Attorney-General

Reference: MS24-001239

Senator Dean Smith
Chair
Senate Standing Committee for the Scrutiny of Bills
Parliament House
CANBERRA ACT 2600

By email: scrutiny.sen@aph.gov.au

Dear Chair

I refer to the Senate Standing Committee for the Scrutiny of Bills (the Committee) consideration of the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024 (the Bill) and subsequent comments made in the Committee's *Scrutiny Digest 12 of 2024* published on 18 September 2024.

I appreciate the time the Committee has taken to consider the Bill, and thank the Committee for the opportunity to address the matters raised. My response to the questions and requests made by the Committee is enclosed. As noted in the response, an addendum to the explanatory memorandum to the Bill in response to the Committee's comments will be tabled in the Parliament as soon as practicable.

I trust this information is of assistance.

Yