not being qualified for the position, lacking the requisite knowledge, intelligence, or experience for the role; or as persons who lie, are too emotional for the task, prone to aggression, or lacking sanity'.[104] The 2023 report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression stated similarly that 'gendered

[98] World Health Assembly, *Strengthening WHO Preparedness for and Response to Health Emergencies*, WHA 74.7 (31 May 2021) para 8(3) <https://apps.who.int/gb/ebwha/pdf_files/WHA74/A74_R7-en.pdfv>.
[99] Szakacs and Bognar (n 13) 23.
[100] Ibid 13.
[101] Lawless, (n30); Al Jazeera, (n30).
[102] Szakacs and Bognar (n 13) 15.
[103] Ibid 10.
[104] Thakur and Hankerson (n 33) 25; see also Jankowicz et al (n 33).

disinformation … uses highly emotive and value-laden content, tailored to local contexts, that undermines women's credibility and competence, stigmatizes them and isolates them', and that 'gender narratives have been invoked against women journalists, sexualising them and attacking their character, integrity, appearance and intelligence as a way of discrediting their reporting and discouraging them from continuing their work'. That report stated further that 'forms of harm emanating from gendered disinformation are varied and deeply consequential to both individuals and society at large', and that targeted individuals pay a 'heavy price psychologically, physically, socially and economically'.[105]

Australian research has similarly found a link between disinformation online and vilification based on race, ethnicity and other characteristics. Research by the Australian Human Rights Commission in 2021, for example, identified a 'correlation between negative media and political narratives about Muslims and Islam and an increase in aggression and violence towards Australian Muslims', and identified 'the perpetuation of stereotypes and the inclusion of misinformation about Muslim people and Islam … as particularly damaging aspects of these narratives'.[106] In 2023, UN human rights experts recognised that the spread of hatred and hate speech against marginalised groups undermines their rights and 'creates fissures in societies', and called upon 'social media companies [to] urgently address posts and activities that advocate hatred and constitute incitement to discrimination, in line with international standards for freedom of expression'.[107]

The inclusion of this category of harm aligns broadly with the approach taken in existing Australian anti-discrimination and anti-vilification legislation, at the Commonwealth level and in most of the states and territories. Specifically:

The Commonwealth *Racial Discrimination Act 1975* prohibits conduct, other than in private, that is reasonably likely to offend, insult, humiliate or intimidate another person or a group of people, if that conduct is done because of the race, colour or national or ethnic origin of the other person or of some or all of the people in the group.108

The Queensland *Anti-Discrimination Act 1991* makes it unlawful to publicly 'incite hatred towards, serious contempt for, or severe ridicule of, a person or group of persons on the ground of the race, religion, sexuality, sex characteristics or gender identity of the person or members of the group'.109

The Tasmanian *Anti-Discrimination Act 1998* makes it unlawful to publicly incite hatred towards, serious contempt for, or severe ridicule of, a person or group of persons on the ground of race, disability, sexual orientation, lawful sexual activity, religious belief, affiliation or activity, or gender identity or sex characteristics, of that person or any member of the group.110

The Northern Territory *Anti-Discrimination Act 1992* prohibits the doing of an act that is reasonably likely to offend, insult, humiliate or intimidate another person or a group of people because of an attribute of the person or of some or all of the people in the group.111

South Australian, Western Australian, New South Wales and Victorian legislation includes narrower provisions relating specifically to the incitement of racial and/or religious hatred. The South Australian *Racial Vilification Act 1996* and the New South Wales *Anti-Discrimination Act 1977* prohibit the incitement of race-based hatred, contempt or ridicule,112 the Western Australian *Criminal Code Act Compilation Act*

[105] Khan, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (n 34) paras 45-46.
[106] AHRC (n 35).
[107] Namakula et al (n 36).
[108] Section 18C.
[109] *Anti-Discrimination Act 1991* (Qld) ss 124A(1).
[110] Section 19.
[111] Section 20A.
[112] *Racial Vilification Act 1996* (SA) s 4; *Anti-Discrimination Act 1977* (NSW) s 20C.

1913 makes it an offence to promote racial harassment or animosity,113 and the Victorian *Racial and Religious Tolerance Act 2001* prohibits the incitement of racial or religious hatred.114

The above-mentioned legislative provisions prohibit persons from engaging in conduct online that may incite hatred or vilification towards an individual or group on the basis of a protected attribute. These provisions do not, however, impose obligations on digital communications platform providers to take proactive and systemic measures in relation to the dissemination of this type of content.

The Online Safety Act and the Commonwealth Criminal Code go some way towards filling this gap. The Online Safety Act empowers the Communications Minister to determine basic online safety expectations for social media, and relevant electronic and designated internet services, including an expectation that they will minimise the availability on their services of: cyber-bullying; cyber-abuse; non-consensual intimate images; abhorrent violent material; and material that is otherwise outside generally accepted community standards.[115] The Online Safety Act also empowers the eSafety Commissioner to undertake certain actions in response to complaints made about those same types of material.[116] The Criminal Code, for its part, requires internet, content and hosting service providers to notify the police of abhorrent violent material hosted on their services, and makes it an offence for a content or hosting service provider to recklessly host abhorrent violent material.[117]

However, neither the Online Safety Act nor the Criminal Code impose obligations on the providers of digital communications platforms to manage the risk posed by the dissemination of seriously harmful false, misleading or deceptive content, unless that content constitutes one of the listed types of material (in the case of the Online Safety Act) or is abhorrent violent material (in the case of the Criminal Code). Moreover, neither of these Acts require digital communications platform providers to proactively empower end-users to identify misinformation and disinformation; nor do they empower the ACMA to take regulatory action aimed at reducing the risk that false, misleading or deceptive content will cause or contribute to serious harm in Australia.

Thus, through the inclusion of vilification as a type of serious harm in clause 14, the regulatory scheme set out in Schedule 9 to the BSA complements existing Australian legislation by requiring digital communications platform providers to proactively manage the risk that content on their platforms will cause or contribute to the vilification of a person or group on the basis of one of the listed attributes.

The inclusion of this category of harm is necessary to protect the right of all Australians to enjoy their human rights and fundamental freedoms without distinction. This right is enshrined in Article 2 of the ICCPR, which requires each States Party to 'ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.' The Human Rights Committee has recognised that vilification of a person or group on

113 Sections 77 and 78.
114 Sections 7(1) and 8(1).
115 *Online Safety Act 2021* (Cth) s 46(1)(c).
116 Ibid, e.g. ss 77 and 88.
117 *Criminal Code Act 1995* (Cth) ss 474.33 and 474.34 of the Schedule.

the basis of their race, ethnicity, religion or other protected attribute can effectively nullify or impair the exercise by that person or group of their human rights and fundamental freedoms, on an equal footing with others.[118] Thus, in order to enjoy their human rights and fundamental freedoms without distinction, individuals must be protected from being vilified because of their identity. Legislative action to manage the risk of vilification online is therefore consistent with and supports the fulfilment of Australia's obligations under the ICCPR.

Paragraph (d): Intentionally inflicted physical injury to an individual in Australia

Paragraph 14(d) covers the intentional infliction of physical injury to an individual in Australia. Experience in Australia and elsewhere shows that online content that is false, misleading or deceptive, and provokes public hatred or anger towards an individual or individuals, can put the targeted individuals in danger. Content inciting violence against individuals could be captured here, but there may also be content that does not directly incite violence, but is nevertheless likely to cause the intentional infliction of physical injury. Such content might include smear campaigns targeting prominent individuals for political or personal reasons, or content incorrectly framing an individual or individuals for wrongdoing, provoking public outrage, if in the circumstances that content can be considered reasonably likely to cause (or contribute to) a person in Australia being intentionally, physically injured.

The word 'intentional' is important to this type of harm. This category of harm is not intended to capture misinformation or disinformation that is likely to result in risk-taking by individuals, or accidental harm; but only content that is reasonably likely to result in an individual being intentionally, physically harmed. The vitriolic misinformation campaign that followed the attacks in Bondi, Sydney in April 2024, that wrongly identified a Jewish Australian individual as responsible for the attacks, resulting in death threats to that individual, provides a recent example.[119] Other examples include a vitriolic misinformation campaign targeting a Gold Coast doctor in February 2022, which also included death threats, following claims on social media that two girls died after being vaccinated for COVID-19 at his practice;[120] false reports about child abductions, spread on social media and messaging apps in France in 2019, which prompted vigilante attacks against Roma people;[121] and a video that went viral in India in 2018, falsely identifying five individuals as child kidnappers, prompting a mob attack on the individuals which killed one and left others injured.[122]

As with most of the other types of harm listed in this clause, the dissemination of content online that would be reasonably likely to cause or contribute to physical injury to a person would also in some cases be prohibited, or would be an offence, under existing Australian law. In particular, under the Criminal Code it is an offence to urge the commission of an offence.[123] This could – if the elements of the offence of incitement were satisfied – include the dissemination of content online that would be reasonably likely to result in a person being physically injured. And, as noted above in relation to paragraph (c) (vilification), the Online Safety Act allows complaints to be made about certain types of violent and abusive material online, some of which might also be reasonably likely to lead to physical harm. Again, as

[118] *Ross v Canada* (n 25) para 11.5; HRC, *Views: Communication No 550/1993*, UN Doc CCPR/C/58/D/550/1993 ('*Faurisson v France*') para 9.6.
[119] See Palmer (n 11); Nguyen and Workman (n 11).
[120] Tsirtsakis (n 12).
[121] AFP (n 13); Szakacs and Bognar (n 13) 14.
[122] Samuels (n 14).
[123] *Criminal Code Act 1995* (Cth) s 11.4(1) of the Schedule.

noted above, however, this existing legislation does not cover all false, misleading or deceptive content disseminated online that would be reasonably likely to result in physical injury. Nor does it impose obligations on digital communications platform providers, or provide the ACMA with regulatory powers, to require digital communications platform providers to manage the risk posed by this type of content.

In order for content disseminated online to be considered reasonably likely to cause or contribute to this type of harm, there is no requirement that the harm actually eventuate. Thus, dissemination of content that is false, misleading or deceptive may be considered misinformation or disinformation on the basis that it is reasonably likely to cause or contribute to the intentional infliction of physical injury to an individual in Australia, regardless of whether such physical injury is in fact inflicted.

The inclusion of this category of harm is necessary to protect the right of all Australians to security of person, enshrined in Article 9 of the ICCPR. The Human Rights Committee has said that the right to security of the person protects individuals against 'intentional infliction of bodily or mental injury'. The Committee has said that in order to safeguard this right, States Parties are required to 'take appropriate measures in response to death threats against persons in the public sphere, and more generally to protect individuals from foreseeable threats to life or bodily integrity proceeding from any governmental or private actors.' The Committee has said moreover that the right to personal security requires States to take 'prospective measures to prevent future injury'. (See HRC, *General Comment No. 35* (n10)).

Paragraph (e): Imminent damage to critical infrastructure or disruption of emergency services

Paragraph 14(e) covers imminent damage to critical infrastructure or imminent disruption of emergency services. Critical infrastructure means the systems, services, capital equipment and permanent installations that are fundamental to the effective functioning of society. The Macquarie Dictionary defines infrastructure as '(1) the basic framework or underlying foundation (as of an organisation or system); (2) the roads, railways, schools and other capital equipment which comprise such an underlying system within a country or region; and (3) the buildings or permanent installations associated with any organisation, operation, etc'.[124] This category of harm encompasses all these things, but is also broader, in that it encompasses not just physical assets but also essential services. This draws on the definition of infrastructure provided by the Cambridge English Dictionary, which is: 'the basic systems and services, such as transport and power supplies, that a country or organisation uses in order to work effectively.'[125] For the purposes of this kind of harm, critical infrastructure includes all these elements.

Emergency services means, pursuant to the definition provided by the Oxford English Dictionary: 'the public organisations that deal with emergencies: the police, fire, ambulance and coastguard services'.[126]

Examples of content that could result in serious harm to critical infrastructure could include the spread of false pricing information, which if disseminated at scale could cause drastic and

[124] *Macquarie Dictionary* (n 86) 'infrastructure' (defs 1-3).
[125] *Cambridge Dictionary* (online at 11 June 2024) 'infrastructure'.
[126] *Oxford English Dictionary* (online at 11 June 2024) 'emergency services'.

sudden changes in user commodity consumption behaviour[127] – for example, false discount notifications encouraging consumers to shift their energy consumption into the peak demand period, resulting in the tripping of overloaded power lines.[128] It could also include misinformation regarding 5G technology, which in Australia in 2020 prompted arson and vandalism attacks at mobile sites due to fear that the 5G network was spreading COVID-19;[129] or it could include a false alert aimed at prompting a large-scale response to a security threat, for example at a major train station or airport, that could result in delays or diversions and thus disrupt critical supply chains.[130]

Misinformation and disinformation can also pose a threat to the functioning, operations or effectiveness of emergency services. This could be the case, for example, in circumstances where content promotes false claims regarding the location of bushfires or the details of emergency evacuation warnings, that could cause people to act on false information, putting themselves in danger and diverting the attention of fire services.

As with the other types of harm, content will not be considered misinformation or disinformation for the purposes of Schedule 9 unless it satisfies the threshold criteria set out in paragraphs 14(g) and 14(h); that is to say, unless it is reasonably likely to cause or contribute to harm that has significant and far-reaching consequences for the Australian community or a segment thereof, or severe consequences for an individual in Australia. Thus, content will not be considered misinformation or disinformation if it is likely to result in only minor damage to critical infrastructure or disruption of emergency services, such as may be caused, for example, if content posted online is likely to provoke minor vandalism or public protest, or place emergency services under additional but manageable strain.

Article 19 of the ICCPR, which enshrines the right to freedom of expression, provides that the freedom of expression may be restricted as necessary to protect 'public order (ordre public)'.[131] The Human Rights Committee has not explicitly defined 'public order (ordre public)', for the purposes of Article 19(3) of the ICCPR; however, in relation to a similar clause describing permissible restrictions on the right of peaceful assembly, the Committee has said that 'public order' refers to 'the sum of the rules that ensure the proper functioning of society, or the set of fundamental principles on which society is founded'.[132] Critical infrastructure and emergency services are included as a kind of harm, for the purpose of defining misinformation and disinformation, on the understanding that protecting against serious harm to critical infrastructure and emergency services is necessary to protect public order.

Paragraph (f): Imminent harm to the Australian economy

Paragraph 14(f) covers imminent harm to the Australian economy, including harm to public confidence in the banking system or financial markets.

---

[127] Saeed Jamalzadeh et al, 'Protecting Infrastructure Performance from Disinformation Attacks' (2020) 12(1) *Scientific Reports* 12177.
[128] Gururaghav Raman et al, 'How Weaponizing Disinformation can Bring Down a City's Power Grid' (2020) 15(8) *PLOS One* 02136517.
[129] ACMA, *A Report to Government* (June 2021) (n 4) 32-3.
[130] Saeed Jamalzadeh et al, 'Weaponized Disinformation Spread and its Impact on Multi-Commodity Critical Infrastructure Networks' (2024) 243 *Reliability Engineering and System Safety* 109819.
[131] ICCPR (n 6) art 19(3).
[132] HRC, *General Comment No 37* (n 61) para 44.

Examples of online content that could cause or contribute to this type of harm could include false or misleading content about the financial health of a corporation, aimed at manipulating stock prices; or false or misleading content warning about the financial health of a financial institution, which if disseminated at a certain scale, could provoke a 'digital bank run'. A bank run occurs when customers lose faith in an institution's ability to look after their money, prompting a large number of customers to withdraw their funds simultaneously. This in turn increases the likelihood that the institution will not be able to cover the withdrawals, sparking further panic and prompting more customers to seek to withdraw their funds. The Assistant Governor of the Reserve Bank of Australia has referred to this as 'herding behaviour', which is enabled by depositors being in close contact, which is turn is enabled by social media.133 Experts suggest that on social media, the psychological behaviour behind a bank run – mass fear of loss of savings – can be amplified and go viral at a pace that exceeds the response capacity of banks and regulators.134 Digital bank runs can cause the collapse of a financial institution, at enormous cost to individuals and to the broader economy.

Several real-world examples illustrate this risk. In March 2023, posts on social media regarding the financial health of Silicon Valley Bank (SVB) went viral, and in response, customers withdrew $42 billion in just a few hours. SVB was placed under receivership the following day. Research into the events leading up to SVB's failure found that Twitter (now X) was the driving force behind the financial panic that ultimately led to the collapse of SVB. That research found that while not all tweets were false, misleading or deceptive, there were 'unequivocal examples of the propagation of misinformation during the run [on SVB]'.[135] In other examples of the way in which misinformation and disinformation online can undermine public confidence in financial institutions, reports indicated that in 2011, an unfounded rumour spread on social media about the Latvian branches of a Stockholm-based bank led to 'queues building up at ATMs as people wanted to withdraw money, which resulted in some ATMs being emptied of money';[136] and in 2019, false information in a WhatsApp post led to a run on Metro Bank in the UK.[137]

Misinformation and disinformation about the health of a financial institution, which undermines public confidence in that institution, can – if disseminated at scale – undermine public confidence in the banking system as a whole. Following the above-mentioned collapse of SVB, for example, the share price of Switzerland's Credit Suisse fell 30 percent.[138]

Content which undermines public confidence in the health of a financial institution will not fall within the scope of paragraph 14(f) unless it is likely to cause or contribute to 'imminent harm to the Australian economy'. This is a high threshold. In line with this high threshold, the example provided in this paragraph is 'harm to public confidence in the *banking system or financial markets*', not just harm to a single institution. Whether dissemination of content on a

[133] Brad Jones, 'Emerging Threats to Financial Stability – New Challenges for the Next Decade' (Speech, Australian Finance Industry Association Conference, Sydney, 31 October 2023) <https://www.rba.gov.au/speeches/2023/sp-ag-2023-10-31.html>.
[134] Jonathan Yerushalmy, '"The first Twitter-fuelled bank run": how social media compounded SVB's collapse' (*The Guardian*, 16 March 2023) <https://www.theguardian.com/business/2023/mar/16/the-first-twitter-fuelled-bank-run-how-social-media-compounded-svbs-collapse>.
[135] Anthony Cookson et al, 'Social Media as a Bank Run Catalyst' (Université Paris-Dauphine Research Paper No 4422754, July 2023) <Social Media as a Bank Run Catalyst by J. Anthony Cookson, Corbin Fox, Javier Gil-Bazo, Juan Felipe Imbet, Christoph Schiller :: SSRN>.
[136] Philip van Doorn, 'Twitter's First Bank Run' (*The Street*, 12 December 2011) < Twitter's First Bank Run - TheStreet>.
[137] Silvia Merler, 'Fast and Furious: How Digital Bank Runs Challenge the Banking-Crisis Rulebook' (*The Why Axis*, Bruegel, 27 March 2023) <https://www.bruegel.org/first-glance/fast-and-furious-how-digital-bank-runs-challenge-banking-crisis-rulebook>.
[138] Yerushalmy (n 134).

digital service could be considered reasonably likely to cause or contribute to (serious) harm to the Australian economy, for example by undermining public confidence in the banking system, would be a question of fact that could only be determined on a case-by-case basis, bearing in mind the factors listed at subclause 13(3).

Another example of misinformation that could cause or contribute to serious harm to the Australian economy is market-related false, misleading or deceptive information, that could disrupt a supply chain or supply chains. Research has highlighted the essential role of accurate information in supply chains. This includes information from customers that signals their preferences to a retailer. Such information is then transmitted 'to the supply chain, from retailers to transportation, storage, manufacturing and suppliers', and then in turn is 'used for transportation, storage, manufacturing and ordering operations and processes.' Demand-related misinformation and disinformation of this nature creates a distorted distinction between forecast and actual demand, and thus 'can disrupt every part of the supply chain'.[139] Misinformation and disinformation can also disrupt supply chains by unnecessarily increasing demand. As demonstrated by a recent study of supply chain disruptions during the COVID-19 pandemic, 'misinformation spreads like wildfire – from tomorrow there will be a complete lockdown – and people rush to the market to stock up on essential items, resulting in stock shortages in shops, causing more demand, and consequently, breaking down the supply chain system'.[140] Similarly to misinformation about a financial institution, whether market-related misinformation would be considered reasonably likely to cause or contribute to serious harm to the Australian economy by disrupting a supply chain would be a question of fact, to be considered on a case-by-case basis in light of the factors listed at subclause 13(3).

Paragraphs (g) and (h)

The effect of paragraphs 14(g) and 14(h) is that in order to be considered misinformation or disinformation for the purposes of Schedule 9, the dissemination of verifiably false, misleading or deceptive content on a digital communications platform must be reasonably likely to cause or contribute to harm that is not only one of the types of harm set out in paragraphs 14(a) to (f), but also has significant and far-reaching consequences for the Australian community or a segment thereof, or severe consequences for an individual in Australia. This is what makes the harm serious. The inclusion of these alternate tests (significant and far-reaching consequences for the Australian community or a segment thereof *or* severe consequences for an individual) reflects the policy intent that if the harm in question only impacts one individual, then in order to be considered 'serious', the consequences of that harm will need to be greater ('severe') than in the case of content that impacts a large number of Australians – in which case, the consequences need only be 'significant'.

In the case of three of the six types of harm, the very nature of those harms as described in clause 14 suggests that the harm cannot impact just a single individual. This is the case for: harm to the operation or integrity of an electoral or referendum process (paragraph 14(a)); harm to public health (paragraph 14(b)); and harm to the Australian economy (paragraph 14(f)). All of these harms necessarily impact the Australian community as a

[139] Pythagoras Petratos and Alessio Faccia, 'Fake News, Misinformation, Disinformation and Supply Chain Risks and Disruptions: Risk Management and Resilience Using Blockchain' (2023) 327 *Annals of Operations Research* 735, 748-49.
[140] Sheshadri et al, 'Role of Fake News and Misinformation in Supply Chain Disruption: Impact of Technology Competency as a Moderator' (2023) 327 *Annals of Operation Research* 659, 660.

whole, or a segment thereof. In order for these types of harm to be 'serious', the consequences of the harm will need to be significant and far-reaching, as set out at paragraph 14(g).

Conversely, the vilification of a group in Australian society or member of a group (paragraph 14(c)), the intentional infliction of physical injury (paragraph 14(d)) and damage to critical infrastructure or disruption of emergency services (paragraph 14(e)) could be serious if the harm had *either* severe consequences for just one person in Australia (paragraph 14(h)), or significant and far-reaching consequences for the Australian community or segment thereof (paragraph 14(g)). It is also possible that harm of a type listed at clause 14 may have significant and far-reaching consequences for the Australian community or a segment thereof, *and* severe consequences for an individual or individuals.

Subclause 13(3) sets out a list of matters to which regard must be had, for the purpose of determining whether content disseminated on a digital service is reasonably likely to cause or contribute to serious harm of one of the types listed in clause 14 (see explanation provided above in relation to subclause 13(3)).

Assessing serious harm – example 1

False information about where and when to vote in a State election could cause or contribute to serious harm. This is because, either alone or in conjunction with other similar content, this type of information could effectively prevent (or contribute to preventing) a large number of people from voting so that the outcome of an election could be influenced. The integrity of the electoral process would thus be undermined. This would have significant and far-reaching consequences for the entire population of the State, which is to say, a segment of the Australian community. In determining whether the dissemination in question would be reasonably likely to cause or contribute to serious harm of this type, consideration would need to be given to the factors listed at subclause 13(3). Particularly pertinent factors would likely include whether the false information was seemingly disseminated by the relevant State electoral authority, the potential speed and reach of the dissemination, and whether the subject matter of the content in question was likely to prevent people from exercising their free and informed choice as electors.

Assessing serious harm – example 2

False, misleading or deceptive information about harmful side effects of vaccines could cause or contribute to serious harm, if – again, either alone or in conjunction with other content – it is sufficiently persuasive and disseminated at such a scale that a large number of people could be persuaded not to get vaccinated. This could cause harm to public health, of a nature that would have significant and far-reaching consequences for the Australian community or a segment thereof. In determining whether the dissemination in question would be reasonably likely to cause or contribute to serious harm of this type, consideration would need to be given to the factors listed at subclause 13(3). Particularly pertinent factors would likely include whether the false information was seemingly disseminated by a relevant health authority, the severity of the side effects being alleged (that is, whether they were sufficiently severe to dissuade people from getting vaccinated), and the potential speed and reach of the dissemination.

Assessing serious harm – example 3

False, misleading or deceptive information about the benefits of a particular diet, with clinically proven adverse effects, could harm public health. Following consideration of the factors listed at subclause 13(3), however, it may be determined that the harm is unlikely to be serious, because it is unlikely to have significant and far-reaching consequences for the Australian community or a segment thereof. This may be because the author of the content is not authoritative enough to sway large numbers of Australians, or because the harmful side effects of the diet are not that significant, or because there is enough other information available on the relevant digital communications platform(s) on healthy diets, to counter the false, misleading or deceptive content in question.

Assessing serious harm – example 4

False information accusing an individual of wrongdoing – not on the basis of race, ethnicity or any other protected attribute – would generally be *unlikely* to cause or contribute to serious harm of a type listed in clause 14. However, paragraph 13(3)(a) requires that, in determining whether the provision of content on a digital service is reasonably likely to cause or contribute to serious harm, consideration be given to the 'circumstances in which the content is disseminated'. In extreme circumstances, false accusations of wrongdoing targeting an individual might be likely to cause (or contribute to) an individual being intentionally, physically harmed. This might be the case, for example, when the alleged wrongdoing is so heinous that it provokes public outrage and a collective desire for vengeance; or when the allegation taps into pre-existing public outrage, and effectively channels that outrage towards the targeted individual (such as, for example, the misinformation campaign targeting the Gold Coast doctor in the context of COVID vaccines, discussed at paragraph 14(d)). Whether this type of false, misleading or deceptive content could be considered reasonably likely to cause or contribute to the intentional infliction of physical injury to an individual, with severe consequences for that individual, would depend on an assessment of all factors listed at subclause 13(3).

Clause 15—Meaning of inauthentic behaviour

Subclause 15(1) explains that dissemination of content on a digital service involves ***inauthentic behaviour*** if one of the circumstances outlined in paragraphs 15(1)(a) to (d) applies.

Paragraph 15(1)(a) covers dissemination that uses an automated system in a way that is reasonably likely to mislead an end-user about a matter covered by subclause 15(2).

Paragraph 15(1)(b) covers circumstances where there are grounds to suspect the dissemination is part of coordinated action that is reasonably likely to mislead an end-user about a matter covered by subclause 15(2).

Paragraph 15(1)(c) covers a situation where there are grounds to suspect that the dissemination uses an arrangement for the purpose of avoiding action by the provider of the digital service to comply with the BSA or another law, or to enforce compliance with the digital service's terms of use.

Paragraph 15(1)(d) allows the digital platform rules to specify other circumstances in which the dissemination of content will constitute inauthentic behaviour. This allows flexibility for rules to be made to respond to new types of inauthentic behaviour as the online landscape

evolves. Allowance for the digital platform rules to specify additional circumstances in which the dissemination of content will constitute inauthentic behaviour also enables the ACMA to adapt the definition of inauthentic behaviour based on information made available pursuant to the operation of other provisions in Schedule 9, including information on misinformation complaints provided by digital communications platforms pursuant to digital platform rules made under paragraph 25(2)(c), and any additional information regarding misinformation and disinformation on digital communications platforms obtained by the ACMA pursuant to clauses 33 and 34.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that the rules would be subject to parliamentary disallowance and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

Subclause 15(2) provides that for the purposes of paragraphs 15(1)(a) and 15(1)(b), the 'matters' – about which the dissemination in question must be reasonably likely to mislead an end-user – are: the identity, purpose or origin of the person disseminating the content; the popularity of the content on the digital service (which might be indicated, for example, through manipulation of the number of interactions with the content, including views, shares, likes and/or downloads); the motive or intention of an end-user; and the source or origin of the content.

Clause 15 has been drafted to cover similar types of disinformation tactics, techniques and procedures as outlined under the definition of '*impermissible manipulative behaviour*' in the European Commission's 2022 Strengthened Code of Practice on Disinformation[141] including:

- the creation and use of fake accounts, account takeovers and bot-driven amplification
- impersonation
- malicious deep fakes
- 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.

The definition of inauthentic behaviour in clause 15 is also broadly reflective of the definition provided by the Australian Code of Practice on Disinformation and Misinformation, which states that 'inauthentic behaviours' include:

> 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 to encourage users of digital platforms to propagate Digital Content.[142]

Content disseminated by means of inauthentic behaviour, as defined by clause 15, would include, but is not limited to content disseminated by means of:

---

[141] European Commission, *The Strengthened Code of Practice on Disinformation 2022* (16 June 2022) <2022 Strengthened Code of Practice on Disinformation | Shaping Europe's digital future (europa.eu)>.
[142] *DIGI Code* (n 2).

- automated programs used to engage in social media for a particular purpose, for example, to amplify misinformation or disinformation or trick people into clicking on scam links, and which typically have the appearance of an ordinary human ('bots')
- fictitious social-media identities, set up with intent to deceive ('catfish' or 'sock puppet' accounts)
- software that directs large numbers of social media accounts to send out the same message, or like and share a post, which manipulates social media algorithms by suggesting there is widespread interest in a particular view, in turn increasing the likelihood that the content in question will be engaged with by others
- automated tools used to generate a large amount of textual web content, specifically designed to satisfy algorithms for maximum retrieval by search engines ('content farms')
- 'layering', which refers to the creation of an online trail from an original source of false information to a more credible one. Pursuant to this tactic, a false fact is initially 'placed' or 'seeded' online, and is then layered through online spreader accounts (fake and real) and AI generated fake or dubious 'news' websites, obscuring its origin. Such layering might for example be propagated by a malign foreign actor, who is initially part of an innocuous social media group, and then builds trust with that group, before proceeding to seed and spread misinformation or disinformation. This misinformation or disinformation is subsequently 'integrated', meaning that it is picked up by real news websites and further disseminated, creating a veneer of plausibility.

Inauthentic behaviour includes coordinated action (paragraph 15(1)(b)), i.e. 'coordinated inauthentic behaviour' (CIB), which is intended to refer to coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation. In 2023, the Australian Senate Select Committee on Foreign Interference through Social Media reported that 'all social media platforms who appeared before the committee stated that they found and removed CIB that sought to influence Australia'.[143]

Prominent examples of CIB detected by digital communications platform providers and reported in recent years include the spread of election-related content by 50,000 Russian-linked spam/bot accounts on Twitter during the 2016 US presidential election;[144] 'Doppelgänger', an online information operation originating from Russia, which since at least February 2022 has targeted multiple countries with the aim of undermining support for Ukraine;[145] and a vast covert influence operation originating in China, disrupted by Meta in 2023, which was active on more than 50 platforms and forums and targeted numerous countries including Taiwan, the US, Australia, the UK, Japan, and global Chinese-speaking audiences.[146]

[143] Senate Select Committee on Foreign Interference through Social Media, Australian Parliament, *Report* (August 2023) <Senate Select Committee on Foreign Interference through Social Media (aph.gov.au)> 154.
[144] Tauhid Zaman, 'Can We Protect Our Election from the Bots' (*Yale Insights*, 16 October 2020) <https://insights.som.yale.edu/insights/can-we-protect-election-from-the-bots>.
[145] EU DisinfoLab, *Doppelganger Operation* (Web Page, 30 May 2024) <https://www.disinfo.eu/doppelganger-operation/>.
[146] Ben Nimmo et al, *Adversarial Threat Report: Second Quarter* (Meta, August 2023) <https://transparency.meta.com/en-gb/metasecurity/threat-reporting/> 11.

Clause 16—Meaning of *excluded dissemination*

Clause 16 explains the meaning of ***excluded dissemination*** for the purposes of Schedule 9. The obligations imposed on digital communications platform providers in relation to misinformation and disinformation on their platforms, and the ACMA's regulatory powers in relation to misinformation and disinformation, would not cover this type of excluded dissemination.

These exclusions assist to ensure that, to the extent that the measures provided in Part 2 of Schedule 9 restrict the right to freedom of expression, those restrictions are reasonable, necessary and proportionate to the achievement of a legitimate objective – that is, the objective of protecting Australians from serious harm caused or contributed to by the dissemination of false, misleading or deceptive information on digital communications platforms.

Paragraph 16(1)(a)

Paragraph 16(1)(a) excludes the dissemination of content that would reasonably be regarded as parody or satire. 'Parody' is defined in the Macquarie Dictionary as 'a humorous or satirical imitation of a serious piece of literature or writing'.[147] 'Satire' means 'the use of irony, sarcasm, ridicule, etc., in exposing, denouncing, or deriding vice, folly, etc.'[148]

The exclusion for content that would reasonably be regarded as satire or parody is important in order to ensure that, insofar as the measures imposed by Part 2 of Schedule 9 restrict the freedom of expression, these restrictions align with Australia's obligations under international human rights law. The UN Special Rapporteur on Disinformation and the Freedom of Opinion and Expression has explicitly recognised that 'under international human rights law, people have the right to express ill-founded opinions and statements or indulge in parody or satire if they so wish'.[149]

The other reason for this exclusion is that if content is reasonably regarded as parody or satire, it would not generally be expected that end-users would perceive and act upon that content as if it were authoritative or factual. Thus, content of this nature would be less likely to mislead or deceive.

An example of the dissemination of content that would be covered by this exclusion would be false information captured in an internet meme designed to make fun of the viewpoint expressed in the meme.

Paragraph 16(1)(b)

Paragraph 16(1)(b) excludes the dissemination of professional news content, which is defined separately under subclause 16(2). The purpose of including the professional news content exception is to not infringe on the independence of the media. The exclusion of *professional news content* also acknowledges that this type of content is subject to the industry's own

[147] *Macquarie Dictionary* (n 86) 'parody' (def 1).
[148] Ibid, 'satire' (def 1).
[149] Khan, *Disinformation and Freedom of Opinion and Expression* (n 18) para 38.

separate and recognised editorial standards. Further, digital platform services should not be in the position of determining if professional news content is misinformation or disinformation.

Paragraph 16(1)(c)

Paragraph 16(1)(c) excludes 'reasonable dissemination of content for any academic, artistic, scientific or religious purpose'. This exclusion sits alongside similar exclusions provided in Australia's anti-discrimination laws. For example, the *Racial Discrimination Act 1975* provides an exemption for 'anything said or done reasonably and in good faith … in the course of any statement, publication, discussion or debate made or held for any genuine academic, artistic or scientific purpose or any other genuine purpose in the public interest'.[150]

Dissemination that might be considered to be for an academic, artistic, scientific or religious purpose (putting aside the question of 'reasonableness') could include:

- informed commentary by an academic on a matter relevant to their expertise, for example, commentary by a legal academic regarding a recent judicial decision or academic publication in their field
- a post by a researcher sharing the results of a scientific study, for the benefit of others working in the same field
- a post by a religious leader, promoting or explaining religious practices or doctrine.

For the purposes of paragraph 16(1)(c), whether the dissemination of content is 'reasonable' dissemination for an academic, artistic, scientific or religious purpose is intended to be an objective test which will be informed by contextual factors.

It is intended that the reasonableness standard in paragraph 16(1)(c) be interpreted similarly to the way in which Australian courts have considered the standard of reasonableness for the purposes of section 18D of the *Racial Discrimination Act 1975*. In relation to section 18D, in the Federal Court of Australia, French J in *Bropho v Human Rights and Equal Opportunity Commission* (2004) said that 'a thing is done reasonably in one of the protected activities in … s 18D [including the distribution of an artistic work, or a statement made for any genuine academic, artistic or scientific purpose] if it bears a rational relationship to that activity and is not disproportionate to what is necessary to carry it out'. French J said that the test 'imports an objective assessment', which 'means a judgment independent of that which the actor thinks is reasonable'.[151] Thus, whether the dissemination would be 'reasonable' would depend on contextual factors and the circumstances of the dissemination.

For the purposes of paragraph 16(1)(c), the focus is on the *dissemination* of content on a digital communications platform; that dissemination must, on an objective assessment, be reasonable for one of the stated purposes. The issue is not the reasonableness of the content itself. In some circumstances this distinction will be immaterial, because if content is in the first place so unreasonable, it will also be unreasonable to share it any further. However, in some circumstances the dissemination of content may be reasonable for the purposes of paragraph 16(1)(c), even if the content itself is unreasonable.

[150] Paragraph 18D(b).
[151] *Bropho v Human Rights and Equal Opportunity Commission* (2004) 135 FCR 105, [79] (French J).

For example, it may be reasonable to reshare content falsely linking a particular ethnic group to a risk of violent crime, in a post that is part of a discussion about the role of social media in perpetuating harmful racial stereotypes.

Subclause 16(2)

Subclause 16(2) provides the definition of ***professional news content*** for the purposes of Schedule 9. It is defined as news content produced by a person who: produces, and publishes online, ***news content*** (see subclause 16(3)) in one or more of the formats listed at paragraph 16(2)(a); is subject to the professional rules listed in one of the subparagraphs of paragraph 16(2)(b); and who has editorial independence from the subjects of the person's news coverage (paragraph 16(2)(c)).

Whether news content is professional news content depends on who produced it to begin with, rather than who posted it. For example, if a news article produced by a professional news outlet was published online by that news outlet and then was reposted by an individual, both posts by the news outlet and the individual would be considered professional news content and would be excluded dissemination.

If content used edited pieces of or extracts of professional news content then it would not be considered professional news content.

To support the definition of professional news content, one of the editorial standards or rules listed in paragraph 16(2)(b) must apply. Subparagraphs 16(2)(b)(i) to (v) largely align with the professional standards test set out in the *Treasury Law Amendments (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021*.

Subparagraph 16(2)(b)(iv) does not list a particular code but instead internal editorial standards that are analogous to the rules in subparagraphs (i), (ii) and (iii). To be considered analogous, internal editorial standards should include, at a minimum:

- a mechanism for accepting, adjudicating and notifying complainants of the outcome of complaints about news content, and
- standards relating to the accuracy and impartiality of news content.

A current example of an analogous editorial standard is the *Media, Entertainment and Arts Alliance (MEAA) Journalist Code of Ethics*.

Subparagraph 16(2)(b)(v) provides that additional rules – to which the producer of news content may be subject, in order for content produced by that person to be considered professional news content – may be specified in the digital platform rules. This flexibility is necessary because it would be impossible to exhaustively list the rules, standards and codes of conduct that may in the future come into existence and that may apply to the producers of news content. Subparagraph 16(2)(b)(iv) will capture future rules and standards that are 'analogous' to the existing rules listed at subparagraphs 16(2)(b)(i) to (iii); however, it may be that as the news landscape evolves, the nature of the rules and standards will also evolve, such that future rules and standards can no longer be considered analogous to anything currently listed in paragraph 16(2)(b).

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on the ACMA's rule-making power. Digital platform rules are a legislative instrument for the

purposes of the Legislation Act. This means that the rules would be subject to parliamentary disallowance and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

Subclause 16(3)

Subclause 16(3) provides that, for the purposes of Schedule 9, ***news content*** is content that reports, investigates or explains any of the following:

- issues or events relevant in engaging persons in public debate and in informing democratic decision-making
- current issues or events of public significance for persons at a local, regional, national or international level
- current issues or events of interest to persons.

Content that is not *news content*, such as letters to the editor or cartoons, but is nonetheless produced by a person described by subclause 16(2), would not be considered *professional news content*. However, that content could still be considered *excluded dissemination* if it met the criteria in paragraph 16(1)(a) or 16(1)(c).

DIVISION 2—TRANSPARENCY

A key feature of Schedule 9 is the framework of obligations which aim to promote transparency across the digital communications platform sector. Division 2 of Part 2 of Schedule 9 (in conjunction with the digital platform rules) introduces a range of transparency and accountability obligations, providing a baseline of minimum requirements, outside of any misinformation codes or misinformation standards, with which the digital communications platforms industry must comply.

These core transparency requirements will better inform the public by giving end-users a greater level of visibility with regards to:

- the risk of misinformation and disinformation on digital communications platforms
- the approach being taken by digital communications platform providers regarding misinformation and disinformation on their platforms
- the steps being taken by digital communications platform providers to better enable end-users to identify misinformation and disinformation on digital communications platforms, including enabling end-users to identify the source of content.

The transparency obligations will have a 6-month delayed application (clause 28) to allow digital communications platform providers to prepare for implementation of these measures.

The transparency obligations broadly align with the objectives of the existing voluntary code (the *Australian Code of Practice on Disinformation and Misinformation*) developed for digital communications platforms by DIGI including measures such as:

- public transparency on actions taken to address misinformation and disinformation
- technical assistance or platform features providing end-users greater visibility into the authenticity, accuracy, provenance and source of digital content

- enabling users to make informed choices.[152]

SUBDIVISION A—PUBLICATION

Clause 17—Digital communications platform provider must publish information

Making information available to the public

Subclause 17(1) imposes a requirement on digital communications platform providers to ensure certain information is both available to end-users on the platform and also publicly accessible to others on the digital communications platform provider's website. The intention is that key information pertaining to misinformation and disinformation on digital communications platforms, and the way in which digital communications platform providers are addressing risks relating to misinformation and disinformation, should be made available and accessible to the public.

Report on risk assessment

Paragraph 17(1)(a) places an obligation on a digital communications platform provider to make publicly accessible a report on the outcomes of an assessment by the provider of risks relating to misinformation and disinformation on their platform. The report is to include the outcomes of an assessment of risks arising from both the design or functioning of the platform and risks arising from the use of the platform by end-users.

While the obligation as described in paragraph 17(1)(a) is to *publish* a report on the outcomes of the provider's risk assessment, in order to comply with this obligation, it is implicit that a digital communications platform provider will need to engage in a process to identify and assess risks relating to misinformation and disinformation on its platform (see also clause 19, which provides that digital platform rules may set out further requirements in relation to risk assessments).

Paragraph 17(1)(a) does not require digital communication platform providers to make accessible their complete risk assessments (although, they may choose to do so). In the case of large providers in particular, a risk assessment may be a lengthy document, identifying threats and including confidential information or damaging information about system vulnerabilities, that providers would be unlikely to want to make public. This is why digital communications platform providers are only required to publish a report on the *outcomes* of their risk assessment. At the discretion of the provider, the report could be an in-depth analysis of the key misinformation or disinformation related risks that the provider has identified; or, it could be a high-level summary of those risks.

The purpose of requiring digital communications platform providers to make accessible a report on the outcomes of a risk assessment, is to require providers to be proactive about conducting a risk assessment in relation to misinformation and disinformation on their platform, and to be transparent as to the outcome of that risk assessment. Any deficiencies in the assessment identified from the report published under paragraph 17(1)(a), or through further information which the ACMA may compel under clause 33 for example, may inform the ACMA's actions in relation to the development of a code or the creation of a standard.

[152] Objectives 1, 4 and 7 of the *DIGI Code* (n 2).

The report in paragraph 17(1)(a) must also meet any requirements prescribed by the digital platform rules.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that they would be subject to parliamentary disallowance, and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

Allowing additional requirements for the risk assessment report to be stipulated in the digital platform rules is necessary for a number of reasons. First, it allows the ACMA flexibility to consider the risk assessment reports made available by digital communications platform providers pursuant to paragraph 17(1)(a), and then – on the basis of those reports – to form a view on the need for further requirements to be stipulated in digital platform rules. Second, it allows the ACMA to elaborate on the nature of the obligation to publish a risk assessment report, in response to the evolving risk landscape. For example, the types of information that should be covered in a summary. And third, pursuant to subsection 33(3A) of the Acts Interpretation Act (which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character with respect to particular matters, that includes the power to make, grant or issue such an instrument with respect to only some of those matters) the ACMA may make digital platform rules setting out requirements relating to risk assessment reports that apply only to particular digital communications platform providers. This allows the ACMA to, if necessary, impose more onerous requirements on high-risk digital communications platforms, and lesser requirements on low-risk platforms.

Policy or policy approach in relation to misinformation and disinformation

Paragraph 17(1)(b) provides that the information a digital communications platform provider must make publicly accessible includes either: the provider's current policy in relation to misinformation and disinformation on the platform; or information on the provider's current policy approach in relation to misinformation and disinformation on the platform. In accordance with section 23 of the Acts Interpretation Act, the reference to the provider's current 'policy' in relation to misinformation and disinformation should be read as also referring to 'policies'. Implicit in this requirement is that the provider therefore must either have a current policy on how it manages misinformation and disinformation on its platform, or has to be able to articulate its current policy approach.

The obligation described by paragraph 17(1)(b) is intentionally broad, and it could be satisfied in multiple ways. A digital communications platform provider could satisfy the obligation by publishing one single policy specifically addressing the steps it takes to manage misinformation and disinformation on its platform. Alternatively, a provider may satisfy the obligation by publishing a number of policies that relate in different ways to misinformation and disinformation on the platform – for example, a provider's terms of use, its policy on misleading and deceptive identities, its policy on handling complaints including complaints of misinformation and disinformation, and information about the provider's approach to recommending, promoting or blocking content. Alternatively, if a provider does not have any policies in relation to misinformation or disinformation, or has such policies but opts not to make those policies publicly available, the obligation described by paragraph 17(1)(b) could alternatively be satisfied by the provider publishing its 'policy approach' to misinformation

and disinformation. In the case of very small or new providers, in particular, this could be – for example – a statement on the provider's website, setting out in broad terms the approach the provider will take to misinformation and disinformation on its platform. Paragraph 17(1)(b) does not set any minimum standards regarding a provider's policy or policies, or policy approach, to misinformation and disinformation. Rather, the intent is that end-users will have access to a base level of information about what all digital communications platform providers are doing about misinformation and disinformation on their platforms; and moreover, that the ACMA will also be able to use this information to, if necessary, inform the development of misinformation codes and standards, or digital platform rules in relation to complaints, for example.

Paragraph 17(1)(b) does not require a digital communications platform provider to periodically update its policy or policy approach to misinformation and disinformation on the platform. However, digital communications platform providers are required to publish their *current* policy or policy approach. This means that if a provider *does* update its policy or policies in relation to misinformation or disinformation, with the result that the previously published iteration of that policy or policy approach is no longer current, the provider would be required to publish the updated policy or policy approach.

The requirement at paragraph 17(1)(b) that the providers of digital communications platforms publish their policy or policy approach in relation to misinformation and disinformation responds to an issue identified in numerous studies on misinformation and disinformation online, including by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: namely, that many digital service providers do not share 'precise and meaningful information about action taken to address misinformation and disinformation', and that lack of transparency regarding companies' content moderation systems and processes is 'disempowering for users and denies agency'.[153]

The requirement to publish policies on managing misinformation and disinformation aligns with recommendations made in a series of reports by UN and regional human rights experts on disinformation and the freedom of expression. In 2017, for example, a joint declaration on 'freedom of expression and "fake news", disinformation and propaganda' by UN and regional human rights experts recommended that 'intermediaries' (including digital communications platform providers) should:

> take effective measures to ensure that their users can both easily access and understand any policies and practices, including terms of service, they have in place for [restricting content], including detailed information about how they are enforced, where relevant by making available clear, concise and easy to understand summaries of or explanatory guides to those policies and practices.[154]

The 2021 report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression similarly recommended that companies 'should adopt clear, narrowly defined content and advertising policies on disinformation and

---

[153] Khan, *Disinformation and Freedom of Expression* (n 18) paras 80-81.

[154] UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda* (3 March 2017) <JointDeclaration3March2017.doc (live.com)> ('*Joint Declaration on Freedom of Expression*').

misinformation', and 'ensure that all policies are easily accessible and understandable by users'.[155] Similarly again, the 2022 report of the UN Secretary-General on countering disinformation for the promotion and protection of human rights and fundamental freedoms called on 'technology enterprises' to 'disclose policies and practices relevant to countering disinformation, including mitigating measures such as removals, labelling, suspension of accounts, demonetisation and de-amplification of content', and 'detailed information on how these measures are taken across geographical areas and languages'.[156]

Media literacy plan

Paragraph 17(1)(c) provides that the information a digital communications platform provider must make publicly accessible includes a current media literacy plan for their platform. Implicit in this requirement is that the provider have a media literacy plan.

A media literacy plan is defined in clause 2 as 'a plan setting out measures the digital communications platform provider of the platform will take to enable end-users to better identify misinformation and disinformation on the platform, including to enable end-users to identify the source of content disseminated on the platform (particularly content that purports to be authoritative or factual).'

A digital communications platform provider's media literacy plan could include measures implemented by the platform, whether through operational, technical, functional or design elements, to provide greater visibility for end-users of the origin and source of the content on the digital communications platform. This could include guidance material to assist end-users to identify reliable, authoritative information sources, or measures communicating caveats or content qualifications the platform may have placed on suspect content, such as flags, content advisories or notices reflecting complaints, disputes or fact-checking undertaken on suspect content. Other examples of measures that could be included in a plan would be information to end-users on watermarking and verification of content as artificially generated content, educational resources to assist end-users with critically evaluating content or digital prompts such as 'think before you share' and links to independent fact-checking organisations through platform algorithms.

The nature and content of each media literacy plan will depend significantly on the type of digital communications platform, and the industry involved, and is a matter for the digital communications platform provider.

The purpose of the requirement is to complement broader media literacy initiatives by Government. This recognises that digital communications platform providers bear considerable responsibility for minimising serious harms from misinformation and disinformation content circulating on their platforms, and media literacy is a recognised, important mechanism to tackle this issue.

The requirement for digital communications platform providers to publish a media literacy plan is also premised on the understanding that if users of digital communications platforms are unable to identify misinformation or disinformation, they are more likely to act on that content, either harming themselves (for example, by acting on content that promotes a

[155] Khan, *Disinformation and Freedom of Expression* (n 18) para 98.
[156] *Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms: Report of the Secretary-General,* UN Doc A/77/287 (12 August 2022) para 61.

harmful medical treatment option) or harming others (for example, by acting on content that falsely accuses another individual of a heinous crime). End-users who are unable to identify misinformation are also more likely to disseminate that content to others, in the belief that it is true. Thus, increasing media literacy reduces the likelihood that content disseminated on digital communications platforms will result in serious harm.

Numerous academic studies as well as reports by international and regional bodies, institutions and human rights experts have highlighted the importance of media literacy as a way to combat misinformation and disinformation without burdening the right to freedom of expression.[157] This is because media literacy initiatives build the resilience of end-users to misinformation and disinformation, while avoiding the risk of 'governments or private actors wielding the power to determine what is truthful'.[158] In 2021, the UN General Assembly passed a resolution affirming that 'media and information literacy' can help ensure 'that the fight against disinformation and misinformation promotes and does not infringe on individuals' freedom of expression and access to information'.[159]

A recent study by the Australian News and Media Research Centre (NMRC) found that 68 percent of Australians had a 'low or very low' level of news literacy. 'News literacy' was measured by asking questions about the operations of news outlets and news organisations, and the way in which decisions are made about the profiling of news stories on Facebook. This is not the same as 'media literacy', as that term is used in paragraph 17(1)(c), but it seems reasonable to assume that end-users with higher news literacy will also be more media literate. The NMRC study found that people who rely on social media for news have lower levels of news literacy than those who rely on traditional news sources, and it suggested that news consumers with low news literacy may find it more difficult to identify misinformation than those with higher news literacy. [160]

The requirement that digital communications platform providers have a media literacy plan aligns with the recommendations made by numerous international and regional human rights experts and UN bodies. The 2021 General Assembly resolution referred to above called on Member States to 'develop and implement policies, action plans and strategies related to the promotion of media and information literacy'. That same resolution also called on social media platforms to 'promote media and information literacy, as a way to empower all people and facilitate digital inclusion and global connectivity, and to assist in the fight against disinformation and misinformation'.[161] The 2017 Joint Declaration by UN and regional human rights experts on disinformation and the freedom of expression similarly called on States to take measures to promote media and digital literacy.[162] The UN Secretary-General's

[157] Fernando Nunez, 'Disinformation Legislation and Freedom of Expression' (2020) 10 *UC Irvine Law Review* 783; Khan, *Disinformation and Freedom of Expression* (n 18) para 94; Lili Levi, 'Media Literacy Beyond the National Security Frame' (2020) 4 *Utah Law Review* 941; Tessa Jolls and Michele Johnsen, 'Media Literacy: A Foundational Skill for Democracy in the 21st Century' (2018) 69 *Hastings Law Journal* 1379; Dana Sirbu, 'Media Literacy as a Response to Fake News' (2019) 21 *Romanian Intelligence Studies Review* 141; Directorate-General for Communication Networks, Content and Technology, European Commission (n 64); *Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms: Report of the Secretary-General* (n 156) para 34.
[158] Nunez (n 157) 785.
[159] GA Res 75/267, UN Doc A/RES/75/267 (29 March 2021).
[160] Sora Park et al, *Digital News Report: Australia 2024* (University of Canberra, June 2024) <https://www.canberra.edu.au/research/faculty-research-centres/nmrc/digital-news-report-australia> 43.
[161] GA Res 75/267, UN Doc A/RES/75/267 (29 March 2021) paras 3, 8.
[162] *Joint Declaration on Freedom of Expression* (n 154) para 3(e).

2022 report on disinformation concluded that 'countering disinformation requires lasting investment in building societal resilience and media and information literacy, thereby empowering individuals to identify, critically analyse and counter disinformation, with a view to enabling their full and effective participation in public affairs'.[163]

Similar to the obligation in paragraph 17(1)(b) to publish a policy or policy approach in relation to misinformation and disinformation, paragraph 17(1)(c) requires digital communications platform providers to ensure that their *current* media literacy plan is accessible to the public. This means that if a provider updates its media literacy plan, with the result that the previously published iteration of that plan is no longer current, the provider would be required to publish the updated plan.

Other information (other than source code) specified in the digital platform rules

Paragraph 17(1)(d) provides that the information a digital communications platform provider must make publicly available also includes any information that is specified in the digital platform rules. Such rules must not include any requirement to publicly disclose source code.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on the ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that they would be subject to parliamentary disallowance, and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

Allowing the ACMA to make digital platform rules specifying additional types of information that digital communications platform providers are required to make publicly available is necessary for a number of reasons.

First, this enables the ACMA to expand the publication requirement based on information made available to the ACMA pursuant to the operation of other provisions in Schedule 9. In particular, prior to making a digital platform rule defining a new type of information that digital communications platform providers are required to make publicly available, the ACMA would be expected to consider the existing information being made available by digital communications platform providers pursuant to clause 17, and on that basis to form a view regarding whether there is an additional type of information that, if made available, could assist to protect the Australian community from serious harm from misinformation or disinformation on digital communications platforms.

Second, allowing the ACMA to make digital platform rules specifying additional types of information that digital communications platform providers should make publicly available means that the publishing obligation can be adapted in response to the evolving digital landscape. For example, if new technologies radically change the way in which the digital platform industry can identify and manage misinformation (for example, as a result of greater automation or artificial intelligence), the ACMA may consider it appropriate that digital communications platform providers be required to publicly disclose whether or not, and/or how, they are making use of those new technologies.

[163] *Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms: Report of the Secretary-General* (n 156), para 58.

Third, as elaborated in the explanation to clause 82, the ACMA's rule-making power is to be interpreted in accordance with subsection 33(3A) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character with respect to particular matters, the power shall be construed as including a power to make, grant or issue such an instrument with respect to some only of those matters, or with respect to a particular class or particular classes of those matters, and to make different provisions with respect to different matters or different classes of matters. This means that the ACMA may, for example, make digital platform rules specifying a new type of information required to be made publicly available by only one class of digital communications platform provider, or by a section or sections of the digital platforms industry. This allows the ACMA to, for purposes of subclause 17(1), if necessary impose more onerous requirements on high-risk digital communications platforms, and lesser requirements on low-risk platforms.

Updates to risk assessments

Subclause 17(2) provides that if the digital communications platform provider updates its assessment of risks related to misinformation and disinformation, paragraph 17(1)(a) applies in relation to the provider's most recent assessment. This means that while clause 17 does not require digital communications platform providers to *periodically* identify and assess risks and report on the outcomes of such an assessment – rather, this is a one-off obligation – if a provider *does* update its assessment of risks, the provider must make a report of the outcomes of that updated risk assessment publicly available.

However, clause 19 provides that digital platform rules may require digital communications platform providers to update their risk assessments at times (e.g. at certain frequencies), or in circumstances specified in the rules (e.g. in response to an event that has triggered a marked increase of misinformation and disinformation on platforms e.g. a pandemic, or outbreak of war). The rules can also require the risk assessment to cover specified matters (e.g. matters that a digital platform provider themselves may not have identified in their risk assessment). Accordingly, the rules could, for example, require certain, high-risk digital communications platform providers to update their risk assessments, and if they were required to do so, subclause 17(2) would require the report to be updated.

Information to which the publishing obligation does not apply

Subclause 17(3) lists certain categories of information that a digital communications platform provider is not required to make publicly available.

Paragraph 17(3)(a) provides that the requirement to make information publicly available does not apply in relation to protected information. Protected information is defined in clause 2 of Schedule 9. It covers a trade secret or other information that has a commercial value that would be (or could reasonably be expected to be) destroyed if the information were publicly disclosed. Further explanation regarding that definition is provided in the explanation to clause 2.

Paragraph 17(3)(b) provides moreover that the requirement to make information publicly available does not apply to personal information (within the meaning of the Privacy Act), and paragraph 17(3)(c) provides that it does not apply to any information the disclosure of which

the provider reasonably considers might cause a significant security vulnerability for the platform or increase misinformation or disinformation. Pursuant to these exemptions, a digital communications platform provider would not be required to publish, for example:

- data protection protocols, if the publication of those protocols might compromise a platform's security arrangements (subparagraph 17(3)(c)(i))
- particulars of a platform's approach to managing misinformation and disinformation which if released publicly might be exploited to amplify the proliferation of, or undermine attempts to counter the spread of, misinformation or disinformation (subparagraph 17(3)(c)(ii)).

Making information available to the ACMA

Subclause 17(4) provides that if a digital communications platform provider fails to comply with subclause 17(1) (or would have failed to comply, if subclause 17(3) were disregarded) in relation to particular information, it must give to the ACMA a copy of that information, together with an explanation of why the information is not publicly accessible. This might include, for example, any information that has not been published because it is a trade secret, or would otherwise hold commercial value that would be diminished if published. It would also include information, that, if made public, would create a significant security issue or might publicly reveal an operational, technical or systems vulnerability that could be exploited to increase misinformation or disinformation, as mentioned in subclause 17(3). The ACMA would have the discretion to publish a provider's rationale for not making certain information publicly accessible (see paragraph 38(3)(a)).

If a digital communications platform provider fails to comply with subclause 17(1), it must provide the ACMA with the information that it has failed to publish within 60 days of that failure, or in other words, within 60 days of the date at which a digital communications platform provider is first required to publish certain information (pursuant to subclause 17(1)) but does not do so.

Pursuant to clause 28, the obligations under clause 17 to publish information and to provide information to the ACMA in the event of failure to publish do not come into effect until 6 months after Schedule 9 commences. The operation of these obligations in relation to platforms in existence at the time Schedule 9 commences, as well as to digital communications platforms that come into existence after the commencement of Schedule 9, is set out in the following table.

Information	**Date at which obligation to publish arises**	**Date at which obligation to make information available to ACMA arises**
Policy or policy approach in relation to misinformation, risk assessment report and media literacy plan	Six months after commencement of Schedule 9 (see clause 28). For platforms that come into existence six or more months after the commencement of Schedule 9, the day those platforms come into existence.	For platforms in existence at the time of the commencement of Schedule 9 or within six months thereof, six months after the commencement of Schedule 9 (see clause 28) + 60 days. For platforms that come into existence six or more months after the commencement of Schedule 9, 60 days after the platform comes into existence.

Updates to the above	At the time of the update or six months after the commencement of Schedule 9, whichever is later.	Six months after the commencement of Schedule 9 + 60 days, or 60 days after the update, whichever is later.

Subclause 17(5) provides that a digital communications platform provider may notify the ACMA that its information referred to in subclause 17(4) contains protected information. Protected information is defined in clause 2 of Schedule 9. It covers a trade secret or other information that has a commercial value that would be (or could reasonably be expected to be) destroyed if the information were publicly disclosed. Further explanation regarding that definition is provided in the explanation to clause 2.

A notice provided for the purposes of subclause 17(5) must identify which information is protected information and explain why. This will enable the ACMA to comply with clauses 39 and 40, which impose limitations on the ACMA's power to publish protected information. Clause 39 provides that the ACMA must not publish protected information except in certain circumstances. Clause 40 provides that if the ACMA has been notified that certain information is protected information, but the ACMA nevertheless proposes to publish that information, the ACMA must give the provider a written notice of its proposal to publish and an invitation to make submissions to the ACMA in relation to that proposal.

However, the requirement in subclause 17(5) does not limit subclause 17(4). That is to say, even if the digital communications platform provider notifies the ACMA that information that would otherwise be required to be made available pursuant to subclause 17(1) contains protected information, it still must provide the ACMA with a copy of that information. This subclause is similar to subclauses 30(11), 33(5) and 34(6).

The note to subclause 17(5) draws attention to clauses 39 and 40, and the limitations on the publication of protected information under clause 38.

Civil penalty provisions

Subclause 17(6) provides that subclauses 17(1) (requirement to publish certain information) and 17(4) (making information available to the ACMA) are civil penalty provisions.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that the maximum penalty for a contravention of a civil penalty provision in Division 2 of Part 2 of Schedule 9 (including subclauses 17(1) and 17(4)) is 5,000 penalty units for a body corporate, and 1,000 penalty units for a person who is not a body corporate.

Clause 72 provides that the contravention of subclause 17(1) and the contravention of subclause 17(4) are both separate contraventions of the subclauses in question for each day the contravention continues. Clause 73 provides that subclauses 17(1) and 17(4) are designated infringement notice provisions and clause 74 provides that the ACMA can issue a warning in relation to their contravention.

Clause 18—Remedial directions—contravention of requirement to publish information

Clause 18 applies if the ACMA is satisfied that a digital communications platform provider has contravened, or is contravening, subclause 17(1) or 17(4) (subclause 18(1)).

Subclause 18(2) provides that the ACMA may give the provider a written direction requiring the provider to take specified action directed towards ensuring that the provider does not contravene these provisions or is unlikely to do so in the future. Subclause 18(2) is to be interpreted in light of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument. Thus, the ACMA would be able to vary the requirements in a written direction provided pursuant to subclause 18(2), or revoke the direction, once provided.

Decisions to issue, vary, or refuse to revoke, a remedial direction under subclause 18(2) are reviewable by the ART (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 75 provides that a direction under subclause 18(2) is taken to be a notice under Schedule 9 for the purposes of the BSA and the ACMA Act. Clauses 77 and 78 provide for the service of notices under Schedule 9 to the BSA.

Subclause 18(3) provides that a digital communications platform provider must not contravene a direction under subclause 18(2).

Subclause 18(4) provides that subclause 18(3) is a civil penalty provision.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that the maximum penalty for a contravention of a civil penalty provision in Division 2 of Part 2 (which includes subclause 18(3)) is 5,000 penalty units for a body corporate and 1,000 penalty units for persons who are not body corporates.

Clause 72 provides that the contravention of subclause 18(3) is a separate contravention for each day the contravention continues.

SUBDIVISION B—RISK MANAGEMENT

Clause 19—ACMA may make digital platform rules in relation to risk management

Risk assessments

Paragraph 19(1)(a) provides that the digital platform rules may require digital communications platform providers to update their assessments of risks relating to misinformation and disinformation on the platforms they provide, at times (e.g. at certain frequencies), or in circumstances specified in the rules (e.g. in response to an event that has triggered a marked increase of misinformation and disinformation on platforms e.g. a pandemic, or outbreak of war).

Rules under paragraph 19(1)(b) could also require the platform's risk assessments to cover certain specified matters (e.g. matters that a digital communications platform provider themselves may not have identified in their risk assessment). For example, the ACMA could make rules that apply only to certain high-risk digital communications platform providers (see subsection 33(3A) of the Acts Interpretation Act). If the ACMA made such rules, subclause 17(2) would require the digital communications platform provider's report on the outcomes of the risk assessment to be updated.

The power to make rules under paragraph 19(2)(b) does not extend to matters such as specifying *how* the risk assessment process underlying the report is actually to be undertaken by the digital communications platform provider, as opposed to the types of matters to be covered. The process of the risk assessment itself is entirely a matter for the digital communications platform provider.

Risk management plans

Paragraphs 19(c), (d) and (e) provide the ACMA with the discretion to make digital platform rules to:

- require digital communications platform providers to have risk management plans for risks relating to misinformation and disinformation (paragraph (c))
- require those risk management plans to be prepared at times, or in circumstances, specified in the rules (paragraph (d))
- require those risk management plans to state the steps (if any) being taken by digital communications platform providers in relation to risks (in respect of misinformation or disinformation) identified by providers or specified in the rules (paragraph (e))

The 'management plan' referred to in paragraphs 19(c) to (e) is intended to mean the processes, strategies and risk treatments which the digital communications platform provider will implement to minimise risks relating to misinformation or disinformation on their platform (if any).

The ACMA would have discretion to require digital communications platform providers to prepare a plan at times, or in circumstances specified in the rules (e.g. in response to an event that has triggered a marked increase of misinformation and disinformation on platforms e.g. a pandemic, or outbreak of war).

The ACMA would also have the discretion to make rules requiring platforms to state in their plan, what steps (if any) the digital communications platform provider is taking with respect to particular risks, that a provider may or may not have identified as part of its risk assessment.

The ACMA could target the application of these rules to certain digital communications platform providers only (see subsection 33(3A) of the Acts Interpretation Act). This could be certain sections of the digital platform industry that have larger numbers of end-users and/or who pose a higher risk due to the nature of their services or their features, for example.

The purpose of these rules is not to empower the ACMA to require the digital communications platform provider to take particular action in relation to specified risks, but simply to require the provider to specify what action, or lack of action, it is taking. In other words, the rule-making power does not extend to the ACMA requiring *how* a digital

communications platform provider's management plan is to address or require action in relation to risks of misinformation and disinformation on the platform; the content of the risk mitigation measures in the plan is a matter for the digital communications platform provider.

As with the other obligations in Division 2 of Part 2, the purpose of the rule-making power is to require digital communications platform providers to be transparent about how they are managing misinformation and disinformation on their platforms. Through requiring this transparency, the ACMA would be able to use information gleaned from Division 2 and from the ACMA's other information powers in Subdivision A and B of Division 3 for example, to inform itself on the adequacy of existing measures taken by digital communications platform providers in relation to misinformation and disinformation. It can use this information to inform itself on whether further action to request a misinformation code or determine a standard is required, and if so, the kinds of matters that should be dealt with in the code or standard.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on the ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that they would be subject to parliamentary disallowance, and would be registered on the Federal Register of Legislation.

Clause 20—Compliance with digital platform rules regarding risk management

Subclause 20(1) provides that a digital communications platform provider must not contravene digital platform rules made for the purposes of clause 19. This is a civil penalty provision (per subclause 20(2)).

Under clause 72, each day during which a contravention of the civil penalty provision continues is counted as a separate contravention.

Subclause 20(1) is also a designated infringement notice provision (per clause 73), and the ACMA may issue a warning if satisfied that a person has contravened the provision (per clause 74).

Clause 21—Remedial directions—contravention of digital platform rules regarding risk management

Subclause 21(1) states that clause 21 applies if the ACMA is satisfied that a digital communications platform provider has contravened, or is contravening, digital platform rules made for the purposes of clause 19 (rules in relation to risk management).

Subclause 21(2) provides for the ACMA to give the provider a remedial direction requiring the provider to take specified action directed towards ensuring that the provider does not contravene digital platform rules made for the purposes of clause 19, or is unlikely to contravene those rules, in the future.

Decisions to issue, vary, or refuse to revoke, a remedial direction under subclause 21(2) are reviewable by the ART (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 75 provides that a remedial direction under subclause 21(2) is taken to be a notice under Schedule 9 for the purposes of the BSA and the ACMA Act. Clauses 77 and 78 provide for the service of notices under Schedule 9 to the BSA.

The digital communications platform provider would be required to comply with the remedial direction (per subclause 21(3)). Failure to do so could give rise to a civil penalty (per subclause 21(4)).

Clause 21 is to be interpreted in light of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument. Thus, the ACMA would be able to vary the requirements in a written direction given pursuant to subclause 21(2), or revoke the direction, once given.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that for persons who are body corporates, the maximum penalty for a contravention of a civil penalty provision in Division 2 of Part 2 of Schedule 9 (which includes subclause 21(3)) is 5,000 penalty units and for persons who are not body corporates, the maximum penalty is 1,000 penalty units.

Clause 72 provides that that the contravention of subclause 21(3) is a separate contravention for each day the contravention continues.

SUBDIVISION C—MEDIA LITERACY PLAN

Clause 22—ACMA may make digital platform rules in relation to media literacy plan

Clause 22 empowers the ACMA to make digital platform rules imposing certain requirements relating to ***media literacy plans*** on digital communications platform providers. Specifically, the digital platform rules could require:

- digital communications platform providers to update media literacy plans for the digital communications platforms they provide, at times, or in circumstances, specified in the rules (paragraph 22(a))
- those media literacy plans to state the media literacy tools digital communications platform providers are using in relation to the risks of misinformation and disinformation they have identified or that are specified in the rules (paragraph 22(b)), and
- providers to give the ACMA assessments of the effectiveness of the media literacy tools mentioned in their media literacy plan (paragraph 22(c)).

A media literacy tool can be (depending on the platform) guidance material, educational resources or user-interface, platform design or other features which guide, alert or otherwise assist an end-user to assess the reliability of content and determine whether content may be misinformation or disinformation. This could include advisory videos, or it may also include design elements (colour schemes, icons, flags or notifications) in a user-interface conveying information on currency, source or provenance of information or whether content is the subject of a complaint or dispute.

The ACMA may exercise its discretion to apply rules only in relation to some digital communications platform providers (see subsection 33(3A) of the Acts Interpretation Act).

For example, it may decide it is appropriate to apply these rules to digital communications platform providers who have larger numbers of end-users, or who have particular features or functions that make them high-risk, to ensure there is no undue regulatory burden on low-risk platforms.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on the ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that they would be subject to parliamentary disallowance, and would be registered on the Federal Register of Legislation.

As with the other obligations in Division 2 of Part 2, the purpose of the rule-making power is to enable the ACMA to obtain further information in addition to what it may already obtain in Division 2 and under its other information powers in Subdivision A and B of Division 3, for example, to inform itself on the adequacy of existing measures taken by digital communications platform providers in relation to managing the risk of misinformation and disinformation on their platforms. The ACMA could use this information to inform a decision as to whether further action to request a misinformation code or determine a standard is required, and if so, the kinds of matters that should be dealt with in the code or standard.

Clause 23—Compliance with digital platform rules regarding media literacy plan

A digital communications platform provider must comply with a digital platform rule made under clause 22 (per subclause 23(1)). Failure to do so is a civil penalty provision (per subclause 23(2)).

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that for persons who are body corporates, the maximum penalty for a contravention of a civil penalty provision in Division 2 of Part 2 of Schedule 9 (which includes subclause 23(1)) is 5,000 penalty units, and for persons who are not body corporates, the maximum penalty is 1,000 penalty units.

Clause 73 provides that subclause 23(1) is a designated infringement notice provision and clause 74 provides that the ACMA can issue a warning in relation to its contravention.

Clause 24—Remedial directions—contravention of digital platform rules regarding media literacy plan

Pursuant to clause 24, the ACMA may issue remedial directions to digital communications platform providers for the purposes of enforcing digital platform rules in relation to media literacy plans.

Subclause 24 applies if the ACMA is satisfied that a digital communications platform provider has contravened, or is contravening, digital platform rules made for the purposes of clause 22 (per subclause 24(1)).

Subclause 24(2) provides that the ACMA may give the digital communications platform provider a written direction requiring the provider to take specified action directed towards ensuring that the provider does not contravene these digital platform rules or is unlikely to do so in the future. Subclause 24(2) is to be interpreted in light of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue

any instrument of a legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument. Thus, the ACMA would be able to vary the requirements in a written direction given pursuant to subclause 24(2), or revoke the direction, once given.

Decisions to issue, vary or refuse to revoke, a remedial direction under subclause 24(2) are reviewable by the ART (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 75 provides that a direction under subclause 24(2) is taken to be a notice under Schedule 9 for the purposes of the BSA and the ACMA Act. Clauses 77 and 78 provide for the service of notices under Schedule 9 to the BSA.

Subclause 24(3) provides that a digital communications platform provider must not contravene a direction made under subclause 24(2).

Subclause 24(4) provides that subclause 24(3) is a civil penalty provision.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that for persons who are body corporates the maximum penalty for a contravention of a civil penalty provision in Division 2 of Part 2 (which includes subclause 24(3)) is 5,000 penalty units and for persons who are not body corporates the maximum penalty is 1,000 penalty units.

SUBDIVISION D—COMPLAINTS

Clause 25—ACMA may make digital platform rules in relation to complaints and dispute handling

Pursuant to subclause 25(1), the ACMA may make digital platform rules for or in relation to complaints and dispute handling processes for misinformation complaints.

Subclause 25(2) provides a non-exhaustive list of matters that may be provided for in such rules. The digital platform rules could, for example, require digital communications platform providers to implement and maintain complaints and disputes handing processes for misinformation complaints, or they could set minimum standards for complaints and dispute handling processes. The digital platform rules may also require digital communications platform providers to publish, or provide to the ACMA, information regarding their complaints and dispute handling process, or regarding misinformation complaints, or responses to those complaints. Such information could include, for example, the time taken by providers to respond to complaints.

However, subclause 25(3) provides that rules made for the purposes of clause 25 must not require a digital communications platform provider to publish certain types of information. Under paragraph 25(3)(a), this includes protected information (which is defined in clause 2 to mean a trade secret or other information that has a commercial value that would be, or could reasonably be expected to be, destroyed if the information were publicly disclosed). Paragraph 25(3)(b) provides that a digital communications platform provider must not be required to publish personal information within the meaning of the Privacy Act. Finally, a digital communications platform provider must not be required to publish information the

disclosure of which the provider reasonably considers might cause a significant security vulnerability for the platform or increase misinformation or disinformation (per paragraph 25(3)(c)).

This clause responds to the recommendation in the fifth interim report of the Digital Platforms Services Inquiry, that digital communications platforms develop improved dispute resolution pathways.164

Misinformation complaint is defined in clause 2 of Schedule 9. It means a complaint in relation to misinformation or disinformation on a digital communications platform (or dissemination that is potentially misinformation or disinformation on a digital communications platform), or in relation to content removed from a digital communications platform on the basis that its dissemination using the platform is misinformation or disinformation on the platform.

Subclause 25(1) should be read together with subsection 33(3A) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character with respect to particular matters, the power shall be construed as including a power to make, grant or issue such an instrument with respect to only some of those matters or with respect to a particular class or particular classes of those matters and to make different provisions with respect to different matters or different classes of matters. This means that it would be open to the ACMA to make digital platform rules regarding complaints and disputes handling processes, for example, that apply to all digital communications platform providers, or that apply only to some digital communications platform providers. This flexibility allows the ACMA to ensure that the regulatory burden on low-risk digital communications platform providers is not unduly onerous.

The ACMA's power to make digital platform rules is elaborated in clause 82. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that the rules would be subject to parliamentary disallowance and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act. Subclause 82(2) sets out, for the avoidance of doubt, some of the limits on the ACMA's power to make digital platform rules.

Allowing the requirements regarding complaints and dispute handling processes to be prescribed by the ACMA in digital platform rules under clause 25 also allows the requirements to be informed by information made available to the ACMA pursuant to the operation of other provisions in Schedule 9. Specifically, prior to making digital platform rules regarding complaints and dispute handling processes, it would be open to the ACMA to consider, for example:

- information provided by digital communications platform providers regarding the risk of misinformation and disinformation on their platforms, made available pursuant to paragraph 17(1)(a)
- digital communications platform providers' existing policies and policy approaches to misinformation and disinformation, made available pursuant to paragraph 17(1)(b)

164 Australian Competition and Consumer Commission, Commonwealth of Australia, *Digital Platform Services Inquiry: Interim Report No 5 – Regulatory Reform* (September 2022) <Digital platform services inquiry - September 2022 interim report.pdf (accc.gov.au)>.

- any additional information regarding misinformation and disinformation on digital communications platforms, obtained by the ACMA pursuant to its information powers in Subdivision A and B of Division 3 of Part 2.

The rule-making power would enable the ACMA to ensure that the requirements in relation to complaints and dispute handling are informed by the voluntary internal dispute resolution code, that the Government is currently working with the digital platforms industry to develop. It allows flexibility for the requirements to be adapted as necessary to adjust to and align with evolving regulation in other contexts such as consumer protection, online safety and other relevant international regulation.

Clause 26—Compliance with digital platform rules regarding complaints and dispute handling

Subclause 26(1) provides that a digital communications platform provider must not contravene digital platform rules made for the purposes of clause 25.

Subclause 26(2) provides that subclause 26(1) is a civil penalty provision.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that for persons who are body corporates, the maximum penalty for a contravention of a civil penalty provision in Division 2 of Part 2 of Schedule 9 (which includes subclause 26(1)) is 5,000 penalty units and for persons who are not body corporates, the maximum penalty is 1,000 penalty units.

Clause 72 provides that the contravention of subclause 26(1) is a separate contravention for each day the contravention continues.

Clause 73 provides that subclause 26(1) is a designated infringement notice provision and clause 74 provides that the ACMA can issue a warning in relation to its contravention.

Clause 27—Remedial directions—contravention of digital platform rules regarding complaints and dispute handling

Subclause 27(1) provides that clause 27 applies if the ACMA is satisfied that a digital communications platform provider has contravened, or is contravening, digital platform rules made for the purposes of clause 25 (i.e. in relation to complaints and dispute handling).

Pursuant to subclause 27(2), the ACMA may issue a remedial direction to the digital communications platform provider requiring them to take specified action directed towards ensuring that the provider does not contravene those digital platform rules or is unlikely to do so in the future.

Subclause 27(2) is to be interpreted in light of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument. Thus, the ACMA would be able to vary the requirements in a written direction provided pursuant to subclause 27(2), or revoke the direction, once provided.

Decisions to issue, vary or refuse to revoke, a remedial direction under subclause 27(2) are reviewable by the ART (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 75 provides that a direction under subclause 27(2) is taken to be a notice under Schedule 9 for the purposes of the BSA and the ACMA Act. Clauses 77 and 78 provide for the service of notices under Schedule 9 to the BSA.

Subclause 27(3) provides that a digital communications platform provider must not contravene a direction under subclause 27(2).

Subclause 27(4) provides that subclause 27(3) is a civil penalty provision.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that for persons who are body corporates, the maximum penalty for a contravention of a civil penalty provision in Division 2 of Part 2 of Schedule 9 (which includes subclause 27(3)) is 5,000 penalty units and for persons who are not body corporates, the maximum penalty is 1,000 penalty units.

Clause 72 provides that that the contravention of subclause 27(3) is a separate contravention for each day the contravention continues.

SUBDIVISION E—MISCELLANEOUS

Clause 28—Delayed start of requirements in this Division

Clause 28 provides that Subdivisions A to D of Division 2 of Part 2 do not apply in relation to a digital communications platform provider until 6 months after the commencement of Schedule 9.

The purpose of this provision is to provide digital communications platform providers with sufficient time to comply with the requirements in Subdivision A of Division 2 of Part 2 of the Bill, and if any rules are made by the ACMA under Subdivisions B to D.

It is the intention that the ACMA would still be able to make rules under clauses 19, 22 and 25 in the first 6 months after the commencement of Schedule 9. However, those rules would not be able to be enforced against a digital communications platform provider until 6 months after that commencement.

Clause 29—Exemptions from this Division

Clause 29 provides that Subdivisions A to D of Division 2 of Part 2 do not apply in relation to a digital communications platform if it is specified in the digital platform rules as exempt from Division 2.

In relation to some of the obligations set out in Division 2, the ACMA already has the power to make digital platform rules to define the scope of those obligations as they relate to particular digital communications platforms (for example clause 22, read together with subsection 33(3A) of the Acts Interpretation Act). Clause 29 supplements these powers by enabling the ACMA to specify classes of digital communications platforms (through the operation of subsection 33(3A) of the Acts Interpretation Act), as exempt from the whole of Subdivisions A to D of Division 2.

The ACMA's power to make digital platform rules is elaborated in clause 82, as are the limits on the ACMA's rule-making power. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that they would be subject to parliamentary disallowance, and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

The purpose of this provision is to enable the ACMA to carve out digital communications platforms from all of the transparency provisions in Subdivisions A to D of Division 2 – the publication, risk management, media literacy plan and complaints provisions. It would be open to the ACMA, for example, to carve out (currently) low-risk digital communications platforms from the scope of the transparency provisions, however keep them in scope for the other provisions of the Bill (e.g. the information gathering powers in Division 3 of Part 2).

Given the nature and features of digital communications platforms are constantly and rapidly evolving, including through new generative artificial intelligence technology, it is necessary to have flexibility for the ACMA to carve out (and back in, if necessary, through revocation of an exemption in reliance on subsection 33(3) of the Acts Interpretation Act), digital communications platforms, through disallowable digital platform rules. Allowing the ACMA to use the digital platform rules to exempt particular digital communications platforms from all of the obligations set out in Division 2 of Part 2 is necessary to allow for future evolutions in the digital landscape.

DIVISION 3—INFORMATION

Division 3 of Part 2 of Schedule 9 provides the ACMA with powers to make digital platform rules to place record-keeping and reporting requirements on digital communications platform providers in relation to misinformation and disinformation (Subdivision A). It also enables the ACMA to gather certain information relating to misinformation and disinformation from digital communications platform providers and other persons (Subdivision B). Finally, it enables the ACMA to publish information on its website relating to misinformation and disinformation, in an effort to improve transparency about digital communications platform providers' systems and processes to prevent and respond to misinformation and disinformation, with exceptions for protected information (Subdivision C).

SUBDIVISION A—RECORD KEEPING AND REPORTING

Clause 30—ACMA may make digital platform rules in relation to records

Clause 30 provides the ACMA with the power to make digital platform rules requiring digital communications platform providers to make and retain records relating to:

- misinformation or disinformation on their platforms
- measures they have implemented to prevent or respond to misinformation or disinformation on their platforms.

The rules may also require digital communications platform providers to prepare reports consisting of information contained in those records, and to give any or all of the reports to the ACMA.

This rule-making power is intended to enhance the transparency of digital communications platform providers' management of misinformation and disinformation on their services, and any improvements in such management over time, and to enable the ACMA to access data related to the management of misinformation and disinformation. Clause 30 is modelled in part on the existing record-keeping rules power in Division 3 of Part 27 of the Telecommunications Act.

The ACMA's power to make digital platform rules is elaborated in clause 82. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that the rules would be subject to parliamentary disallowance and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act. Subclause 82(2) clarifies, for the avoidance of doubt, some limitations on the ACMA's power to make digital platform rules.

As expressed in clause 30, the digital platform rules apply generally to digital communications platform providers. However, this clause should be read together with subsection 33(3A) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character with respect to particular matters, the power shall be construed as including a power to make, grant or issue such an instrument with respect to some only of those matters. This means that the ACMA may make digital platform rules which prescribe requirements relating to record keeping or reporting that apply to all digital communications platform providers, or that apply only to a class of digital communications platform providers or to a section or sections of the digital platforms industry. This flexibility allows the ACMA to ensure that the regulatory burden on providers of low-risk digital communications platforms is not unduly onerous.

Records

Subclause 30(1) states that the digital platform rules may require digital communications platform providers to make and retain records relating to the matters outlined in paragraphs 30(1)(a) and (b).

Paragraph 30(1)(a) covers records relating to misinformation or disinformation on digital communications platforms. Paragraph 30(1)(b) covers records relating to measures implemented to prevent or respond to misinformation or disinformation on digital communications platforms, including the effectiveness of the measures. For example, it would be open to the ACMA to make a digital platform rule requiring digital communications platform providers to make and retain records about measures they are taking in relation to content about which they frequently receive misinformation complaints; or it could make a digital platform rule requiring digital communications platform providers to make and retain

records about specific tools or techniques they are using to address misinformation and disinformation, including (but not limited to) labelling, fact-checking, supporting media literacy or providing authoritative information to end-users.

For clarity, the references in paragraphs 30(1)(a) and (b) to, respectively, misinformation or disinformation on digital communications platforms, and measures implemented to prevent or respond thereto, are intended also to include information about the *absence* of misinformation and disinformation and the *absence* of measures taken in response. Thus, pursuant to paragraph 30(1)(b), the digital platform rules may require – for example – a digital communications platform provider that has not implemented any measures to prevent or respond to misinformation and disinformation to make and retain a record regarding its lack of action.

Subclause 30(2) provides that, before the ACMA makes a digital platform rule for the purposes of clause 30 in relation to a digital communications platform, the ACMA must consider the matters in paragraphs 30(2)(a) and (b).

Paragraph 30(2)(a) provides that the ACMA must consider the privacy of end-users before making a digital platform rule in relation to records. This requirement would be particularly important if the ACMA were to make a digital platform rule for the purpose of this clause requiring digital communications platform providers to make and retain records containing personal information, as that term is defined in section 6 of the Privacy Act. This might arise, for example, if the ACMA were to make a digital platform rule requiring a digital communications platform provider to make and retain records of examples of misinformation and disinformation posted by individual end-users that have been removed from the digital communications platform.

When considering the privacy of end-users before making a digital platform rule in relation to records, the ACMA would be expected to consider the extent to which particular records are necessary and reasonable for the purpose of regulating misinformation and disinformation. For example, it is expected that the ACMA would consider the extent to which it may be feasible to use de-identified records to achieve the objectives stated in the legislation, and should ensure that if digital communications platform providers are required to retain records of personal information, these are only required to be retained for the period of time reasonably necessary to achieve those objectives. Any risks to the privacy of end-users would also be minimised by the fact that the rules would not be permitted to require digital communications platform providers to make or retain records of the content of private messages or VoIP communications (subclause 30(3) – see further discussion of that subclause below). In addition, the ACMA must comply with the requirements of the Privacy Act when dealing with personal information, including Australian Privacy Principle 11 (about security of personal information).

Paragraph 30(2)(b) provides that the ACMA must consider whether any proposed rule is required for the performance of the ACMA's functions under paragraphs 10(1)(mb), (mc), (md), (me), (mf), (mg), or (q) of the ACMA Act. The functions in paragraphs 10(1)(mb) to (mg) are inserted into the ACMA Act by Item 2 of Schedule 2 to the Bill. They include functions such as: assisting sections of the digital platform industry to develop misinformation codes; developing standards, monitoring compliance with Schedule 9 to the BSA, misinformation codes, misinformation standards and the digital platform rules; and conducting investigations into, and informing itself, the Minister and the public about,

misinformation and disinformation on digital communications platforms. The function in paragraph 10(1)(q) is about reporting to and advising the Minister in relation to the broadcasting, broadcasting video on demand, internet and datacasting industries.

As mentioned above, subclause 30(3) provides that digital platform rules made for the purposes of this clause must not require digital communications platform providers to make or retain records of the content of private messages or VoIP communications. Private messages are excluded for the purpose of protecting the privacy of Australian end-users. VoIP communications are excluded for privacy and workability purposes.

However, the digital platform rules may still require digital communications platform providers to make or retain records on information *relating to* private messages. For example, the rules could require records to be kept on the number of complaints from individuals about misinformation in private messages on the digital communications platform that the platform provider has received, or measures digital communications platform providers have taken to address misinformation or disinformation on their private messaging applications. This would provide insights into the potential volume of misinformation and disinformation on the service without disclosing the content of the private messages themselves.

Another example is that digital communications platform providers that operate private messaging services could be asked to maintain and provide records about whether (and how) they provide access to authoritative sources of information to their users.

Subclause 30(4) provides that digital communications platform rules may specify the manner and form in which the records are to be made. The digital platform rules may also specify the period for which the records are to be retained. This will allow for consistency in how digital communications platform providers keep records. The rules would facilitate the ACMA being able to design universal metrics and include common retention periods for ease of data analysis, should it wish.

Reporting

Subclauses 30(5) to (9) provide for the digital platform rules to make requirements relating to reporting.

Subclause 30(5) provides that the rules may require digital communications platform providers to prepare reports consisting of information contained in the records. The rules could require such reports to contain a variety of matters related to misinformation and disinformation on digital communications platforms, or the provider's management thereof. Subclause 30(6) provides that the rules may require any or all reports to be given to the ACMA, and subclause 30(7) provides that the rules may specify the manner and form in which reports should be prepared.

Subclause 30(8) provides that the digital platform rules may require reports to be prepared as and when required by the ACMA (paragraph 30(8)(a)); or that they may require periodic reports, at regular intervals to be specified in the digital platform rules (paragraph 30(8)(b)). The provision for the digital platform rules to require reports 'as and when required' by the ACMA enables the ACMA to require reports relating to misinformation and disinformation in relation to – for example – particularly high-risk subject matters, or particularly high-risk events. The ACMA may, for example, require digital communications platform providers to

provide reports on election-related misinformation and disinformation on their platforms in the lead up to Commonwealth elections; or, in the context of a pandemic, the ACMA could require providers to prepare reports on health-related misinformation and disinformation. Conversely, the provision for the digital platform rules to require periodic reports at specified intervals allows the ACMA to, for example, require digital communications platform providers to provide annual reports on measures taken to prevent or respond to misinformation and disinformation.

For the avoidance of doubt, paragraphs 30(8)(a) and (b) are not mutually exclusive. That is to say, the ACMA make may digital platform rules requiring digital communications platform providers to (for example) provide annual reports on measures taken to respond to misinformation and disinformation, as well as (for example) reports on election-related misinformation and disinformation in the lead up to Commonwealth elections.

Subclause 30(9) provides that the digital platform rules may require or permit reports to be prepared in accordance with specified software requirements and specified authentication requirements on a specified kind of data processing device (within the meaning of the Telecommunications Act) or by way of a specified kind of electronic transmission.

Source code and protected information

Subclause 30(10) provides that the digital platform rules must not require digital communications platform providers to prepare reports containing source code. This subclause provides an additional layer of protection for source code, as compared to other types of protected information. This clause only prevents the ACMA from requiring digital communications platform providers to prepare reports *containing* source code. This does not preclude the ACMA from requesting digital communications platform providers to prepare reports *about* a source code or source codes – for example, about whether source codes are being used and why, and about what the source codes being used by a provider are intended to achieve. For example, the ACMA could require information about what type of content a provider's recommender system (an information filtering system that promotes content expected to be most pertinent to an end-user) is prioritising, and whether such a system or systems could be recommending content containing misinformation or disinformation.

Subclause 30(11) provides that a digital communications platform provider may notify the ACMA that information in a report required by the digital platform rules to be given to the ACMA is protected information. Protected information is defined in clause 2 of Schedule 9. It covers a trade secret or other information that has a commercial value that would be (or could reasonably be expected to be) destroyed if the information were publicly disclosed.
The notice must identify the information that is protected and explain why that is the case. This subclause is similar to subclauses 17(5), 33(5) and 34(6).

The presence of protected information in the report would not affect the requirement to provide the report to the ACMA (depending on the terms of the digital platform rules). However, it would affect the circumstances in which the ACMA could publish the information and the publication process (per clauses 39 and 40). The note to subclause 30(11) draws attention to clauses 39 and 40 and the limitations on the publication of protected information under clause 38.

Relationship with information gathering powers

Subclause 30(12) provides that clause 30 does not limit clauses 33 or 34 (which are about the general information-gathering powers of the ACMA). This is to ensure that the ACMA can use its information-gathering powers while digital platform rules relating to records are in existence. For example, if the digital platform rules provided for a digital communications platform provider to report annually to the ACMA, the ACMA could still make an ad hoc request for information from the platform provider at another time in circumstances covered by clause 33.

Clause 31—Compliance with digital platform rules regarding records and reports

The ACMA would have several graduated mechanisms available to ensure compliance with the digital platform rules relating to records and reports. The ACMA would be able to choose the enforcement mechanism most appropriate to the situation if enforcement action was required.

Subclause 31(1) provides that a digital communications platform provider must not contravene digital platform rules made for the purposes of clause 30.

Subclause 31(2) provides that subclause 31(1) is a civil penalty provision.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) into the BSA, which provides that for persons who are body corporates, the maximum penalty for a contravention of Subdivision A of Division 3 of Part 2 (which includes clause 31) is 5,000 penalty units, and for persons who are not body corporates, the maximum penalty is 1,000 penalty units.

Clause 72 provides that the contravention of subclause 31(1) is a separate contravention for each day the contravention continues. Clause 73 provides that subclause 31(1) is a designated infringement notice provision and clause 74 provides that the ACMA can issue a warning in relation to its contravention.

Clause 32—Remedial directions—contravention of digital platform rules regarding records and reports

Pursuant to clause 32 the ACMA may issue remedial directions to digital communications platform providers for the purposes of enforcing digital platform rules regarding records and reports.

Subclause 32(1) provides that clause 32 applies if the ACMA is satisfied that a digital communications platform provider has contravened, or is contravening, digital platform rules made for the purposes of clause 30.

Subclause 32(2) provides that the ACMA may give a digital platform provider identified under subclause 32(1) a written direction requiring the provider to take specified action to ensure they do not contravene the digital platform rules made for clause 30, or are unlikely to do so in the future.

Subclause 32(2) is to be interpreted in light of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a

legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument. Thus, the ACMA would be able to vary the requirements in a written direction provided pursuant to subclause 32(2), or revoke the direction, once provided.

Clause 75 provides that a direction under subclause 32(2) is taken to be a notice under Schedule 9 for the purposes of the BSA and the ACMA Act. Clauses 77 and 78 provide for the service of notices under Schedule 9 to the BSA.

Decisions to issue, vary or refuse to revoke, a remedial direction under subclause 32(2) are reviewable by the ART (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Subclause 32(3) provides that a digital communications platform provider must not contravene a direction made under subclause 32(2). Subclause 32(4) provides that subclause 32(3) is a civil penalty provision.

Clause 72 provides that that the contravention of subclause 32(3) is a separate contravention for each day the contravention continues.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5E) to the BSA, which provides that for persons who are body corporates, the maximum penalty for a contravention of Subdivision A of Division 3 of Part 2 (which includes clause 32) is 5,000 penalty units, and for persons who are not body corporates, the maximum penalty is 1,000 penalty units.

SUBDIVISION B—INFORMATION GATHERING

Clause 33—ACMA may obtain information and documents from digital communications platform providers

Clause 33 provides that the ACMA may obtain information and documents (other than source code) from digital communications platform providers. Clause 33 is applicable at all times to all digital communications platform providers, even if they are simultaneously subject to digital platform rules under clause 30. This is to ensure the ACMA can seek information on an as needs basis. This allows the ACMA to use ad hoc requests to obtain information, and make information available, outside of regular reporting periods that may be set out in digital platform rules pursuant to clause 30. This would allow the ACMA to gain insights into the extent of misinformation and disinformation on digital communication platforms and the effectiveness of measures to combat its spread, including the effectiveness of voluntary codes, approved misinformation codes or misinformation standards. Clause 33 applies to information and documents whether or not the information or documents came into existence before or after the commencement of the Bill (see subitem 34(2) of Schedule 2 to the Bill).

Scope

Subclause 33(1) sets out that clause 33 applies to a digital communications platform provider if both paragraphs 33(1)(a) and (b) are satisfied. Paragraph 33(1)(a) requires that the ACMA has reasonable grounds to believe the digital communications platform provider has information or a document (other than source code) relevant to misinformation or disinformation on the platform, or to measures implemented to prevent or respond to

misinformation or disinformation on the platform, including regarding the effectiveness of such measures. These are the same matters that may be subject to digital platform rules about record keeping under paragraphs 30(1)(a) and (b).

Paragraph 33(1)(b) requires that the ACMA considers that obtaining the information or document is necessary for the ACMA to carry out its functions under paragraphs 10(1)(mb), (mc), (md) (me), (mf), (mg) or (q) of the ACMA Act. Item 2 of Schedule 2 to the Bill inserts the functions in paragraphs 10(1)(mb) to (mg). They include functions such as: assisting sections of the digital platform industry to develop misinformation codes; developing standards, monitoring compliance with Schedule 9 to the BSA, misinformation codes, misinformation standards and the digital platform rules; and conducting investigations into, and informing itself, the Minister and the public about, misinformation and disinformation on digital communications platforms. The function in paragraph 10(1)(q) is about reporting to and advising the Minister in relation to the broadcasting, broadcasting video on demand, internet and datacasting industries.

ACMA may require information or documents

Subclause 33(2) sets out that the ACMA may, by written notice to a digital communications platform provider, require the provider:

- to give the ACMA, within the period and in the manner and form specified in the notice, any such information
- to produce to the ACMA, within the period and in the manner specified in the notice, any such documents, or
- to make copies of any such documents and to produce to the ACMA, within the period and in the manner specified in the notice, those copies.

The purpose of this subclause is to ensure that the ACMA is able to obtain the required information, documents or copies of documents regardless of the geographic location, type or corporate structure of the digital communications platform provider.

A notice cannot require a digital communications platform provider to give information, or produce a document or copy, that would reveal the content of a private message or VoIP communication sent by an end-user of the platform (other than a private message or VoIP communication relating to the internal operations of the platform sent by an employee of, or person providing services to, the provider) (per subclause 33(3)). The purpose of this provision is to ensure the ACMA cannot use its information gathering powers to require the disclosure of the content of private messages and VoIP communications, and therefore to protect the privacy of end-users.

Subclause 33(3) does not prevent the ACMA requiring information or documents that *relate* to private messages or VoIP communications, provided the information or documents can be provided without the content of private messages or VoIP communications being divulged. For example, the ACMA could seek information about the number of complaints received by digital communications platform providers relating to misinformation in private messages on the platform, or it could seek information about the measures that providers have taken to address misinformation or disinformation on their private messaging applications. This type of information could provide the ACMA with a better understanding of the potential volume of misinformation and disinformation on a digital communications platform, without

requiring the content of messages themselves to be revealed. Similarly, subclause 33(3) would not prevent the ACMA seeking information from providers that operate private messaging applications about whether (and how) they provide access to authoritative sources of information to the users of those applications.

Pursuant to subclause 33(3), the protection for the content of private messages and VoIP communications does not apply to private messages or VoIP communications relating to the internal operations of the platform, sent by an employee of, or person providing services to, the platform provider. This is to ensure that the ACMA is able to use its information gathering powers to obtain information from providers relating to the internal operations of a digital communications platform, in order to properly carry out its functions under Schedule 9 to the BSA.

Subclause 33(4) provides that a digital communications platform provider must comply with a requirement under subclause 33(2).

Protected information

Subclause 33(5) provides that a digital communications platform provider may notify the ACMA that information or a document required to be given to the ACMA contains protected information. The notice must identify the information that is protected and explain why that is the case. This subclause is similar to subclauses 17(5), 30(11) and 34(6).

Protected information is defined in clause 2 of Schedule 9. It covers a trade secret or other information that has a commercial value that would be (or could reasonably be expected to be) destroyed if the information were publicly disclosed.

Note that the digital communications platform provider is not excused from providing the information to the ACMA on the grounds that it is protected information. However, notifying the ACMA that the information or documents contain protected information will affect the circumstances in which the ACMA could publish the information and the publication process (per clauses 39 and 40). The note to subclause 33(5) draws attention to clauses 39 and 40 and the limitations on the publication of protected information under clause 38.

Civil penalty provision

Subclause 33(6) provides that subclause 33(4) is a civil penalty provision.

Clause 72 provides that that the contravention of subclause 33(4) is a separate contravention for each day the contravention continues. Clause 73 provides that subclause 33(4) is a designated infringement notice provision and clause 74 provides that the ACMA can issue a warning in relation to the provision's contravention.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5F) into the BSA, which provides that for persons who are body corporates the maximum penalty for a contravention of subclause 33(4) is 40 penalty units, and for persons who are not body corporates the maximum penalty is 30 penalty units.

Item 25 of Schedule 2 to the Bill inserts new paragraphs 205ZA(1)(ab) to (ad) into the BSA and provides that the infringement notice penalty for a contravention of subclause 33(4) for a

person who is a body corporate is 8 penalty units and for a person who is not a body corporate is 6 penalty units.

Requirements for notice

Subclause 33(7) provides that a notice given to a person under subclause 33(2) must set out the effect of subclauses 33(4) and 33(6). This means that the person will be on notice that a failure to comply attracts a civil penalty. The notice must also draw attention to paragraph 72(j) (regarding separate conventions) and subsection 205F(1) (regarding the power for the Federal Court to make a civil penalty order).

Clause 34—ACMA may obtain information and documents from other persons

Clause 34 provides that the ACMA may obtain information and documents from other persons.

This clause has been included to enable the ACMA to obtain information and documents relating to the matters specified in subclause 34(1) from a wider range of sources than digital communications platform providers alone. This is so the ACMA can obtain relevant information that digital communications platform providers do not possess, or if required, check the integrity of information provided by digital communications platform providers. Clause 34 applies to information and documents whether or not the information or documents came into existence before or after the commencement of the Bill (see subitem 34(2) of Schedule 2 to the Bill).

Scope

Subclause 34(1) sets out that clause 34 applies to a person if the ACMA has reasonable grounds to believe the person has information or a document (other than source code) relevant to misinformation or disinformation on a digital communications platform (paragraph 34(1)(a)) and/or measures implemented by a digital communications platform provider to prevent or respond to misinformation or disinformation on a digital communications platform, including the effectiveness of the measures (paragraph 34(1)(b)).

However, under paragraph 34(1)(b), the ACMA must consider that it requires the information or document for the performance of the ACMA's function under paragraph 10(1)(md) of the ACMA Act only. This function, inserted by item 2 of Schedule 2 to the Bill, is monitoring compliance with Schedule 9 to the BSA, misinformation codes, misinformation standards and digital platform rules. This is more limited than the power to request information and documents from digital communications platform providers, which can relate to a broader range of the ACMA's functions.

Subclause 34(2) explains when paragraph 34(1)(a) does not apply. It does not apply in relation to information or documents relating to content posted by the person on the digital communications platform, other than content posted in the person's capacity as: a fact-checker, a content moderator, an employee of the provider of the platform, or a person providing services to the provider of the platform. The intention is to distinguish between what persons post in a personal capacity (which is outside the scope of clause 34) and what they post in their professional capacity as part of their role in connection with the digital

communications platform provider, for example, for the purpose of monitoring the provider's compliance with misinformation codes or misinformation standards.

In this way, clause 34 does not intend to capture end-users who merely post or engage with content on digital communications platforms. This clause is intended to empower the ACMA to seek information from people connected to a digital communications platform in a professional capacity. For example, the ACMA could seek information from a former company director of a digital communications platform about misinformation policies used at a particular point in time.

ACMA may require information or documents

Subclause 34(3) states that the ACMA may, by written notice to a person, require the person to:

- give the ACMA, within the period and in the manner and form specified in the notice, any such information,
- produce to the ACMA, within the period and in the manner specified in the notice, any such documents, or
- make copies of any such documents and to produce to the ACMA, within the period and in the manner specified in the notice, those copies.

A notice cannot require a person to give information, or produce a document or copy, that would reveal the content of a private message or VoIP communication (subclause 34(4)).

Subclause 34(5) provides that a person to whom a notice has been given under subclause 34(3) must comply with a requirement under subclause 34(3).

Protected information

Subclause 34(6) provides that a person may notify the ACMA that information given or a document or copy produced under clause 34 contains protected information. The notice must identify the information that is protected information and explain why that is the case. This subclause is similar to subclauses 17(5), 30(11) and 33(5).

Protected information is defined in clause 2 of Schedule 9. It covers a trade secret or other information that has a commercial value that would be (or could reasonably be expected to be) destroyed if the information were publicly disclosed.

Note that the person is not excused from providing the information to the ACMA on the grounds that it is protected information. However, notifying the ACMA that the information or documents contain protected information will affect the circumstances in which the ACMA could publish the information and the publication process (per clauses 39 and 40). The note to subclause 34(6) draws attention to clauses 39 and 40 and the limitations on the publication of protected information under clause 38.

Civil penalty provision

Subclause 34(7) provides that subclause 34(5) is a civil penalty provision.

Clause 72 provides that that the contravention of subclause 34(5) is a separate contravention for each day the contravention continues. Clause 73 provides that subclause 34(5) is a designated infringement notice provision and clause 74 provides that the ACMA can issue a warning in relation to its contravention.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5F) into the BSA, which provides that for persons who are body corporates the maximum penalty for a contravention of subclause 34(5) is 40 penalty units and for persons who are not body corporates the maximum penalty is 30 penalty units.

Item 25 of Schedule 2 to the Bill inserts new paragraphs 205ZA(1)(ab) to (ad) into the BSA and provides that the infringement notice penalty for contravention of subclause 34(5) for a person who is a body corporate is 8 penalty units and for a person who is not a body corporate is 6 penalty units.

Requirements for notice

Subclause 34(8) provides that a notice given to a person under subclause 34(3) must set out the effect of subclauses 34(5) and 34(7). This means that the person will be on notice that a failure to comply attracts a civil penalty. The notice must also draw attention to paragraph 72(k) (regarding separate conventions) and subsection 205F(1) (regarding the power for the Federal Court to make a civil penalty order).

Clause 35—Copying documents—reasonable compensation

Clause 35 provides that where the ACMA has required a person to make and provide copies of documents under paragraphs 33(2)(c) or 34(3)(c), the person is entitled to reasonable compensation from the ACMA for complying with that requirement.

Clause 36—Copies of documents

Clause 36 permits the ACMA to inspect documents or copies of documents produced under Subdivision B (information gathering) and make and retain copies of, or take and retain extracts from, such documents. Where a person was required to produce a copy of the document, the ACMA may retain that copy.

Clause 37—ACMA may retain documents

Clause 37 permits the ACMA to retain documents produced under Subdivision B (information gathering) for as long as is necessary (subclause 37(1)). The person otherwise entitled to possession of the document would be entitled to be supplied with a copy of the document certified by the ACMA to be a true copy (subclause 37(2)). The certified copy must be received in all courts and tribunals as evidence as if it were the original (subclause 37(3)). Until the ACMA has provided such a copy, the person is entitled to have access to the document to inspect and make copies of it or take extracts from it (subclause 37(4)).

SUBDIVISION C—PUBLISHING INFORMATION

Clause 38—Publication on website

Clause 38 provides that the ACMA may publish information relating to the matters outlined in subclause 38(1) on its website. These matters are the same as those in subclauses 30(1) and 33(1): misinformation or disinformation on digital communications platforms and measures implemented to prevent or respond to misinformation or disinformation on digital communications platforms, including regarding effectiveness of the measures.

Subclause 38(2) provides that the information may relate to any particular digital communications platform or digital communications platform provider (paragraph 38(2)(a)), a class of digital communications platforms or platform providers (paragraph 38(2)(b)), or all digital communications platforms or platform providers (paragraph 38(2)(c)).

Subclause 38(3) provides that the information may include information obtained by the ACMA under paragraph 17(4)(b) (statement of the reason why a digital communications platform provider has not published certain information), Subdivision D of Division 2 of Part 2 (information relating to complaints) or Division 3 of Part 2 (information that the ACMA obtains through reports provided by digital communications platform providers, or through specific requests that the ACMA makes for information from digital communications platform providers or other persons).

Subclause 17(4) provides that if a digital communications platform provider fails to comply with the obligation to publish a report of the outcomes of a risk assessment, its policy or policy approach in relation to misinformation and disinformation or its media literacy plan, it must provide a copy of that information to the ACMA (paragraph 17(4)(a)), together with a statement of the reason why it has not made the information accessible to the public on its website and to end-users (paragraph 17(4)(b)). Empowering the ACMA to publish the reasons provided by digital communications platform providers for not publishing this core transparency information is intended to further incentivise providers to publish this information, as required by subclause 17(1), and in the event of failure to publish, to provide the ACMA with a justification that withstands public scrutiny. For the avoidance of doubt, pursuant to subclause 38(3) the ACMA could decide to publish any, all or none of the information made available to it pursuant to paragraph 17(4)(b). For example, a digital communications platform provider may publish its policy or policy approach in relation to misinformation and disinformation (thus satisfying paragraph 17(1)(b)), but fail to publish a report of the outcome of its risk assessment and its media literacy plan (thus failing to satisfy paragraphs 17(1)(a) and (c)). Pursuant to clause 17(4), that provider must provide the ACMA with a report of the outcome of its risk assessment, and its media literacy plan, together with its reasons for failing to publish both products. For reasons determined by the ACMA, pursuant to subclause 38(3), the ACMA may exercise its discretion to publish the provider's reasons for failing to publish a report of the outcomes of its risk assessment, but not the provider's reasons for failing to publish its media literacy plan.

The note to clause 38 explains that the ACMA is subject to the Privacy Act, and the requirements therein relating to the collection, use and disclosure of personal information. The Privacy Act provides a number of safeguards to promote responsible handling of personal information by entities.

Clause 38 is also limited by clause 39, as explained below.

Publication is an important aspect of the information-gathering powers as it allows the ACMA to be transparent about the information it collects, and keeps Australians informed about what is happening on the digital communications platforms they use. Publication of information received under Division 3 of Part 2 is also intended to encourage compliance and good practice by digital communications platforms. The ACMA's ability to publicly name when a particular platform has inadequate records, or disclose when information reveals issues with a platform's systems and policies for addressing misinformation and disinformation, can be a significant incentive for compliance.

Clause 39—Protected information

Clause 39 provides that if the ACMA is satisfied that information is protected information, the ACMA must not publish that information under clause 38 unless:

- the information is already in the public domain (paragraph 39(a))
- the information is required to be disclosed under a law of the Commonwealth, a State or a Territory (paragraph 39(b))
- the ACMA obtains consent to the publication from the owner of the trade secret (where the information is a trade secret) (subparagraph 39(c)(i))
- the ACMA obtains consent to the publication from the owner of the information (for any other case other than information that is a trade secret (subparagraph 39(c)(ii)).

Protected information is defined in clause 2 of Schedule 9. It covers a trade secret or other information that has a commercial value that would be (or could reasonably be expected to be) destroyed if the information were publicly disclosed.

Clause 40—Publication process in relation to protected information

Clause 40 provides a publication process to be followed where the ACMA proposes to publish information that relates to a digital communications platform or a digital communications platform provider, in cases where the ACMA has been notified that the information is protected information.

Clause 40 is intended to apply where the ACMA is proposing to publish the information because either it is not satisfied that the information is protected information, or because one of the circumstances mentioned in paragraphs 39(a) to (c) applies.

Subclause 40(2) provides that if the ACMA proposes to publish such information, the ACMA must give the digital communications platform provider a written notice stating that the ACMA proposes to publish the information and giving the provider 30 days in which to make submissions to the ACMA in relation to the proposed publication.

After the end of the 30 days, the ACMA must consider any submissions that have been made by the provider and decide whether or not to publish the information under clause 38 (subclauses 40(3) and (4)).

If the ACMA decides to publish the information, the ACMA must give the provider a written notice of its decision and then wait another 30 days before publishing the information (subclause 40(5)). The purpose of requiring the ACMA to wait 30 days before implementing

a decision is to enable time for a digital communications platform provider who disagrees with the ACMA's decision to apply to the ART for review of the decision (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 41—Relationship with Part 7A of the *Australian Communications and Media Authority Act 2005*

Clause 41 provides that Division 3 of Part 2 does not limit part 7A of the ACMA Act. The ACMA would be able to publish information on its website under clause 38 or disclose information as authorised by Part 7A of the ACMA Act.

Part 7A of the ACMA Act allows the ACMA to disclose authorised disclosure information (within the meaning of the ACMA Act) in certain situations, including to other listed Commonwealth authorities. The list contains a number of named authorities, and includes a provision that the ACMA may give information to any non-corporate Commonwealth entity not otherwise covered that is responsible for enforcing one or more laws of the Commonwealth.

DIVISION 4—MISINFORMATION CODES AND MISINFORMATION STANDARDS

Division 4 sets out the framework for industry to seek approval and registration by the ACMA of misinformation codes that have been developed by bodies and associations that represent sections of the digital platform industry. Provided that the codes satisfy certain requirements, the ACMA would be able to approve and register the codes and subsequently enforce them using a suite of enforcement powers, such as formal warnings and remedial directions.

The ACMA also has the power to make an industry standard (requiring industry compliance) in certain circumstances that applies to participants in a particular section of the digital platform industry.

The ACMA may request that a code be developed where the ACMA is satisfied that development of the code is necessary in order to prevent or respond to misinformation or disinformation on digital communications platforms, or to address systemic issues in relation to misinformation or disinformation on digital communications platforms, and in circumstances where in the absence of the request, it is unlikely that a code would be developed within a reasonable period. The ACMA may make a standard in certain circumstances, for example, if a request for a code to be developed is not complied with, or there has been a partial failure of an existing misinformation code.

SUBDIVISION A—INTERPRETATION

Clause 42—Sections of the digital platform industry

Clause 42 sets out how ***section of the digital platform industry*** is to be ascertained for the purposes of Schedule 9.

This clause has been drafted so that the ACMA may register a code or make a standard to only apply to some digital communications platforms with a certain commonality, instead of the entire digital platform industry.

Subclause 42(2) provides that digital communications platform providers of the kinds of digital services in paragraphs (a) to (d) (being providers of connective media services, content aggregation services, internet search engine services and media sharing services), are respectively a section of the digital platform industry.

Subclause 42(3) provides that any providers of a kind of digital service determined by the Minister under subclause 5(7) would also be a ***section of the digital platform industry***. This ability for the Minister to make a determination is necessary in order for the framework to be responsive to a rapidly evolving industry.

Subclause 42(4) allows the digital platform rules to specify additional kinds of digital communications platforms, the providers of which constitute a section of the digital platform industry for the purposes of Schedule 9. This flexibility is necessary because it would be impossible to exhaustively list the types of digital communications platforms that may in the future come into existence, the providers of which would appropriately be considered a section of the digital platforms industry. Thus, this subclause allows the ACMA to keep the list of sections of the digital platforms industry up-to-date, as technologies evolve.

The ACMA's power to make digital platform rules is elaborated in clause 82. Digital platform rules are a legislative instrument for the purposes of the Legislation Act. This means that the rules would be subject to parliamentary disallowance and would be registered on the Federal Register of Legislation. They would need to be accompanied by a statement of compatibility with human rights, included in the explanatory statement to the rules, in accordance with the section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act. Subclause 82(2) sets limits on the ACMA's power to make digital platform rules.

Subclause 42(5) requires that the section of the digital platform industry must be identified by a unique name and/or number in the digital platform rules. This is intended to support participants of the digital platform industry to more readily identify their obligations, including when a code or standard is made concerning them.

Subclause 42(6) states that digital platform rules made for the purpose of subclause 42(4) have effect accordingly.

Sections of the digital platform industry created by the digital platform rules do not need to be mutually exclusive, and may include any combination or subset of existing sections of industry (see subclause 42(7)).

The purpose of subclause (7) is to ensure the ACMA can apply targeted regulation. The advantage of this is that misinformation codes or misinformation standards could have specific provisions for particular types of platforms (for example, internet search engines, which would be a subset of content aggregation services, or social media services, which would be a subset of connective media services).

Subclause 42(8) explains that subclause 42(7) does not, by implication, limit subclause 42(4). In other words, a section of the digital platform industry does not have to be an aggregate or subset of an existing section of the industry, but could also be an entirely new section of the industry.

Clause 43—Participants in a section of the digital platform industry

Clause 43 defines ***participant*** for the purposes of Schedule 9. That is, if a digital communications platform provider is a member of a group that constitutes a section of the digital platform industry, the provider is a ***participant*** in that section of the digital platform industry.

Being a 'member of a group' should not be read in the sense of formal membership to an established organisation. Membership is informal and based upon the nature of the digital service (as outlined in subclause 5(1)) provided by the digital communications platform provider. For example, if a digital communications platform was a connective media service (as outlined in subclause 5(2)), then the provider of that service would be a member of a group of digital communications platform providers who provide connective media services. In other words, such a digital communications platform provider would be a participant in the connective media services section of the digital platform industry.

SUBDIVISION B—GENERAL PRINCIPLES RELATING TO MISINFORMATION CODES AND MISINFORMATION STANDARDS

Clause 44—Examples of matters that may be dealt with by misinformation codes and misinformation standards

Clause 44 provides examples of measures that may be included in a misinformation code or misinformation standard (see the explanation at subclause 44(1)). It does not contain an exhaustive list of what the ACMA could require a code or standard to contain.

Subclause 44(2) explains that the applicability of a particular example will depend on which section of the digital platform industry is involved.

Subclause 44(3) sets out the list of examples of matters that could be included in a misinformation code or misinformation standard:

(a) Preventing or responding to misinformation or disinformation on digital communications platforms

A code or standard could set out objectives relating to preventing or responding to misinformation. Digital communications platform providers in scope of a code could then take actions to meet the objectives in a manner that would be appropriate to the nature of the particular section of the industry. The intention is that, subject to the limits in the operative clauses of Schedule 9, codes and standards may also encourage or mandate specific and proactive, preventative measures as well as responsive measures.

The term 'preventing' is intended to have its ordinary meaning. This could include specific measures to minimise the spread of misinformation or disinformation, such as altering recommendation algorithms to prevent misinformation or disinformation content being propagated, or closing or limiting the reach of accounts that repeatedly disseminate misinformation or disinformation. Note that, in accordance with clause 67, codes or standards could only require blocking an end-user from using a platform if they were involved in dissemination of disinformation involving inauthentic behaviour on the platform. A code or

standard could also seek to prevent misinformation or disinformation by pre-vetting the placement of advertisements containing misinformation or disinformation on the platform.

The term 'responding' is also intended to have its ordinary meaning. Responding to misinformation or disinformation could include requiring platforms to remove content where it is disinformation that involves inauthentic behaviour. As stated in clause 67, the codes or standards could not require a digital communications platform provider to remove content that is not disinformation involving inauthentic behaviour. However, a response does not necessarily require the removal of content that is misinformation or disinformation. It could also involve addressing the consequences of conduct that constitutes misinformation or disinformation. For example, a code or standard could require platforms to put in place measures to 'nudge' users to consider whether to on-share the information.

(b) Using technology to prevent or respond to misinformation or disinformation on digital communications platforms

The intention of the example in paragraph (b) is to indicate that misinformation codes or standards may, subject to Schedule 9, deal with the use of technology to address the same matters mentioned in paragraph (a). Digital communications platform providers could be required to use automated processes and technology to detect and act appropriately on misinformation and disinformation under a misinformation code or misinformation standard. For example, they could be required to use technology or algorithms to 'downrank' or reduce the spread of misinformation or disinformation, or to 'nudge' a person to reflect on the information before sharing it.

(c) Preventing or responding to misinformation or disinformation on digital communications platforms that constitutes an act of foreign interference

The term 'foreign interference' as used here is intended to have the same meaning as provided in section 4 of the *Australian Security Intelligence Organisation Act 1979.*

This example is listed separately from the example in paragraph 44(3)(a) to highlight that misinformation codes and misinformation standards could require participants to identify and treat instances of foreign interference differently to other instances of misinformation and disinformation.

(d) Preventing advertising involving misinformation or disinformation on digital communications platforms

Digital communications platform providers may be required to reject potential advertisements on their service if the advertisements contain misinformation or disinformation as part of the advertisement. This could include, for example, advertising for an alternative health product using a premise that was misinformation or disinformation that caused or contributed to harm to public health in Australia or to the efficacy of preventative health measures for Australians.

For clarity, this measure would not limit any obligations under the Australian Consumer Law in the Competition and Consumer Act or under the *Therapeutic Goods Act 1989.* The intention of this example is to ensure that digital communications platform providers could be required by the ACMA to take a proactive approach to dealing with misinformation and disinformation in advertising that could be spread at scale, on or through their platforms.

(e) Preventing monetisation of misinformation or disinformation on digital communications platforms

Digital communications platform providers could be required by the ACMA to prevent users that disseminate misinformation or disinformation content from earning money that could come from advertisements that accompany the misinformation or disinformation content.

(f) Supporting fact-checking

Misinformation codes or misinformation standards could require digital communications platform providers to support fact-checking. Depending on the platform, this obligation could be met by allowing and supporting fact-checking organisations to give authoritative advice on content that is misinformation or disinformation. It could also include a requirement that digital communications platform providers improve their labelling of fact-checked materials, or use technology to 'nudge' a person to think about or fact-check content themselves before sharing.

(g) Allowing end-users to detect and report misinformation or disinformation on digital communications platforms

Digital communications platform providers may be required to enable end-users to report misinformation or disinformation on their services for appropriate action by the digital communications platform provider. It could be designed to incentivise adequate systems and processes for the reporting of complaints about misinformation and disinformation on digital communications platforms.

(h) Giving information to end-users about the source of political or issues-based advertisements

Digital communications platform providers may be required to increase transparency to end-users about political or issues-based advertising they see on digital communications platforms.

(i) Policies and procedures for receiving and handling reports and complaints from end-users

Misinformation codes or standards may set out requirements relating to the receipt and handling of reports and complaints from end-users.

This subparagraph supplements clause 25, which empowers the ACMA to make digital platform rules requiring digital communications platform providers to implement and maintain processes for handling misinformation complaints, and setting minimum standards for those processes.

The ACMA will not have a role in handling individual complaints under a code or standard, nor in relation to specific pieces of content.

The effect of complaints processes being included in the non-exhaustive list of matters provided at clause 44 – that is, as an example of matters that may be included in misinformation codes or misinformation standards – is that requirements relating to complaint

handling processes may be included in misinformation codes and/or misinformation standards (pursuant to clause 44) and/or digital platform rules (pursuant to clause 25). However, pursuant to clause 66, if a misinformation code or misinformation standard conflicts with a digital platform rule that applies to a digital communications platform provider, the code or standard will have no effect to the extent of the inconsistency. The following two scenarios provide an example of the way in which these clauses may interact.

Scenario 1

The ACMA makes a digital platform rule pursuant to clause 25, requiring all digital communications platform providers in a certain sector to have a complaints and dispute handling process. The relevant sector of the digital communications platform industry then develops a misinformation code, setting out the specifics of the complaints process that must be implemented by digital communications platforms to whom that code applies. The ACMA approves and registers the code (pursuant to clause 47 and 64). Thereafter, digital communications platforms to whom the code applies must comply with the misinformation code (clause 52).

Scenario 2

The ACMA makes a digital platform rule pursuant to clause 25, stating that all digital communications platform providers must have a complaints process, and specifying minimum standards for that process. A section of the digital platforms industry then develops a misinformation code. ACMA considers whether the misinformation code complies with the minimum standards prescribed by the digital platform rules, and following such consideration, registers the code (clause 47).

The ACMA subsequently determines that that section of the industry poses a particularly high-risk of misinformation and disinformation, and that the misinformation code developed by that section of the industry (and registered by the ACMA) is not adequately protecting the Australian community from misinformation and disinformation. This is partially because the complaints handling process prescribed by the misinformation code is proving inadequate for that section of the industry (even though it complies with the minimum standards prescribed by the digital platform rules). The ACMA requests that the deficiencies be addressed (pursuant to paragraph 58(1)(c)), and the request is not complied with. In light of the particularly high-risk, the ACMA then determines a misinformation standard for that section of the industry (pursuant subclause 58(3)), which sets out specific requirements for a misinformation complaints process, applicable to that section of the industry.

(j) Giving end-users and others information about misinformation or disinformation on digital communications platforms, including management of misinformation or disinformation on digital communications platforms

Digital communications platform providers may be required to report to end-users about misinformation and disinformation on their services. Depending on the requirement in a code or standard, this may also include:

- communicating clear policies and terms of use as they relate to misinformation
- steps taken by the platform to identify and mitigate misinformation risks to protect end-users

- explaining the procedures to make complaints and dispute the handling of misinformation on their service
- measures to assist end-users to better recognise misinformation and disinformation and identify authoritative information sources on the platform.

(k) Giving end-users and others information about authoritative content and factual information on digital communications platforms

Digital communications platform providers may be required to provide end-users with links to authoritative sources of information and factual information to counter and respond to misinformation and disinformation.

(l) improving media literacy of end-users

A misinformation code or misinformation standard could require digital communications platform providers to take specific measures to improve the media literacy of end-users. All digital communications platform providers will be required, pursuant to paragraph 17(1)(c), to have and publish a media literacy plan, setting out the measures the provider will take to enable end-users to better identify misinformation and disinformation. Non-compliance with the requirement to have and publish a media literacy plan, including any additional requirements set out in the rules at subclause 22(1) may result in the digital communications platform receiving a formal warning (subclause 74(1)), a remedial direction (clause 18 and subclause 24(2)), an infringement notice (clause 73), or a civil penalty (subclause 17(6) and subclause 23(2)).

The effect of media literacy being included in the non-exhaustive list of matters provided at clause 44 – that is, examples of matters that may be included in misinformation codes or misinformation standards – is that notwithstanding the fact that all digital communications platform providers are already required by subclause 17(1)(c) to have and publish a media literacy plan), misinformation codes and misinformation standards may set out specific things that digital communications platform providers must actually *do* to improve the media literacy of their users. The obligation described in subclauses 17(1)(c) are intended simply to require digital communication platform providers to have a media literacy plan and be transparent as to what they have. Misinformation codes or misinformation standards may be used – if necessary – to supplement this obligation by requiring digital communications platform providers to take *specific* measures to improve media literacy, and to monitor and report on the effectiveness of those measures.

Clause 45—Limitation—private messages

Clause 45 provides that a misinformation code or misinformation standard must not contain requirements relating to the content of private messages or the encryption of private messages.

The policy intention is that a misinformation code or misinformation standard may still include requirements for messaging services on digital communications platforms. However, they must not require the digital communications platform provider to access messages in order to monitor for misinformation or disinformation.

A measure that could achieve this, for example, is allowing users to directly send messages with content they are unsure about the factuality of to a partnered fact-checker, without the digital communications platform provider directly knowing the contents of the message. The popular instant messaging service WhatsApp already provides this service in several countries, although Australia is not one of them as at 2024.[165]

Clause 46—Limitation—VoIP communications

Clause 46 provides that the ACMA must not approve a code in full or in part, or determine a standard, under this Division that contains requirements relating to VoIP communications.

This limitation has been included for privacy and workability purposes. VoIP communications are of an instantaneous nature and it would be very difficult for digital communications platform providers to apply any measures to prevent or respond to misinformation and disinformation on real time audio.

SUBDIVISION C—MISINFORMATION CODES

Subdivision C sets out the requirements and process for registration of misinformation codes.

Clause 47—Approval of codes

Clause 47 provides for ACMA to approve and register a misinformation code and the circumstances that must be met for that to occur. The requirements would apply regardless of whether the ACMA requested the development of the code (see clause 48) or an industry body or association was seeking on its own initiative to have a voluntary code registered (clause 48). A misinformation code that has been approved by ACMA would be a legislative instrument that digital communications platform providers within the scope of that code would need to comply with.

Scope

Clause 47 sets out requirements that would need to be fulfilled before a code could be approved by the ACMA.

Pursuant to paragraph 47(1)(a), the ACMA must first be satisfied that the body or association that has developed the code represents a particular section of the digital platform industry. The term 'section of the digital platform industry' has the meaning given by clause 42. The ACMA must also be satisfied that the code applies to participants in that section of the digital platform industry and deals with one or more matters relating to the operation of digital communications platforms by those participants (paragraph 47(1)(b)). Clause 43 sets out who is a 'participant' in a section of the digital platform industry. The body or association would need to provide a copy of the code to the ACMA (paragraph 47(1)(c)).

Paragraph 47(1)(d) sets out a list of matters of which the ACMA must be satisfied, before approving a misinformation code or part thereof.

[165] WhatsApp, 'IFCN Fact-Checking Organizations on WhatsApp', *Frequently Asked Questions* (2024) <https://faq.whatsapp.com/5059120540855664>.

Subparagraph 47(1)(d)(i) provides that the ACMA must be satisfied that the code (or part of the code) requires participants in the relevant section of the digital platform industry to implement measures to prevent or respond to misinformation or disinformation on the platforms. Subparagraph 47(1)(d)(ii) provides that the ACMA must also be satisfied that the code (or part of the code) enables assessment of compliance with the measures.

Subparagraphs 47(1)(d)(iii) and (iv) provide that prior to approving a code, the ACMA must be satisfied that the code (or part thereof) is: reasonably appropriate and adapted to achieving the purpose of providing adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on the platforms; and goes no further is than reasonably necessary to provide that protection.

The reference to 'adequate protection for the Australian community' in these subparagraphs must be understood in relation to all aspects of the definition of misinformation and disinformation, in particular the meaning of 'serious harm' as defined by clause 14. That is to say, in order for the ACMA to register a misinformation code, it must be satisfied that the measures included in that code adequately protect the Australian community from the risk that certain false, misleading or deceptive content disseminated on a digital communications platform will cause or contribute to serious harm of a type described at clause 14.

The requirement expressed by subparagraphs 47(1)(d)(iii) and (iv) is aimed at ensuring that the power conferred on the ACMA is wholly valid, by making clear on the face of the legislation that the power it confers cannot be exercised in a way that would transgress the constitutional limits imposed by the implied freedom of political communication, which the High Court of Australia has recognised as impliedly protected by the Australian Constitution.[166] Freedom of political communication in this context means people's ability to communicate 'information and opinions about matters relevant to the exercise and discharge of governmental powers and functions on their behalf'.[167] The requirement that before exercising its power to approve a misinformation code or part thereof, the ACMA must be satisfied of the matters listed at subparagraphs 47(1)(d)(iii) and (iv), recognises that this constitutionally implied freedom is a limitation on Parliament's legislative power to empower ACMA to approve misinformation codes. The test set out at subparagraphs 47(1)(d)(iii) and (iv) aligns with the test endorsed by the High Court of Australia for assessing the consistency of Commonwealth legislation with the implied freedom of political communication. Pursuant to this test, Commonwealth legislation that burdens the freedom of political communication (either in its terms, operation or effect) must have a legitimate purpose, and be reasonably appropriate and adapted (or in other words, proportionate) to the achievement of that legitimate purpose.[168] This has been interpreted to mean that the burden on freedom of political communication must not be 'unreasonably greater than [would be] achievable by other means'.[169]

Paragraphs 47(1)(e)–(f) provide that the ACMA must be also satisfied that consultation with participants in the relevant section of the digital platform industry and with the public more

[166] *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1 ('*Nationwide News*'*)*; *Australian Capital Television Pty Ltd v The Commonwealth* (1992) 177 CLR 106 ('*Australian Capital Television'*).
[167] *Nationwide News* (n 166) 72 (Deane and Toohey JJ).
[168] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520 ('*Lange*'), 562 (the Court; *LibertyWorks Inc v Commonwealth* (2021) 274 CLR 1, [45]-[46] (Kiefel CJ, Keane and Gleeson JJ), [93] (Gageler J), [134] (Gordon J), [200] (Edelman J), [247] (Steward J).
[169] *Coleman v Power* (2004) 220 CLR 1, [100] (McHugh J).

generally occurred prior to the ACMA registering a code. Consultation must allow for both digital communications platform providers and the community at large to make submissions about any part of the code. The consultation period in both cases must be at least 30 days (clause 47(2)), and the ACMA must be satisfied that the body or association considered any submissions before submitting the code to the ACMA for registration.

Paragraph 47(1)(g) also requires the ACMA to be satisfied that at least one body or association that represents the interests of consumers has been consulted about the development of the code. This was drafted to ensure consumer interests were considered in the case of limited submissions during public consultation under paragraph 47(1)(f).

Approval of codes

Subclause 47(3) provides that the ACMA may, by written notice given to the body or association, approve the code or part of the code.

If the ACMA refuses to approve a misinformation code or part of a misinformation code, the body or association that developed the misinformation code may apply to the ART for review of the decision (per the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Subclause 47(4) explains that the approval of a code is not a legislative instrument. This provision is included to assist readers, as the approval is not a legislative instrument within the meaning of subsection 8(1) of the Legislation Act. This is because the ACMA's approval of the code in and of itself does not determine the law or affect privileges, interests, obligations or rights. Rather, it is a preliminary step before the approved code, in the form of a legislative instrument, is lodged on the Federal Register of Legislation. The approved code will take effect once the legislative instrument is registered on the Federal Register of Legislation (see subclause 47(6)). The code as approved and registered on the Federal Register of Legislation would be a legislative instrument (see subclause 47(6) below).

If the ACMA approves part of a misinformation code, Schedule 9 has effect as if the part were a misinformation code (per subclause 47(5)). This subclause could be used in the event that the ACMA is dissatisfied with some provisions of a draft code, but is satisfied with the rest of the provisions.

Approved code is a legislative instrument

Subclause 47(6) provides that a misinformation code approved by the ACMA is deemed to be a legislative instrument.

This means that the approved misinformation code would be subject to parliamentary scrutiny and disallowance, and would be required to be accompanied by an explanatory statement, including a statement of compatibility with human rights, in accordance with section 15J of the Legislation Act and section 9 of the Human Rights (Parliamentary Scrutiny) Act. The intention is that the preparation of this supporting material would be the responsibility of the ACMA, not the industry body or association that developed the misinformation code.

Per subclause 47(7), the ACMA is deemed to be the rule-maker for a misinformation code approved under Division 4 of Part 2. This means that the ACMA will be responsible for

lodging the approved misinformation code, along with an explanatory statement for the code, for registration on the Federal Register of Legislation, in accordance with section 15G of the Legislation Act. It also means that the ACMA must be satisfied that any consultation that it considers is appropriate and reasonably practicable to undertake has been undertaken in relation to the misinformation code, per section 17 of the Legislation Act. It is anticipated that the consultation set out in paragraphs 47(1)(e), (f) and (g) would generally be sufficient for this purpose.

In addition to registering the approved code on the Federal Register of Legislation, the ACMA would also be responsible for registering the approved code on its own electronic Register of misinformation codes and standards (see clause 64).

In the event that an approved misinformation code (or provisions of that code) were to be disallowed by Parliament in accordance with section 42 of the Legislation Act, the legislative instrument (or part thereof) would be immediately repealed (section 42(1) of the Legislation Act), and accordingly the ACMA would be required to remove the code (or part thereof) from its Register of misinformation codes and standards (subclause 64(6)). The misinformation code (or part thereof) could nevertheless still be followed by the relevant industry body or association as a voluntary code; it would just not be legally binding and enforceable.

Clause 48—ACMA may request codes

Clause 48 allows the ACMA to request industry bodies and associations to develop a misinformation code that applies to participants in a section of the digital platform industry.

Under subclause 48(1) the ACMA must first be satisfied that the body or association in question represents a particular section of the digital platform industry. The ACMA is then empowered to request by written notice given to the body or association that the body or association develop a code that applies to participants in that section of the digital platform industry and deals with one or more specified matters (paragraph 48(1)(a)).

The body or association must give the ACMA a copy of the code within the period specified in the notice (paragraph 48(1)(b)). Subclause 48(2) provides that the ACMA must specify a period in the notice under subclause 48(1) of at least 120 days. Depending on the complexity of a request under subclause 48(1), or other factors such as the potential difficulty for industry to undertake necessary consultation in the time available, the ACMA may determine a time period in excess of 120 days. In any event, the ACMA also has discretion to consider requests for extending the period if necessary (see subclause 48(4)).

Subclause 48(3) provides that the ACMA must not make a request (to develop a code) under subclause 48(1) in relation to a particular section of the digital platform industry unless the ACMA is satisfied that the development of the code is necessary to prevent or respond to misinformation and disinformation (subparagraph 48(3)(a)(i)) or to address systemic issues in relation to misinformation or disinformation (subparagraph 48(3)(a)(ii)).

Systemic issues are best defined as those risks which present as (i) a gap or error in business procedure or an error or limitation of a technical system, which, because it is repeated in routine, automated or deployed at scale, amplifies a vulnerability and risk for the platform, or (ii) a generic procedure or technical system, which, employed industry-wide, effectively magnifies vulnerability and risk across the sector as a whole, or (iii) use of a platform by end-

users which results in the escalated dissemination of, or exposure to, misinformation or disinformation content via that platform.

The ACMA would also need to be satisfied that if it did not make a request, it would be unlikely that the code would be developed within a reasonable period (paragraph 48(3)(b)).

Subclause 48(4) allows the ACMA to vary the request for the development of a code by extending the period specified for the development of the code to be given to the ACMA. Requests for extending the period could take into consideration efforts undertaken by the relevant body or association(s) to meet indicative targets specified in subclause 48(6).

Subclause 48(5) provides that subclause 48(4) does not limit the application of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make an instrument, the power shall be construed as including a power exercisable in the like manner and subject to the like conditions (if any) to repeal, rescind, revoke, amend, or vary any such instrument.

Subclause 48(6) provides that the ACMA's notice may specify indicative targets for achieving progress in developing the code.

There are no penalties for not complying with a request to provide a code. However, non-compliance with a request for a code may lead to the ACMA making a standard– that is, participants in a particular section of the digital platform industry would be required to comply with any standard determined by the ACMA under clause 55.

The ACMA is not required to make a request under clause 48 before determining a standard if there are exceptional and urgent circumstances (see clause 59).

Clause 49—Publication of notice where no body or association represents a section of the digital platform industry

Under subclause 49(1) if the ACMA is satisfied that a particular section of the digital platform industry is not represented by a body or association, the ACMA may publish a notice on its website setting out: (a) if a body or association were to come into existence within a specified period, the ACMA would likely give a notice to that body or association under subclause 48(1) requesting the body or association to develop a code; and (b) the matter or matters relating to the operation of digital communications platforms to be dealt with by the code that would be likely to be specified in the notice. The period specified under subparagraph 49(1) for the body or association to come into existence must be at least 60 days (subclause 49(2)).

There are no penalties for not forming a body or association. However, participants in a particular section of the digital platform industry would be required to comply with any standard determined by the ACMA under clause 56.

The ACMA is not required to publish a notice under clause 49 before determining a standard if there are exceptional and urgent circumstances (see clause 59).

Clause 50—Variation of misinformation codes

Clause 50 sets out the process that ACMA must follow before approving a draft variation to a registered misinformation code. The process is similar to the approval of a new code (clause 47), including in relation to body/association representation, applicability to participants, and providing a copy of the code to the ACMA (see paragraphs 50(1)(a)–(c), which are similar to paragraphs 47(1)(a)–(c)).

The factors of which the ACMA must be satisfied under paragraph 50(1)(d) before approving a draft variation of a code are the same as those of which the ACMA must be satisfied under paragraph 47(1)(d) before approving the code (namely that the code as proposed to be varied requires participants in that section of the digital platform industry to implement measures to prevent or respond to misinformation or disinformation on the platforms, enables the assessment of compliance with the measures, is reasonably appropriate and adapted to achieving the purpose of providing adequate protection for the Australian community from serious harm caused or contributed to by misinformation and disinformation on the platforms, and goes no further than reasonably necessary to provide that protection). These requirements are discussed further in the explanation to paragraph 47(1)(d) (on the approval of misinformation codes).

Except in a case where the draft variation is of a minor nature, the ACMA must be satisfied that participants of the relevant section of the digital platforms industry were invited to make submissions and that the submissions were considered, and that at least one body or association representing the interests of consumers was consulted about the proposed variation (per paragraphs 50(1)(f) and (g)). These requirements are similar to the requirements at 47(1)(f) and (g), in relation to the approval of codes. A draft variation would be considered minor if it did not alter any requirements on digital platform providers (for example, if it updated the name of the body or association that produced the code or involved corrections for typographical errors).

Period for making submissions

Subclause 50(2) provides that a period specified for submissions under subparagraphs 50(1)(e)(i) or 50(1)(f)(i) must run for at least 30 days.

Approval of draft variation

Subclause 50(3) provides that the ACMA may, by written notice given to the body or association, approve the draft variation. Subclause 50(4) provides that the draft variation, and the approval of the draft variation, are not legislative instruments. This provision is included to assist readers, as the instrument is not a legislative instrument within the meaning of subsection 8(1) of the Legislation Act. This is because the ACMA's approval of the draft variation in and of itself does not determine the law or affect privileges, interests, obligations or rights. Rather, it is a preliminary step before the variation, in the form of a legislative instrument, is lodged on the Federal Register of Legislation. The approved variation to the code will take effect once the legislative instrument varying the code is registered on the Federal Register of Legislation (see subclause 50(5)).

The legislative instrument varying the misinformation code in accordance with the ACMA's approval would be subject to parliamentary scrutiny and disallowance, and would be required

to be registered on the Federal Register of Legislation. As with the approval of the initial code, the ACMA would be responsible for preparing the explanatory statement, including statement of compatibility with human rights, for the variation instrument, and lodging the instrument and explanatory material for registration on the Federal Register of Legislation. The ACMA must be satisfied that any consultation that it considers is appropriate and reasonably practicable to undertake has been undertaken in relation to the variation of the misinformation code, per section 17 of the Legislation Act. It is anticipated that the consultation set out in paragraphs 50(1)(e), (f) and (g) would generally be sufficient for this purpose.

The ACMA would also be responsible for updating the misinformation code on its Register of misinformation codes and standards to incorporate the changes made by the variation instrument (see clause 64(4)).

In the event that an instrument varying a misinformation code were to be revoked or disallowed by Parliament in accordance with section 42 of the Legislation Act, the variation instrument would be repealed (immediately per subsection 42(1) of the Legislation Act in the case of disallowance). Accordingly, the ACMA would need to reverse any variation already incorporated into its electronic Register (subclause 64(6)). The previously approved misinformation code would remain binding on the relevant section of the digital platform industry.

If the ACMA refuses to approve a draft variation of a misinformation code, the body or association that developed the draft variation may apply to the ART for review of the decision (per the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 51—Revocation of misinformation codes and provisions of misinformation codes

Clause 51 provides that the ACMA may, by legislative instrument, revoke a misinformation code, or a provision of a misinformation code (subclause 51(1)). If the ACMA revokes a provision of the code, then Schedule 9 has effect in relation to things occurring after the revocation as if the code did not include the provision (subclause 51(2)).

Similarly to an instrument giving legal effect to an approved misinformation code, an instrument revoking a code is a legislative instrument as defined by section 8 of the Legislation Act. The ACMA would be required to prepare an explanatory statement, including a statement of compatibility with human rights, for the revocation instrument. The instrument of revocation would be subject to parliamentary scrutiny and disallowance, and would be required to be registered on the Federal Register of Legislation.

The ACMA would also be responsible for removing the revoked misinformation code or provision from the ACMA's Register kept under clause 64.

In the event that an instrument of revocation were to be disallowed by Parliament in accordance with section 42 of the Legislation Act, the instrument of revocation would be immediately repealed (per subsection 42(1) of the Legislation Act), and accordingly the misinformation code would remain in force on the Federal Register and on the ACMA's Register of misinformation codes and standards.
Examples of the reasons the ACMA may wish to revoke a code or a provision include:

- the code is no longer required as the industry body which developed the code no longer exists
- the code or provision has been superseded by a standard
- the code or provision is no longer necessary to protect the community from misinformation and disinformation
- the code or provision is replaced with a new code or provision.

Clause 52—Compliance with approved misinformation code

Subclause 52(1) provides that if a misinformation code approved under Division 4 of Part 2 that applies to a particular section of the digital platform industry is in force (paragraph (a)) and a digital communications platform provider is a participant in that section (paragraph (b)), the provider must comply with the code.

A code will come 'in force' when it has been approved, registered on the Federal Register of Legislation and commenced in accordance with its terms and section 12 of the Legislation Act. A code will cease to be 'in force' when repealed, which includes disallowance.

Subclause 52(2) provides that subclause 52(1) is a civil penalty provision.

Subclause 52(3) provides that an application for a civil penalty order for a contravention of subclause 52(1) must not be made under section 205F unless, before the contravention, the ACMA issued a formal warning to that person under clause 74 in relation to any contravention of subclause 52(1). This subclause does not require that a formal warning must have been issued in relation to *the particular* contravention in relation to which a proceeding is brought against a person, pursuant to subclause 52(3). Rather, it suffices that a warning was issued in relation to *any* contravention of subclause 52(1). This means that the ACMA need only issue one warning per digital communications platform provider, not one warning per contravention. Thus, if the ACMA issues a warning to a digital communications platform provider in relation to that provider's failure to comply with a particular aspect of a registered misinformation code, and that provider subsequently fails to comply with another aspect of that misinformation code, an application for a civil penalty order may be brought against that provider in relation to either its earlier or later contravention – without any requirement for a warning to be provided in relation to the later contravention.

Clause 73 provides that subclause 52(1) is a designated infringement notice provision, and clause 53 provides that the ACMA may issue a remedial direction in relation to a potential contravention of a misinformation code. Clause 74 provides that the ACMA can issue a warning in relation to the contravention of a misinformation code. For the avoidance of doubt, subclause 52(3) does not require that a formal warning be given to a digital communications platform provider prior to the issuance of a remedial direction or infringement notice.

Clause 53—Remedial directions—contravention of misinformation code

If the ACMA is satisfied that a digital communications platform provider has contravened or is contravening a code approved under Division 4 of Part 2 that is in force (subclause 53(1)), then subclause 53(2) empowers the ACMA to give the provider a written direction requiring

the provider to take specified action directed towards ensuring that the provider does not contravene the code or is unlikely to contravene the code in future.

A code is 'in force' when it has been approved, registered on the Federal Register of Legislation and commenced in accordance with its terms and section 12 of the Legislation Act.

Subclause 53(2) is to be interpreted in light of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument. Thus, the ACMA would be able to vary the requirements in a written direction provided pursuant to subclause 53(2), or revoke the direction, once provided.

Remedial directions can be used in the event of non-compliance if the ACMA considers it necessary to stipulate certain actions that should be taken to stop or reduce the likelihood of future non-compliance. These may be general, but they can also be specific. For example, the ACMA may use remedial directions to require that a non-compliant industry participant appoint an independent consultant to review processes or systems used by the provider to meet the code requirements. Remedial directions could be published.

Decisions to issue, vary or refuse to revoke, a remedial direction under subclause 53(2) are reviewable by the ART (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 75 provides that a direction under subclause 53(2) is taken to be a notice under Schedule 9 to the BSA for the purposes of the BSA and the ACMA Act. Clauses 77 and 78 provide for the service of notices under Schedule 9 to the BSA.

This would make clear that the ACMA may delegate the power to issue a remedial direction under section 51 of the ACMA Act, as the ACMA's power to issue notices under Schedule 9 can be delegated (see paragraph 53(2)(k) of the ACMA Act, to be amended by item 3 of Schedule 2 to the Bill). Notices under Schedule 9 are able to be served by electronic means without the consent of the recipient (see clause 77). In addition, if a corporation is incorporated outside Australia and does not have a registered or principal office in Australia, then a notice under Schedule 9 may be served on an agent of the corporation in Australia (see clause 78).

Subclause 53(3) provides that a digital communications platform provider must not contravene a direction under subclause 53(2).

Civil penalty provision

Subclause 53(4) provides that subclause 53(3) is a civil penalty provision.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5G) in the BSA, which provides that for persons who are body corporates the maximum penalty for a contravention of subclause 53(3) is 10,000 penalty units or 2% of the annual turnover of the body corporate during the turnover period (whichever is greater) and for persons who are not body corporates the maximum penalty is 2,000 penalty units.

SUBDIVISION D—MISINFORMATION STANDARDS

Under Subdivision D the ACMA may determine ***misinformation standards*** where a request for a code is not complied with (clause 55), where no industry body has been formed (clause 56), where there has been a total or partial failure of a misinformation code (clauses 57 and 58), or in exceptional and urgent circumstances (clause 59). Subdivision D also sets out the circumstances in which the ACMA may vary or revoke a misinformation standard, and the consequences for non-compliance.

The particular conditions with regards to which the ACMA must be satisfied in order to determine or vary a misinformation standard in various circumstances are discussed below. In all circumstances, the ACMA must be satisfied that the determination of a misinformation standard, or the variation thereof, is necessary to provide adequate protection for the Australian community from the risk of misinformation or disinformation on the digital communications platforms to which the standard applies. As with the equivalent requirement for the registration and variation of misinformation codes (subparagraphs 47(1)(d)(iii) and 50(1)(d)(iii)), the ACMA may only determine or vary a standard if it is satisfied that the determination of a standard is necessary to protect the Australian community from the risk that certain false, misleading or deceptive content disseminated on the digital communications platforms will cause or contribute to serious harm of a type described at clause 14.

Clause 54—Limitation in relation to freedom of political communication

Clause 54 requires that the ACMA must not determine a misinformation standard under Division 4 of Part 2 unless the ACMA is satisfied that the standard is reasonably appropriate and adapted to provide adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on the platforms (paragraph 54(a)). The standard must go no further than reasonably necessary to provide that protection (paragraph 54(b)).

As with the equivalent clauses in relation to the registration of misinformation codes and the making of digital platform rules, this requirement is aimed at ensuring that the power conferred on the ACMA is wholly valid, by making clear on the face of the legislation that the power it confers cannot be exercised in a way that would transgress the constitutional limits imposed by the implied freedom of political communication, which the High Court of Australia has recognised as impliedly protected by the Australian Constitution.[170] Freedom of political communication in this context means people's ability to communicate 'information and opinions about matters relevant to the exercise and discharge of governmental powers and functions on their behalf'.[171] The requirement that the ACMA consider the freedom of political communication, before exercising its power to determine a misinformation standard, recognises that this constitutionally implied freedom is a limitation on Parliament's legislative power to empower the ACMA to determine such a standard. It means that before determining a standard, the ACMA must carefully consider the way in which each of the measures contained in the standard burden the implied freedom of political communication, and whether in all the circumstances, the burden imposed by the standard overall is reasonable and not excessive.

[170] *Nationwide News* (n 166); *Australian Capital Television* (n 170).
[171] *Nationwide News* (n 166) 72 (Deane and Toohey JJ).

The test set out at clause 54 broadly aligns with the test endorsed by the High Court of Australia for assessing the consistency of Commonwealth legislation with the implied freedom of political communication. Pursuant to this test, Commonwealth legislation that burdens the freedom of political communication (either in its terms, operation or effect) must have a legitimate purpose, and be reasonably appropriate and adapted (or in other words, proportionate) to the achievement of that legitimate purpose.[172] This has been interpreted to mean that the burden on freedom of political communication must not be 'unreasonably greater than [would be] achievable by other means'.[173]

In the case of a misinformation standard, to the extent that measures in such a standard burden the freedom of political communication, such a burden would generally be considered justifiable if the standard was a necessary and proportionate response to the risk that misinformation or disinformation on digital communications platforms will cause serious harm – as described in clause 14 – in Australia.

There is an identical requirement in relation to the ACMA's power to vary a misinformation standard, discussed below (subclause 60(2)).

Clause 54 includes a note that an assessment of whether a standard is compatible with human rights must be prepared and included in the explanatory statement for the standard: see section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act.

Clause 55—ACMA may determine standards—request for a code is not complied with

Clause 55 empowers the ACMA to determine a standard if there has been a request for a code pursuant to subclause 48(1), and either: that request has not been complied with; or targets for progress in the development of the code have not been met; or the request was complied with, but the ACMA subsequently refused to register the code.

Subclause 55(1) sets out the circumstances that must apply. For the clause to apply, paragraph 55(1)(a) sets out that the ACMA must have made a relevant request under subclause 48(1). This request is in relation to the development of a code that is to apply to participants in a particular section of the digital platform industry (subparagraph (i)) and that is to deal with one or more matters relating to the operation of digital communications platforms by those participants (subparagraph (ii)).

One of the conditions listed in paragraph 55(1)(b) must also apply: (i) the request is not complied with; (ii) if indicative targets for achieving progress in the development of the code were specified in the notice of request—any of those indicative targets were not met; or (iii) the request is complied with but the ACMA subsequently refuses to approve the code.

Paragraph 55(1)(c) requires that the ACMA must also be satisfied that it is necessary for the ACMA to determine a standard in relation to that matter or those matters (see subparagraph 55(1)(a)(ii)) in order to provide adequate protection for the community from serious harm caused or contributed to by misinformation or disinformation on the platforms. The

[172] *Lange* (n 168); *LibertyWorks* (n 172) [45]-[46] (Kiefel CJ, Keane and Gleeson JJ), [93] (Gageler J), [134] (Gordon J), [200] (Edelman J), [247] (Steward J).
[173] *Coleman v Power* (n 169) [100] (McHugh J).

requirement expressed in paragraph 55(1)(c) is aimed at ensuring that misinformation standards determined under this clause do not infringe the freedom of political communication, which the High Court of Australia has recognised as impliedly protected by the Australian Constitution.

For the avoidance of doubt, if the ACMA has determined that a misinformation code is necessary, and its request for a misinformation code is not complied with, the matters that necessitated the request for a code in the first place may be identical or similar to the matters that would necessitate a standard under paragraph (c).

The ACMA is empowered by subclause 55(2) to determine a ***misinformation standard***, by legislative instrument, that applies to participants in that section of the digital platform industry and deals with that matter or those matters (see subparagraph 55(1)(a)(ii)).

Subclause 55(3) requires the ACMA to consult the body or association to whom the request to develop a code mentioned in paragraph 55(1)(a) was made before determining a standard under clause 55.

Clause 56—ACMA may determine standards—no industry body or association formed

Clause 56 applies in the circumstances set out in subclause 56(1): where the ACMA is satisfied that a particular section of the digital platform industry is not represented by a body or association (paragraph 56(1)(a)); the ACMA has published a notice under subclause 49(1) that meets the requirements of paragraph 56(1)(c) (paragraph 56(1)(b)); no such body or association comes into existence within the period specified in the notice (paragraph 56(1)(d)); and the ACMA is satisfied that it is necessary for it to determine a standard in relation to the matter or matters relating to the operation of digital communications platforms by participants in that section of the digital platform industry (as set out in the notice) in order to provide adequate protection for the community from serious harm caused or contributed to by misinformation or disinformation on digital communications platforms (paragraph 56(1)(e)). As for the identical test in paragraph 55(1)(c), the purpose of this requirement is to ensure that misinformation standards determined under this clause do not infringe the freedom of political communication, which the High Court of Australia has recognised as impliedly protected by the Australian Constitution.

Subclause 56(2) explains that the ACMA may determine a ***misinformation standard***, by legislative instrument, that applies to participants in the particular section of the digital platform industry and deals with that matter or those matters. Standards are a necessary tool to address misinformation and disinformation in the scenario where a body or association has not formed to seek to make a misinformation code.

Clause 57—ACMA may determine standards—total failure of misinformation code

Clause 57 applies in the circumstances set out in subclause 57(1): if a misinformation code approved under Division 4 of Part 2 of Schedule 9 has been in force for at least 180 days (paragraph 57(1)(a)); the ACMA is satisfied that the code is totally deficient as defined by subclause 57(6) (paragraph 57(1)(b)); the ACMA has given the body or association that developed the code a written notice requesting the deficiencies be addressed within a period of at least 30 days (paragraph 57(1)(c) and subclause 57(2)); and the ACMA is satisfied that it is necessary for it to determine a standard that applies to participants in that section of the

digital platform industry in relation to the matter or matters relating to the operation of digital communications platforms (as set out in the notice) in order to provide adequate protection for the community from serious harm caused or contributed to by misinformation or disinformation on the platforms (paragraph 57(1)(d)). As for the identical test in paragraphs 55(1)(c) and 56(1)(e), the purpose of this last requirement is to ensure that misinformation standards determined under this clause do not infringe the freedom of political communication, which the High Court of Australia has recognised as impliedly protected by the Australian Constitution.

If the conditions set out at subclauses 57(1) and 57(2) are satisfied, the ACMA may, by legislative instrument, determine a ***misinformation standard*** (subclause 57(3)).

Before the ACMA determines a misinformation standard under subclause 57(3), the ACMA must consult under subclause 57(4) a body or association, if any, that it is satisfied represents the particular section of the digital platform industry.

Subclause 57(5) provides that the misinformation code ceases to be in force on the day on which the standard commences. Clarification is also provided that subclause 57(5) does not affect any investigation, proceeding or remedy in respect of a contravention of the code that occurred before that day. Subclause 57(5) has been included for the avoidance of doubt, to clarify that if a particular digital communications platform is under investigation for non-compliance with a provision of a registered code, that investigation can continue, and a finding of non-compliance may be made, even if – during the course of the investigation – the code is replaced by a misinformation standard.

Subclause 57(6) explains that a misinformation code is ***totally deficient*** if, and only if, the code is not operating to provide adequate protection for the community from serious harm caused or contributed to by misinformation or disinformation on the digital communications platforms.

A finding that a code has failed to provide adequate community protection could be made, for example, on the basis of investigations undertaken by the ACMA – supported by the use of information-gathering powers in Division 3 of Part 2 of Schedule 9. It could also, for example, be made on the basis of widespread non-compliance with the misinformation code, necessitating the need for further regulatory intervention.

Clause 58—ACMA may determine standards—partial failure of misinformation code

Clause 58 empowers the ACMA to determine a standard where there has only been a partial failure of a misinformation code, in order to deal with matters in relation to which the code is deficient.

Clause 58 applies in the circumstances set out in subclause 58(1). These circumstances include that a misinformation code approved under Division 4 of Part 2 (that applies to participants in a particular section of the digital platforms industry and deals with 2 or more matters relating to the operation of the digital communications platforms by those participants) has been in force for at least 180 days (paragraph 58(1)(a)) and that clause 57 does not apply to the code (paragraph 58(1)(b)) (that is, the code is not totally deficient but is operating effectively in relation to at least one of the matters it deals with).

Subclause 58(1) also requires that:

- the ACMA is satisfied that the code's treatment of one or more of the matters it deals with is deficient (the ***deficient matter*** or ***deficient matters***) (paragraph 58(1)(c) and subclause 58(6))
- the ACMA has given the body or association that developed the code a written notice requesting that the deficiencies be addressed within a period not less than 30 days (paragraph 58(1)(d) and subclause 58(2))
- the ACMA is satisfied that it is necessary for it to determine a standard that deals with the deficient matter or deficient matters in order to provide adequate protection for the community from serious harm caused or contributed to by misinformation or disinformation on the digital communications platforms (paragraph 58(1)(e)). As for the identical test in paragraphs 55(1)(c), 56(1)(e), and 57(1)(d), the purpose of this last requirement is to ensure that misinformation standards determined under this clause do not infringe the freedom of political communication, which the High Court of Australia has recognised as impliedly protected by the Australian Constitution.

If the conditions set out at subclauses 58(1) and 58(2) are satisfied, the ACMA may, by legislative instrument, determine a ***misinformation standard*** (subclause 58(3)). Before doing so, the ACMA must have consulted with the body or association, if any, that represents the relevant section of the digital platform industry (subclause 58(4)).

Subclause 58(5) provides that on and after the day on which the standard commences, the partially deficient code ceases to be in force to the extent to which it deals with the deficient matter or deficient matters. However, the rest of the misinformation code continues in effect. Clarification is also provided that subclause 58(5) does not affect any investigation, proceeding or remedy in respect of a contravention of the code that occurred before that day.

Clause 59—ACMA may determine standards—emerging circumstances

Clause 59 applies if the ACMA is satisfied of the 3 matters listed at paragraphs 59(1)(a)–(c).

First, the ACMA must be satisfied that in order to provide adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on digital communications platforms, it is necessary for the ACMA to determine a standard (applying to a particular section of the digital platform industry and dealing with one or more matters relating to the operation of a digital communications platform) (paragraph 59(1)(a)). As for the identical test in paragraphs 55(1)(c), 56(1)(e), 57(1)(d) and 58(1)(e), the purpose of this requirement is to ensure that misinformation standards determined under this clause do not infringe the freedom of political communication, which the High Court of Australia has recognised as impliedly protected by the Australian Constitution.

Secondly, the ACMA must be satisfied that there are exceptional and urgent circumstances justifying the determination of the standard (paragraph 59(1)(b)). These circumstances may include a time of conflict, natural disaster, or a significant unforeseen public health event.

Thirdly, the ACMA must be satisfied that it is unlikely that a code dealing with that matter or matters could be developed under this Division within a reasonable period in the circumstances (paragraph 59(1)(c)). For example, if allowing industry time to develop a code in a period of at least 120 days (as provided for in subclause 48(2)) would expose the

community to inadequate protection from seriously harmful misinformation and/or disinformation, then a standard could be put in place to address the emerging circumstance(s).

Another potential reason that clause 59 may be enlivened is if the ACMA formed the view that a body or association(s) that could otherwise make codes was unwilling or unable to make a code that could be registered to address the emerging circumstances. Or, conversely, in particular circumstances, given the seriousness of the harm a body or association may prefer government to take the lead in setting out how digital communications platform providers must respond to misinformation and disinformation, rather than taking an active role in drafting provisions themselves.

Before the ACMA determines a ***misinformation standard***, by legislative instrument, under subclause 59(2), the ACMA must consult under subclause 59(3) a body or association, if any, that it is satisfied represents the relevant section of the digital platform industry.

Clause 60—Variation of misinformation standards

Subclause 60(1) provides that the ACMA may vary a misinformation standard, by legislative instrument, if it is satisfied that doing so is necessary to provide adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on the digital communications platforms to which the misinformation standard applies.

Subclause 60(2) requires that before varying a standard, the ACMA must be satisfied that the standard (as varied) is reasonably appropriate and adapted to achieving the purpose of providing adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation on the platforms, and goes no further than reasonably necessary to provide that protection. This is identical to the requirement provided at clause 54, in relation to the determination of a misinformation standard, as well as the requirements provided at paragraphs 47(1)(d) and 50(1)(d) regarding the approval and variation (respectively) of misinformation codes. An explanation of this requirement as it relates to misinformation standards is provided at clause 54.

Clause 61—Revocation of misinformation standards

Clause 61 provides that the ACMA may, by legislative instrument, revoke a misinformation standard. The ACMA could elect to revoke a misinformation standard if, for example:

- An industry body or association has formed, and has responded to a subsequent request to make an adequate misinformation code covering the matters that are otherwise dealt with in a standard.
- The emerging circumstance that necessitated that a misinformation standard be made under clause 59 no longer applies.
- A standard has been replaced or varied in its entirety.

Clause 62—Compliance with misinformation standard

Clause 62 sets out the requirement to comply with misinformation standards. The compliance and enforcement options available to the ACMA to enforce a misinformation standard are more immediate than for a misinformation code in that failure to comply with a misinformation standard could give rise to an application for a civil penalty order without the

ACMA first having given the person a formal warning (c/f subclause 52(3)). This is intentional, and reflects that the standard-making power is the most significant graduated power in Schedule 9.

Subclause 62(1) provides that a digital communications platform provider must comply with a misinformation standard that applies to participants in a particular section of the digital platform industry and is in force, if the provider is a participant in that section of the digital platform industry.

A standard will come 'in force' when it has been determined, registered on the Federal Register of Legislation and commenced in accordance with its terms and section 12 of the Legislation Act. A standard will cease to be 'in force' when repealed, which includes disallowance.

Subclause 62(2) provides that subclause 62(1) is a civil penalty provision.

Clause 73 provides that subclause 62(1) is a designated infringement notice provision and clause 74 provides that the ACMA can issue a warning in relation to its contravention.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5H) to the BSA, which provides that for persons who are body corporates the maximum penalty for a contravention of subclause 62(1) is 25,000 penalty units or 5% of the annual turnover of the body corporate during the turnover period (whichever is greater) and for persons who are not body corporates the maximum penalty is 5,000 penalty units.

Clause 63—Remedial directions—contravention of misinformation standard

Clause 63 empowers the ACMA to issue remedial directions in relation to contraventions of misinformation standards.

Clause 63 applies where a misinformation standard that applies to participants in a particular section of the digital platform industry is in force (paragraph 63(1)(a)) and the ACMA is satisfied that a digital communications platform provider who is a participant in that section (paragraph 63(1)(b)) has contravened, or is contravening, the standard (paragraph 63(1)(c)).

A standard will come 'in force' when it has been determined, registered on the Federal Register of Legislation and commenced in accordance with its terms and section 12 of the Legislation Act.

Subclause 63(2) provides that the ACMA may give the digital communications platform provider a written direction requiring the provider to take specified action to ensure the provider does not contravene the standard (or to ensure the provider is unlikely to contravene the standard) in the future. Subclause 63(2) is to be interpreted in light of subsection 33(3) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument. Thus, the ACMA would be able to vary the requirements in a written direction provided pursuant to subclause 63(2), or revoke the direction, once provided.

Decisions to issue, vary or refuse to revoke a remedial direction under subclause 63(2) are reviewable by the ART (see the amendments to subsection 204(1) of the BSA made by item 14 of Schedule 2).

Clause 75 provides that a direction under subclause 63(2) is taken to be a notice under Schedule 9 for the purposes of the BSA and the ACMA Act. Clauses 77 and 78 provide for the service of notices under Schedule 9 to the BSA.

Subclause 63(3) provides that a digital communications platform provider must not contravene a direction made under subclause 63(2).

Civil penalty provision

Subclause 63(4) provides that subclause 63(3) is a civil penalty provision.

Item 20 of Schedule 2 to the Bill inserts a new subsection 205F(5H) in the BSA, which provides that for persons who are body corporates the maximum penalty for a contravention of subclause 63(3) is 25,000 penalty units or 5% of the annual turnover of the body corporate during the turnover period (whichever is greater) and for persons who are not body corporates the maximum penalty is 5,000 penalty units.

SUBDIVISION E—REGISTER OF MISINFORMATION CODES AND MISINFORMATION STANDARDS

Clause 64—ACMA to maintain Register of misinformation codes and misinformation standards

Register

Clause 64 sets out the requirements for the Register of misinformation codes and misinformation standards. Subclause 64(1) explains that the Register maintained by the ACMA is to include:

- all misinformation codes approved under Division 4 of Part 2
- all misinformation standards
- all requests made under clause 48, and
- all notices under clause 49.

The Register is to be maintained by electronic means and made available for inspection on the internet (per subclauses 64(2) and (3)).

Variation of misinformation codes and misinformation standards

If an approved misinformation code is varied by legislative instrument under clause 50, the ACMA must update the version of the misinformation code included in the Register accordingly (per subclause 64(4)). The code on the Register should reflect the approved code as varied.

Similarly, if the ACMA varies a misinformation standard, the ACMA must update the misinformation standard included in the Register accordingly (per subclause 64(5)). The standard on the Register should reflect the standard as varied.

Revocation of misinformation codes and misinformation standards

If an approved misinformation code (or a provision of an approved misinformation code) is revoked or otherwise ceases to be in force, subclause 64(6) provides that the ACMA must remove the code or provision from the Register.

In addition to revocation under subclause 51(1), an approved misinformation code could also cease to be in force because it has been replaced by a standard in the event of a total failure of the code (see subclause 54(5)), or may partially cease to be in force in the event of a partial failure of the code (see subclause 58(5)). It could also cease to be in force because of external events such as disallowance (per subsection 42(1) of the Legislation Act) or sunsetting (per section 50 of the Legislation Act).

Similarly, if a misinformation standard or a provision of a misinformation standard is revoked or otherwise ceases to be in force, the ACMA must remove the standard or provision from the Register. In addition to revocation under clause 61, a standard could also cease to be in force because of external events such as disallowance (per subsection 42(1) of the Legislation Act) or sunsetting (per section 50 of the Legislation Act).

Legislative instruments

Subclause 64(8) provides that if the ACMA is required to include a legislative instrument in the Register, it is not required to do so until after the legislative instrument is registered under the Legislation Act (i.e. on the Federal Register of Legislation).

SUBDIVISION F—MISCELLANEOUS

Clause 65—Misinformation standards prevail over inconsistent misinformation codes

Clause 65 provides that a where an approved misinformation code that is applicable to a digital communications platform provider is inconsistent with a misinformation standard determined under Division 4 that is also applicable to the provider, the code has no effect to the extent of the inconsistency.

Clause 66—Digital platform rules prevail over inconsistent misinformation codes and standards

Clause 66 provides that an approved misinformation code or misinformation standard has no effect to the extent to which it is inconsistent with the digital platform rules.

DIVISION 5—GENERAL PROVISIONS

Division 5 sets out a few general matters clarifying removal of content and blocking end-users, the ACMA's investigation and hearings powers, annual reports by the ACMA, reviews of Part 2 of Schedule 9 and the relationship with other laws.

Clause 67—Removing content and blocking end-users

Subclause 67(1) provides that nothing in Part 2 of Schedule 9, or in the digital platform rules, approved misinformation codes or misinformation standards, requires a digital communications platform provider to:

- remove content where the dissemination is not disinformation on the platform involving inauthentic behaviour; or
- prevent an end-user from using a digital communications platform, where the end-user is not engaged in disinformation involving inauthentic behaviour.

This limitation reflects the fact that the measures set out in Schedule 9 to the BSA are focused on systems and processes, rather than the regulation of individual pieces of content or the behaviour of end-users. The provisions are intended to make clear that nothing in Part 2, or in any digital platform rules, approved codes or standards can require the removal of content or blocking of end-users unless the dissemination involves inauthentic behaviour. Subclause 67(1) ensures that the focus on systems and processes will be retained in all digital platform rules and misinformation codes and standards that are made, approved or determined respectively pursuant to Part 2 of Schedule 9.

The limitation expressed in subclause 67(1) does not prevent any other matters relating to the management of misinformation and disinformation from being included in misinformation codes or misinformation standards, including but not limited to the examples listed in clause 44.

Subclause 67(1) assists to ensure that to the extent that the measures in Schedule 9 restrict the freedom of expression, those measures – including the ACMA's regulatory powers, and the transparency obligations imposed on digital communications platform providers – are the least intrusive means available to protect people in Australia from the serious harm that can be caused by misinformation and disinformation on digital communications platforms. This ensures that, in line with Australia's obligations in relation to the right to freedom of expression in international human rights law, the measures are necessary and proportionate to the achievement of a legitimate goal.

Subclause 67(2) provides that while nothing in Part 2 of Schedule 9 *requires* a digital communications platform provider to remove specific content or block accounts except in the case of inauthentic behaviour, nothing in Part 2 *prevents* a digital communications platform provider from removing content or preventing an end-user from using their platform. This is consistent with Schedule 9's intention that digital communications platform providers – not the ACMA – must remain ultimately responsible for decisions about specific pieces of content hosted on their platforms, and about the end-users thereof. Thus, digital communications platform providers remain free to voluntarily remove content from their platforms in accordance with their own terms of use, whether or not that content is misinformation or disinformation as defined in clause 13. Similarly, digital communications platform providers remain free to voluntarily ban end-users from using their platforms in accordance with their own terms of use, whether or not those end-users have disseminated misinformation or disinformation as defined in clause 13.

Subclause 67(3) provides that clause 67 does not limit any other law that requires removal of content from a digital communications platform.

Clause 68—Investigations and hearings—limitation on scope

Clause 68 limits the scope to conduct investigations and hold hearings relating to misinformation and disinformation, ensuring that such investigations and hearings cannot relate to particular content posted on a digital communications platform by a single end-user identifiable by the ACMA.

Investigations

Section 117 of the BSA allows the ACMA to conduct investigations for the purposes of the performance or exercise of its broadcasting, content and datacasting functions and related powers. Section 171 of the BSA provides that the Minister may direct the ACMA in writing to investigate any matter with respect to which the Parliament can make laws under section 51(v) of the Constitution ('the communications power').

Subclause 68(1) limits the investigation power in section 117 of the BSA in relation to the ACMA's new misinformation and disinformation functions, inserted into section 10 of the ACMA Act (see item 2 of Schedule 2 to the Bill). An investigation for the purposes of these functions must not relate to content posted on a digital communications platform by a single end-user identifiable by the ACMA.

Similarly, subclause 68(2) provides that the Minister may not direct the ACMA to investigate particular content posted on a digital communications platform by a single end-user identifiable by the ACMA, despite section 171 of the BSA.

Hearings

Section 182 of the BSA allows the ACMA to hold hearings for the purposes of the performance or exercise of its broadcasting content and datacasting functions and related powers. Section 183 allows the Minister to direct the ACMA in writing to hold a hearing in relation to any matter in the interests of due administration of the BSA.

Subclause 68(3) limits the hearings power in section 182 of the BSA in relation to the ACMA's new misinformation and disinformation functions. A hearing for the purposes of these functions must not relate to content posted on a digital communications platform by a single end-user identifiable by the ACMA.

Similarly, subclause 68(4) provides that the Minister may not direct the ACMA to hold hearings regarding particular content posted on a digital communications platform by a single end-user identifiable by the ACMA, despite section 183 of the BSA.

Part 13 otherwise unaffected

Subclause 68(5) clarifies that Part 2 of Schedule 9 does not otherwise limit the operation of Part 13 of the BSA. Given the Bill inserts a new Schedule to the BSA, it picks up on existing powers in the BSA, including Part 13 (information gathering by the ACMA).

Clause 69—Annual reporting by ACMA

Clause 69 requires the ACMA to prepare a report, after the end of a financial year, on the operation of Part 2 of Schedule 9 during the financial year (paragraph 69(1)(a)). This could include commentary from the ACMA on the need for misinformation codes and misinformation standards. Under section 34C of the Acts Interpretation Act, the report will be required to be given to the Minister as soon as practicable after the end of the financial year.

The ACMA must give the report to the Minister for presentation to the Parliament (paragraph 69(1)(b)) (noting that the Minister must cause a copy of the report to be tabled within 15 sitting days under section 34C of the Acts Interpretation Act). The ACMA must cause a copy of the report to be published on the ACMA's website (subclause 69(2)).

The requirement for the ACMA to prepare a report applies in relation to any financial year that starts at or after the commencement of item 34 of Schedule 2 to the Bill (see subitem 34(3) of that Schedule).

Clause 70—Review of operation of this Part

Clause 70 provides for a triannual review of the operation of Part 2 of Schedule 9. The Minister is to set up a review as soon as possible after the third anniversary of commencement of Schedule 9 and afterwards at intervals of no longer than 3 years (subclause 70(1)).

The review must provide for public consultation (subclause 70(3)) and is to include an assessment of the impact of Part 2 on freedom of expression (paragraph 70(2)(a)) and consider whether Part 2 should be amended (paragraph 70(2)(b)).

The first time the review is conducted, consideration must be given to whether there is a need for Part 2 of Schedule 9 to be amended to include a scheme for third party data access (paragraph 70(2)(c)). Such a scheme would involve requiring digital communications platform providers to give accredited independent researchers access to data regarding misinformation or disinformation on digital communications platforms. The European Union (EU) has been consulting since early 2023 on the development of a third-party data sharing regime including governance, privacy and data access charges. The first triennial review may consider developments in the EU and in other jurisdictions.[174] Furthermore, by the time of the first review of Part 2 of Schedule 9, more information would be known on whether the information provided by digital communications platform providers pursuant to subclauses 17(1) and (4), and records/reports to the ACMA by digital communications platforms, can be substantiated without data access for researchers.

A report of the review is required (subclause 70(4)) and must be tabled in each House of the Parliament within 15 sitting days of completion (subclause 70(5)).

Clause 71—Relationship with other laws

Clause 71 states that Part 2 of Schedule 9 (misinformation and disinformation), digital platform rules made for the purposes of the Part, approved misinformation codes and misinformation standards do not limit the operation of:

[174] At the time of writing, regulations have not been made under *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services amending Directive 2000/31/EC (Digital Services Act)* [2022] OJ L 277, art 40(13).

a) Schedule 8 to the BSA;
b) the *Commonwealth Electoral Act 1918*;
c) the Competition and Consumer Act;
d) the *Criminal Code;*
e) Parts 4 and 9 of the Online Safety Act (about basic online safety expectations and the online content scheme);
f) the *Referendum (Machinery Provisions) Act 1984*;
g) the Telecommunications Act.

Schedule 8 to the BSA confers power on the ACMA to make rules about gambling promotional content provided on an online content service in conjunction with a live sporting event, and to give remedial directions to online content service providers that contravene specified rules.

The Australian Consumer Law (Schedule 4 to the Competition and Consumer Act) prohibits certain business practices and creates various enforceable rights for consumers. Of particular note, section 18 of the Australian Consumer Law prohibits conduct, in trade or commerce, that is misleading or deceptive or is likely to mislead or deceive. It is not intended that a misinformation code approved, or a misinformation standard determined, under Part 2 of Schedule 9 be construed to affect, exclude or interpret the Australian Consumer Law. Where a person has an obligation under the Australian Consumer Law, this should also be complied with separately.

It is intended that the measures in the Bill complement existing offences in the *Criminal Code Act 1995*. This includes, for example, offences for content or hosting service providers to host abhorrent violent material in Subdivision H of Division 474 of the Criminal Code. Subdivision H also requires internet, content and hosting service providers to notify the police of abhorrent violent material hosted on their services. If the elements of the offence of incitement in section 11.4 of the Criminal Code were satisfied, it is likely that using a digital communications platform to disseminate false, misleading or deceptive content that would be reasonably likely to result in the intentional infliction of physical injury – in other words, content satisfying the definition of misinformation or disinformation.

It is an offence under section 329 of the *Commonwealth Electoral Act 1918* to publish or distribute anything likely to mislead or deceive an elector in relation to the casting of a vote, during the election period, and there is an equivalent offence in section 122 of the *Referendum (Machinery Provisions) Act 1984*, in relation to referendums.

Part 4 of the Online Safety Act allows the Minister to determine basic online safety expectations for social media services, relevant electronic services and designated internet services including requiring the provider of those services to provide reports about compliance with those expectations. Part 9 of that Act provides for an online content scheme, which provides for industry codes and standards in relation to online content and includes powers to require removal of online content in certain circumstances.

Under Part 6 of the Telecommunications Act, bodies and associations that represent sections of the telecommunications industry, the telemarketing industry or the fax marketing industry may develop industry codes, which may be registered by the ACMA.

PART 3—MISCELLANEOUS

Part 3 sets out miscellaneous matters: enforcement (Division 1), other matters (Division 2) and the power to make digital platform rules (Division 3).

DIVISION 1—ENFORCEMENT

The enforcement powers in Division 1 of Part 3 of Schedule 9 draw on the ACMA's existing enforcement framework under the BSA. The ACMA's graduated approach to compliance and enforcement is set out in the ACMA's general compliance and enforcement policy and the *Broadcasting Services – Enforcement Guidelines of the ACMA 2021*.[175] These Guidelines set out the following:

The ACMA adopts a strategic risk-based approach to compliance and enforcement. The decision as to what, if any, enforcement action should be taken by the ACMA is made in the light of the facts of the matter and having regard to the objects of the BSA and the regulatory policy underpinning it (sections 3 and 4 of the BSA).

The ACMA's compliance and enforcement approach is to take action that is commensurate with the seriousness of the conduct which includes consideration of the nature and consequences of the conduct (section 5 of the BSA).

Where the ACMA is of the view that a regulatory breach has occurred, the ACMA will take regulatory action commensurate with the seriousness of the breach and the level of harm. The ACMA will generally use the minimum power or intervention necessary to achieve the desired result, which, in many cases, is compliance with the relevant obligation.

The ACMA's approach to enforcement will always be influenced by the particular facts and circumstances of each case and how the ACMA Authority or delegate is minded to address non-compliance at any given time.

In deciding which compliance or enforcement option or combination of options to use, the ACMA considers a range of factors including:

- the relevant regulatory objective
- whether the conduct was deliberate, inadvertent or reckless
- whether the conduct has caused, or may cause, detriment to another person, and the nature, seriousness and extent of that detriment
- whether the conduct indicates systemic issues that may pose ongoing compliance or enforcement issues
- whether the person (provider) has been the subject of prior compliance or enforcement action and the outcome of that action
- the personal and general educative/deterrent effect of acting
- the seniority and level of experience of the person/s involved in the conduct
- what, if any, action has been taken to remedy and address the consequences of the conduct
- whether the subject of the investigation has cooperated with the ACMA

[175] ACMA, 'Compliance and enforcement policy' (29 January 2024) <Compliance and enforcement policy | ACMA>; *Broadcasting Services – Enforcement Guidelines of the ACMA 2021* (Cth), available on the Federal Register of Legislation <https://www.legislation.gov.au/F2021L01123/latest/text>.

- whether the issues involved require urgent action/intervention by the ACMA.

Clause 72—Separate contraventions

Clause 72 provides that the contravention of each provision listed is a separate contravention of that provision for each day the contravention continues.

Clause 73—Designated infringement provisions

Clause 73 lists the provisions that are designated infringement notice provisions. Part 14E of the BSA sets out a system of infringement notices for contravention of designated infringement notice provisions as an alternative to the institution of court proceedings. Part 14E of the BSA provides detail about matters such as when an infringement notice can be given, what should be included in an infringement notice and penalty amounts.

Clause 74—Warnings

Subclause 74(1) lists the provisions in relation to which the ACMA can issue a formal warning if the ACMA is satisfied that a person has contravened the provision in question.

This subclause is intended to enable the ACMA to formally communicate its concerns about a contravention of a civil penalty provision. It may, for example, be issued in relation to minor contraventions where a simple warning is likely to cause a change in behaviour. The issuing of a formal warning does not prevent the ACMA from initiating proceedings for a contravention of a civil penalty provision.

Subclause 74(2) provides that for the purposes of the BSA and the ACMA Act, a warning given under subclause 74(1) is taken to be a notice under Schedule 9 to the BSA. The ACMA's power to issue notices under Schedule 9 can be delegated (see paragraph 53(2)(k) of the ACMA Act, to be amended by item 3 of Schedule 2 to the Bill). Notices under Schedule 9 are able to be served by electronic means without the consent of the recipient (see clause 77). In addition, if a corporation is incorporated outside Australia and does not have a registered or principal office in Australia, then a notice under Schedule 9 may be served on an agent of the corporation in Australia (see clause 78).

Clause 75—Remedial directions

Subclause 75(1) lists the provisions under which the ACMA can issue a remedial direction and provides that a remedial direction under those provisions is taken to be a notice under Schedule 9 to the BSA for the purposes of the BSA and the ACMA Act. The ACMA's power to issue notices under Schedule 9 can be delegated (see paragraph 53(2)(k) of the ACMA Act, to be amended by item 3 of Schedule 2 to the Bill). Notices under Schedule 9 are able to be served by electronic means without the consent of the recipient (see clause 77). In addition, if a corporation is incorporated outside Australia and does not have a registered or principal office in Australia, then a notice under Schedule 9 may be served on an agent of the corporation in Australia (see clause 78).

Subclause 75(2) explains that a direction under any of the provisions mentioned in subclause 75(1) is not a legislative instrument. This is a declaratory provision rather than an exemption because the directions are not of a legislative character.

The ACMA will be empowered to give a provider a written direction requiring the provider to take specified action (including specifying the compliance time for this action) directed towards ensuring that a clause is not contravened, or is not likely to be contravened, in the future.

In some cases, a contravention of a remedial direction will also be a continuing offence in respect of each day during which the contravention continues (see clause 72).

Clause 76 — No ancillary contravention of civil penalty provisions in this Schedule

Clause 76 provides that section 205E (ancillary contravention of civil penalty provision) does not apply in relation to a civil penalty provision in Schedule 9. The purpose of excluding ancillary contraventions is due to the risk that if section 205E was applied to the clauses in Schedule 9, it could apply more broadly than intended to inadvertently capture end-users and make them liable for civil penalties. For example, if a code or standard contained a general obligation on platforms to minimise the spread of misinformation or disinformation, an individual who then spread that verifiably false content widely could be seen to be aiding or abetting a contravention of the code or standard.

DIVISION 2—OTHER MATTERS

Clause 77—Service of notices by electronic means

Clause 77 provides that paragraphs 9(1)(d) and 9(2)(d) of the *Electronic Transactions Act 1999* do not apply to a notice under Schedule 9 (or a notice under any other provision of the BSA, so far as that provision relates to Schedule 9). Paragraphs 9(1)(d) and 9(2)(d) of the *Electronic Transactions Act 1999* deal with the consent of the recipient of information to the information being given by way of electronic communication (as explained in the note). A requirement for consent is not considered appropriate in circumstances where the ACMA may frequently have access to electronic contact details only.

Clause 78—Service of summons, process or notice on corporations incorporated outside Australia

Clause 78 is a deeming provision setting out the circumstances in which certain summons, processes or notices under or in connection with Schedule 9 (see paragraphs 78(1)(a) to (c)) will be taken to have been served on, or given to, an overseas body corporate. Clause 78 has the effect that where the body corporate incorporated outside of Australia does not have a registered or principal office in Australia (paragraph 78(1)(e)) but has an agent in Australia (paragraph 78(1)(f)), then a summons, process or notice will be deemed to have been served on, or given to, the body corporate where it is served on or given to the body corporate's agent in Australia (subclause 78(2)).

Subclause 78(3) clarifies that subclause 78(2) does not override section 28A of the Acts Interpretation Act and instead, operates in addition to that provision. Section 28A deals with the service of documents. Paragraph 28A(1)(b) provides that a document may be served on a body corporate by leaving it at, or sending it by pre-paid post to, the head office, a registered office or a principal office of the body corporate.

Clause 79—Acquisition of property

Clause 79 provides that the provisions of Schedule 9 have no effect to the extent to which their operation would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from a person otherwise than on just terms.

Clause 80—Concurrent operation of State and Territory laws

In accordance with clause 80, it is the intention of the Parliament that Schedule 9 is not to 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 Schedule 9.

Clause 80 is intended to allow different State or Territory laws that address other aspects of the harms mentioned in Schedule 9, for example, to operate concurrently with Schedule 9 insofar as possible.

Clause 81—Schedule not to affect performance of State or Territory functions

Clause 81 provides that a power conferred by Schedule 9 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.

This will prevent any unintended interference with the activities of the State or Territory governments (for example, their activities in relation to certain harms).

DIVISION 3—DIGITAL PLATFORM RULES

Clause 82—Digital platform rules

Subclause 82(1) provides that the ACMA may make rules, by legislative instrument, referred to as the ***digital platform rules***. The rules can prescribe matters required or permitted by the BSA to be prescribed by the digital platform rules or necessary or convenient to be prescribed for carrying out or giving effect to Schedule 9.

The effect of this subclause is that the ACMA may make digital platform rules in relation to all matters which are described in Schedule 9 as capable of being prescribed or further defined in digital platform rules. These matters are:

- the maximum number of end-users to which a message may be sent from an end-user using a digital communications platform, in order to be considered a private message (clause 2)
- additional conditions required to be satisfied in order for a digital service to be considered a connective media service, a content aggregation service, an internet search engine service or a media sharing service (clause 5)
- additional circumstances in which dissemination of content on a digital service will be considered to involve inauthentic behaviour (clause 15)
- additional rules to which a person may be subject, in order to be considered capable of producing professional news content (subparagraph 16(2)(b)(v))
- requirements for reports on the outcomes of risk assessments relating to misinformation and disinformation on digital communications platforms (paragraph 17(1)(a))

- additional types of information, other than source code, required to be published by digital communications platform providers (paragraph 17(1)(d))
- certain matters relating to risk management (clause 19)
- certain matters relating to media literacy plans (clause 22)
- complaints and dispute handling processes for misinformation complaints (clause 25)
- digital communications platforms who are exempt from Division 2 (Transparency obligations) of Part 2 (clause 29)
- requirements for digital communications platform providers to make and retain records relating to misinformation and disinformation, and measures implemented by digital communications platform providers to prevent or respond to misinformation or disinformation on digital communications platforms, and to prepare reports consisting of information contained in those records (clause 30)
- kinds of digital communications platforms whose providers constitute a section of the digital platform industry for the purposes of Schedule 9 (clause 42)
- providing that decisions of the ACMA under the digital platform rules are reviewable decisions for the purposes of section 204 of the BSA (appeals to the Administrative Appeals Tribunal) (subsection 204(4A) of the BSA inserted by item 15 of Schedule 2 to the Bill).

The rules made by the ACMA under subclause 82(1) are a legislative instrument for the purposes of the Legislation Act. This means that the rules would be subject to parliamentary disallowance and would be registered on the Federal Register of Legislation. They would be required to be accompanied by a statement of compatibility with human rights, to be included in the explanatory statement for the rules, in accordance with section 9 of the Human Rights (Parliamentary Scrutiny) Act and section 15J of the Legislation Act. Pursuant to subsection 33(3) of the Acts Interpretation Act, the ACMA could vary the requirements specified in the digital platform rules by legislative instrument, or revoke the digital platform rules, also by legislative instrument.

The ACMA's power to make digital platform rules should be read in light of subsection 33(3A) of the Acts Interpretation Act, which provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character with respect to particular matters, the power shall be construed as including a power to make, grant or issue such an instrument with respect to some only of those matters or with respect to a particular class or classes of those matters and to make different provision with respect to different matters or classes of matters. This means that the ACMA may make digital platform rules that apply to all digital communications platform providers, or it may make digital platform rules that apply only to a class of digital communications platform providers or to a section or sections of the digital platform industry.

Subclause 82(2) is a standard provision clarifying the limitations on the power to make rules. To avoid doubt, the rules cannot:

- create an offence or civil penalty;
- provide coercive enforcement powers;
- impose a tax;
- set an amount to be appropriated from the Consolidated Review Fund; or
- directly amend the text of the BSA.

Subclause 82(3) clarifies that digital platform rules may make provision for or in relation to a particular matter by empowering the ACMA to make decisions of an administrative character. This is to avoid any doubt that the Parliament intends the ACMA to, for example, be able to make rules that would operate on the basis of the ACMA's administrative discretion in appropriate cases.

In connection with subclause 82(3), item 15 of Schedule 2 to the Bill inserts new subsection 204(4A) into the BSA, providing that an application may be made to the ART for review of a decision of the ACMA under the digital platform rules, where the rules provide that the decision is reviewable for the purposes of section 204 of the BSA.

Subclause 82(4) is a standard provision that ensures relevant regulations prevail over any inconsistent digital platform rules.

SCHEDULE 2—CONSEQUENTIAL AMENDMENTS AND TRANSITIONAL PROVISIONS

PART 1—MAIN AMENDMENTS AND TRANSITIONAL PROVISIONS

Australian Communications and Media Authority Act 2005

Items 1 to 3 of Schedule 2 amend the ACMA Act.

Item 1—Section 3 (subparagraph (b)(i) of the definition of authorised disclosure information)

Item 1 amends the definition of ***authorised disclosure information*** in section 3 of the ACMA Act so that the term includes information obtained by the ACMA as a result of the exercise of its powers under Schedule 9 to the BSA. This means that the information dealt with in Schedule 9 can be disclosed under Part 7A of the ACMA Act in certain circumstances. For example, section 59D of the ACMA Act permits an ACMA official authorised by the Chair, in writing, for the purposes of that section to disclose 'authorised disclosure information' (ADI) to certain authorities if satisfied that the information will enable or assist the authority to perform or exercise any of its functions or powers.

Item 2—After paragraph 10(1)(ma)

Item 2 adds the following functions to the list of the ACMA's broadcasting, content and datacasting functions in subsection 10(1) of the ACMA Act:

> *(mb) to assist bodies or associations that the ACMA is satisfied represent sections of the digital platform industry to develop codes under Division 4 of Part 2 of Schedule 9 to the BSA;*
>
> The intention is to provide the ACMA with the function to assist digital platform industry bodies or associations to develop codes requiring participants in those sections of the digital platform industry to implement measures to prevent or respond to misinformation and disinformation on their digital communications platforms, and to approve those codes if certain requirements are met.

(mc) to develop standards under Division 4 of Part 2 of Schedule 9 to the BSA;

The intention is to provide the ACMA with the function to determine misinformation standards for the digital platform industry through a legislative instrument. Misinformation standards could be made where a request for a code is not complied with, where no industry body or association has been formed, where there has been a total or partial failure of a misinformation code, or to address emerging circumstances. Measures included in misinformation standards attract higher penalties than measures included in misinformation codes, reflecting the graduated nature of the powers. A standard made by the ACMA could apply to one or more sections of the industry.

(md) to monitor compliance with Schedule 9 to the BSA, digital platform rules, misinformation codes and misinformation standards;

The intention is to provide the ACMA with the function to monitor digital communications platform providers' compliance with misinformation codes and misinformation standards made under Division 4 of Part 2 of Schedule 9 to the BSA, and digital platform rules made under clause 82 of that Schedule. This could include, for example, monitoring compliance with digital platform rules requiring providers to keep records and provide reports to the ACMA as mentioned in clause 30 of that Schedule.

(me) to conduct investigations relating to misinformation and disinformation on digital communications platforms;

The intention is to provide the ACMA with the function to conduct investigations into digital communications platform providers' compliance with their obligations under Schedule 9 to the BSA, the digital platform rules, misinformation codes and misinformation standards. Investigations and hearings powers in relation to the ACMA's misinformation and disinformation functions are intended to be limited in scope, in that they must not relate to particular content posted on a digital communications platform by a single end-user identifiable by the ACMA (see clause 68 of Schedule 9 to the BSA).

(mf) to inform itself and advise the Minister in relation to misinformation and disinformation on digital communications platforms;

The intention of this function is that the information gathered from digital communications platform providers and other persons regarding misinformation or disinformation on digital communications platforms and measures taken to prevent or respond to it, could inform analysis by the ACMA and advice to the Minister on the effectiveness of providers' measures to combat misinformation and disinformation on their platforms.

(mg) to make available to the public information about matters relating to misinformation and disinformation on digital communications platforms;

The intention of this function is to provide greater transparency and insights into the effectiveness of providers' measures to combat misinformation and disinformation on their platforms, empowering Australians by providing them with greater visibility of how digital communications platform providers manage online misinformation and disinformation. The ACMA may publish information on its website in line with Subdivision C of Division 3 of Part 2 of Schedule 9 to the BSA, which may include insights that arise from the ACMA's analysis and assessment of providers' measures to combat misinformation and disinformation on their platforms.

Inclusion of these functions in respect of misinformation and disinformation brings digital communications platforms within scope of the ACMA's remit. The added functions align with the ACMA's existing functions that deal with broadcasting, content, datacasting and telecommunications.

Item 3—Paragraph 53(2)(k)

Item 3 adds a reference to Schedule 9 to the BSA after the reference to Schedule 8 in paragraph 53(2)(k) of the ACMA Act. Section 53 of the ACMA Act limits the power of the ACMA, or a Division of the ACMA, to delegate functions and powers under sections 51 and 52 of that Act. Paragraph 53(2)(k) limits the ability to delegate powers to issue, or extend the time for compliance with, notices, with some specified exceptions. Item 3 would provide that notices under Schedule 9 are an exception (i.e. the power to issue or extend the time for compliance with a notice under Schedule 9 *can* be delegated).

Broadcasting Services Act 1992

Items 4 to 29 of Schedule 2 amend the BSA.

Item 4—Title

Item 4 adjusts the long title to the BSA to replace 'and content services' with ', content services and digital communications platforms'. As amended, the long title will be 'An Act relating to broadcasting services, broadcasting video on demand services, datacasting services, online services, content services and digital communications platforms, and for related purposes'.

Item 5—After paragraph 3(1)(hb)

Item 5 adds the following objects of the BSA to the list of objects in in subsection 3(1):

(hc) to encourage digital communications platform providers to protect the Australian community against certain kinds of harm caused or contributed to by misinformation or disinformation on digital communications platforms; and

The intention is to encourage digital communications platform providers to have measures in place to protect the Australian community against the harms identified in clause 14 of Schedule 9, including through measures such as content authentication and media literacy initiatives.

(hd) to provide end-users in Australia with visibility in relation to decision-making by digital communications platform providers in managing misinformation and disinformation on digital communications platforms; and

The intention is to increase transparency for end-users in Australia around actions undertaken by digital communications platform providers to identify and address misinformation and disinformation. The ACMA may publish information relating to misinformation or disinformation on its website in line with Subdivision C of Division 3 of Part 2 of Schedule 9.

(he) to strengthen transparency and accountability requirements in relation to misinformation and disinformation on digital communications platforms;

The intention is to improve public awareness and visibility about the policies and measures adopted by digital communications platforms to manage misinformation and disinformation on their services.

These objects are included to cover, in particular:

- the obligations imposed on a digital communications platform provider to publish their current policy or policy approach in relation to misinformation and disinformation, a report on the outcomes of their assessment of risks relating to misinformation and disinformation on the platform, a current media literacy plan, and any other information (other than source code) specified in digital platform rules, as set out in Division 2 of Part 2 of Schedule 9 (the 'transparency' obligations)
- the ACMA's power to make digital platform rules in relation to complaints and dispute handing processes for misinformation complaints, also set out in Division 2 of Part 2 of Schedule 9
- the ACMA's power to make digital platform rules with regards to record keeping and reporting, set out in Subdivision A of Division 3 of Part 2 of Schedule 9
- the ACMA's information-gathering and publishing powers, set out in Subdivisions B and C of Division 3 of Part 2 of Schedule 9
- the ACMA's powers to approve and determine (respectively) misinformation codes and misinformation standards, set out in Division 4 of Part 2 of Schedule 9
- the ACMA's power to take action in relation to non-compliance by digital communications platform providers with the obligations set out in Schedule 9, or in rules, codes or standards that are made, approved or determined pursuant thereto.

Item 6—At the end of subsection 3(1)

Item 6 inserts a note at the end of subsection 3(1) of the BSA to draw attention to the further objects of Part 2 of Schedule 9 that are set out in clause 11 of Schedule 9.

Item 7—Subsection 3(2)

Item 7 inserts signpost definitions into subsection 3(2) of the BSA to indicate that key terms used in the new objects in paragraphs 3(1)(hc) to (he) of the BSA have the same meaning as in Schedule 9 to the BSA (namely the terms 'digital communications platform', 'digital communications platform provider', 'disinformation' and 'misinformation').

Item 8—After subsection 4(3AB)

Section 4 of the BSA sets out the Parliament's regulatory policy intentions behind the BSA. Item 8 inserts a new subsection 4(3AC) which sets out the Parliament's regulatory policy intention in relation to misinformation and disinformation on digital communications platforms, specifically that digital communications platforms be regulated in a manner that:

- enables public interest considerations in relation to misinformation and disinformation on digital communications platforms to be addressed in a way that does not impose unnecessary financial and administrative burdens on digital communications platform providers; and
- will readily accommodate technological change; and
- encourages the provision of digital communications platforms to the Australian community; and
- encourages the development of technologies relating to digital communications platforms.

This amendment supports the intent that digital communications platforms are accessible to Australian end-users and that the matters in Schedule 9 to the BSA should not unduly limit the adoption of new technologies in the industry for Australians.

Item 9—Subsection 4(4)

Item 9 inserts signpost definitions into subsection 4(4) of the BSA to indicate that key terms used in subsection 4(3AC) of the BSA have the same meaning as in Schedule 9 to the BSA (namely the terms 'digital communications platform', 'digital communications platform provider', 'disinformation' and 'misinformation').

Item 10—Paragraph 5(1)(a)

Section 5 of the BSA sets out the role of the ACMA. Item 10 amends paragraph 5(1)(a) to make it clear that the ACMA has responsibility for monitoring the digital communications platform industry. This is in addition to the ACMA's existing responsibility for monitoring the broadcasting industry, the broadcasting video on demand industry, the datacasting industry and the online content service industry.

Item 11—Subsection 5(4)

Item 11 inserts a signpost definition into subsection 5(4) of the BSA to explain that 'digital communications platform' has the same meaning in section 5 as it does in Schedule 9 to the BSA.

Item 12—Subsection 6(1) (definition of newspaper)

Item 12 amends the definition of 'newspaper' in subsection 6(1) of the BSA so that the definition does not apply in Schedule 9 to the BSA. In Schedule 9, the term 'professional news content' is defined in subclause 16(2). That definition contains a reference to 'newspaper' (see subparagraph 16(2)(a)(i)) which is intended to take its ordinary meaning.

Item 13—Subsection 98D(2)

Subsection 98D(2) of the BSA provides that if the operation of the BSA, aside from certain excluded provisions, would result in the acquisition of property from a person otherwise than on just terms, then the Commonwealth is liable to pay compensation of a reasonable amount to the person in respect of the acquisition.

Item 13 amends subsection 98D(2) so that it does not apply to Schedule 9. This is because clause 79 of Schedule 9 deals with acquisition of property under that Schedule, and provides that the provisions of Schedule 9 are to be read down so that they do not operate in a way that would result in an acquisition of property otherwise than on just terms. Therefore, there will be no need for compensation under subsection 98D(2).

Item 14—Subsection 204(1) (at the end of the table)

Section 204 of the BSA sets out in table form decisions under the BSA in relation to which an application for review may be made to the ART, and who may make such an application.

Item 14 adds 6 additional rows to this table. The first three rows to be added to the table allow a person to whom a remedial direction is given under subclauses 18(2), 21(2), 24(2), 27(2), 32(2), 53(2) or 63(2) of Schedule 9 to seek review of a decision to give, vary, or refuse to revoke that direction.

The fourth row allows a person to whom a notice was given under subclause 40(2) of Schedule 9 to seek review of a decision to publish information under clause 38 of Schedule 9.

The fifth and sixth rows to be added to the table in section 204 of the BSA allow a body or association that developed a misinformation code, or a draft variation of a misinformation code, to seek review of a decision under subclause 47(3) of Schedule 9 to refuse to approve the misinformation code or part of a misinformation code, or a decision under subclause 50(3) of Schedule 9 to refuse to approve a draft variation of a misinformation code, respectively.

Item 15—After subsection 204(4)

Item 15 inserts new subsection 204(4A) into the BSA, providing that an application may be made to the ART for review of a decision of the ACMA under the digital platform rules, so long as those rules provide that the decision is a reviewable decision for the purposes of section 204.

This item is included in connection with subclause 82(3) of Schedule 9 to the BSA, which clarifies that digital platform rules may make provision for or in relation to a particular matter by empowering the ACMA to make decisions of an administrative character. As some, but not all, decisions the ACMA may empower itself to make under those provisions may be appropriate for merits review, subsection 204(4A) would enable the ACMA, in developing rules, to provide for merits review where it is appropriate. For example, it is likely the ACMA would provide for merits review where its decision would affect the interests of a person, but

that it may not be necessary to do so where decisions would be of a procedural or preliminary nature, would have no appropriate remedy or would have such limited impact that the costs of review cannot be justified.

Item 16—Subsection 204(5) (heading)

Item 16 removes the current heading from subsection 204(5) of the BSA ('Online content service provider rules') and replaces it with the heading 'Definitions'. This change is made as a consequence of item 17, which inserts a definition into subsection 204(5) that does not relate to the online content service provider rules.

Item 17—Subsection 204(5)

Item 17 inserts a new signpost definition of the term 'digital platform rules' (used in subsection 204(4A), which is inserted by item 15) to explain that the term has the same meaning in section 204 as in Schedule 9 to the BSA.

Item 18—At the end of section 205E

Subsection 205E of the BSA sets out a civil penalty provision for the ancillary contravention by a person of another civil penalty provision in the BSA (for example, aiding or abetting a contravention). Clause 76 of Schedule 9 to the BSA (inserted by Schedule 1 to the Bill) provides that section 205E of the BSA does not apply in relation to a civil penalty provision in Schedule 9. The rationale for disapplying section 205E is set out in the explanation of clause 76. Item 18 adds a note at the end of section 205E to refer to, and explain the effect of, clause 76.

Item 19—Subsection 205F(4)

Subsection 205F(1) provides that if the Federal Court is satisfied that a person has contravened a civil penalty provision, the Federal Court may order the person to pay the Commonwealth a pecuniary penalty.

Subsection 205F(4) provides that the maximum penalties for the contravention of many of the civil penalty provisions in the BSA are currently set with reference to the maximum penalty that can be imposed on a person convicted of a corresponding criminal offence.

Schedule 9 to the BSA includes several civil penalty provisions. However, it does not create corresponding criminal offences. Item 19 therefore amends subsection 205F(4) to exclude a provision in Schedule 9 to the BSA from the operation of that subsection.

Item 20—After subsection 205F(5D)

Item 20 inserts subsections 205F(5E) to (5H) to set out maximum penalty amounts in relation to the contravention of civil penalty provisions in Schedule 9.

Subsection 205F(5E) provides that the pecuniary penalty payable by a person in respect of a contravention of a civil penalty provision in Division 2 (Transparency) of Part 2 of Schedule 9 or Subdivision A of Division 3 (Record keeping and reporting) of that Part must not exceed:

5,000 penalty units if the person is a body corporate; or 1,000 penalty units if the person is not a body corporate.

Subsection 205F(5F) provides that the pecuniary penalty payable by a person in respect of a contravention of the information-gathering powers in subclauses 33(4) or 34(5) of Schedule 9 must not exceed: 40 penalty units if the person is a body corporate; or 30 penalty units if the person is not a body corporate.

Subsection 205F(5G) provides that the pecuniary penalty payable by a person in respect of a contravention of an approved misinformation code (subclause 52(1)), or a remedial direction to comply with an approved misinformation code (subclause 53(3)), of Schedule 9 must not exceed: for a body corporate – the greater of 10 000 penalty units and 2% of the annual turnover of the body corporate during the ***turnover period***; or 2000 penalty units if the person is not a body corporate. The 'turnover period' is 12 months ending at the end of the month in which the conduct constituting the contravention occurred.

Subsection 205F(5H) provides that the pecuniary penalty payable by a person in respect of a contravention of a misinformation standard (subclause 62(1)) or a remedial direction to comply with a misinformation standard (subclause 63(3)) of Schedule 9 must not exceed: for a body corporate — the greater of 25 000 penalty units and 5% of the annual turnover of the body corporate during the ***turnover period***; or 5000 penalty units if the person is not a body corporate. The 'turnover period' is 12 months ending at the end of the month in which the conduct constituting the contravention occurred.

Item 21—At the end of section 205PA

Item 21 adds to the simplified outline of Part 14C (Injunctions) of the BSA to note that the Federal Court may grant injunctions in relation to contraventions of civil penalty provisions in Schedule 9.

Item 22—Section 205Q

Section 205Q provides that the Federal Court may, on the application of the ACMA, grant an injunction restraining a person from engaging in conduct, and, if in the court's opinion it is desirable to do so, requiring a person to do something, if the person has engaged, is engaging or is proposing to engage in conduct that contravenes certain provisions of the BSA. Item 22 replaces text in section 205Q of the BSA so as to include a reference to a civil penalty provision in Schedule 9. The effect of this amendment is that the Federal Court may, on the application of the ACMA, grant injunctions in relation to contraventions of civil penalty provisions in Schedule 9.

Item 23—Section 205XA

Section 205XA empowers an authorised infringement notice officer to give formal warnings regarding contraventions of designated infringement notice provisions, with the exception of designated infringement notice provisions in Part 9E. Item 23 inserts a reference to Schedule 9 into section 205XA of the BSA to provide that section 205XA does not apply in relation to the designated infringement notice provisions in Schedule 9.

This amendment has been included because the ACMA would already have a formal warning power under clause 74 of Schedule 9 for contraventions of provisions in that Schedule.

Item 24—At the end of subsection 205Y(5)

Item 24 adds a reference to Schedule 9 into subsection 205Y(5) of the BSA.

Section 205Y of the BSA sets out when an infringement notice may be issued. Generally, an infringement notice cannot be issued unless a formal warning has previously been given under section 205XA (per subsection 205Y(4)). This is subject to the exception in subsection 205Y(5) that the requirement for a warning does not apply in relation to a contravention of a designated infringement notice provision in Part 9E of the BSA.

Since section 205XA does not apply in relation to a designated infringement notice provision in Schedule 9 (per item 23), item 24 necessarily adds an additional exception to subsection 205Y(5) to provide that no warning is required under section 205XA before issuing an infringement notice relating to a contravention of a designated infringement notice provision in Schedule 9.

Item 25—After paragraph 205ZA(1)(aa)

Subsection 205ZA(1) of the BSA sets out the amount of a penalty to be specified in an infringement notice given to a person under the provisions listed in each paragraph of that subsection.

Item 25 inserts new paragraphs 205ZA(1)(ab), (ac) and (ad) to deal with penalty amounts to be specified in infringement notices relating to Schedule 9.

If the person is a body corporate and the infringement notice relates to the information-gathering powers in subclauses 33(4) or 34(5) of Schedule 9, the penalty to be specified in the infringement notice is 8 penalty units (paragraph 205ZA(1)(ab)).

If the person is not a body corporate and the infringement notice relates to subclauses 33(4) or 34(5) of Schedule 9, the penalty to be specified in the infringement notice is 6 penalty units (paragraph 205ZA(1)(ac)).

If the person is a body corporate and the infringement notice relates to a provision of Schedule 9 other than subclause 33(4) or 34(5), the penalty to be specified in the infringement notice is 60 penalty units (paragraph 205ZA(1)(ad)).

If the person is not a body corporate and the infringement notice relates to a provision of Schedule 9 other than subclause 33(4) or 34(5), then existing paragraph 205ZA(1)(b) of the BSA would apply, and the infringement notice penalty would be 10 penalty units.

Item 26—Paragraph 205ZA(1)(a)

The amendment in item 26 is required due to the amendment in item 25. Paragraph 205ZA(1)(a) sets out the penalty to be specified in an infringement notice given to a commercial television broadcasting licensee or a subscription television broadcasting licensee, except where the penalty is provided for in one of the preceding paragraphs in

subsection 205ZA(1). Item 26 has the effect that paragraph 205ZA(1)(a) will not apply to infringement notices relating to Schedule 9, given that item 25 inserts separate paragraphs to deal with infringement notices relating to that Schedule.

Item 27—Section 216E (heading)

Section 216E of the BSA gives effect to Schedule 8 to the BSA, which confers powers on the ACMA to make rules about gambling promotional content provided on an online content service in conjunction with live coverage of a sporting event. Item 27 adds the words 'gambling promotional content' to the heading of section 216E. This amendment is required due to the amendment made to the heading of Schedule 8 by item 28 of Schedule 2 to the Bill.

Item 28—Schedule 8 (heading)

Item 28 adds the words 'gambling promotional content' to the heading of Schedule 8 to the BSA, to clarify that the focus of Schedule 8 is to regulate gambling promotional content provided on an online content service. This helps to distinguish the subject matter of Schedule 8 from the subject matter of Schedule 9, which deals with misinformation and disinformation on digital communications platforms.

Item 29—After clause 30 of Schedule 8

Item 29 inserts new clause 31 in Schedule 8 to the BSA. Clause 31 clarifies that Schedule 8 does not limit the operation of Schedule 9 to the BSA.

Online Safety Act 2021

Items 30 and 31 amend the Online Safety Act.

Item 30—Section 231 (heading)

Item 30 inserts a reference to Schedule 9 in the heading to section 231 of the Online Safety Act. This amendment is required due to the amendment in item 31.

Item 31—Section 231

Item 31 inserts a reference to Schedule 9 in section 231 of the Online Safety Act, to clarify that the Online Safety Act does not limit the operation of Schedule 9 to the BSA.

Telecommunications Act 1997

Items 32 and 33 amend the Telecommunications Act.

Item 32—Section 116 (heading)

Item 32 makes changes to the heading to section 116 of the Telecommunications Act. This amendment is required due to the amendment made by item 33.

Item 33—At the end of section 116

Section 116 of the Telecommunications Act provides that, for the purposes of Part 6 (industry codes and industry standards) of that Act, an industry code or standard that deals with a matter relating to a content service has no effect to the extent to which the matter is dealt with by a code registered, or standard determined, under Part 9 of the BSA.

Item 33 amends section 116 of the Telecommunications Act to ensure that, for the purposes of Part 6 of that Act, industry codes and standards also have no effect to the extent to which they deal with a matter that is dealt with by a code approved or standard determined under Schedule 9 to the BSA.

Item 34—Transitional provisions

Subitem 34(1) provides that subclauses 13(1) and (2) of Schedule 9 to the BSA (which are about the meanings of 'misinformation' and 'disinformation') apply in relation to any content disseminated using a digital service, whether disseminated before or after the commencement of item 34.

Subitem 34(2) provides for the purposes of subclauses 33(1) and 34(1) of Schedule 9 to the BSA (that is, powers for the ACMA to obtain information and documents relevant to misinformation or disinformation from digital communications platform providers and other persons), it does not matter whether the information or document came into existence before or after the commencement of item 34.

Subitem 34(3) provides that clause 69 of Schedule 9 to the BSA (that is, the requirement for the ACMA to prepare an annual report on the operation of Part 2 of Schedule 9) applies in relation to any financial year starting at or after the commencement of item 34. That is, the ACMA is required to report on the operation of Part 2 of Schedule 9 after each financial year, beginning with the first full financial year that starts at or after the commencement of item 34.

Item 34 commences on the day after the Bill receives the Royal Assent (see item 3 of the table in subclause 2(1) of the Bill).

PART 2—CONTINGENT AMENDMENTS

Broadcasting Services Act 1992

Item 35—Subsection 204(4A)

Item 35 replaces the reference to the Administrative Appeals Tribunal in subsection 204(4A) of the BSA (which is inserted by item 15) with a reference to the Administrative Review Tribunal. This amendment is required to deal with the commencement of the *Administrative Review Tribunal Act 2024*, and the amendment does not commence until after that Act has commenced (see item 4 of the table in subclause 2(1) of the Bill).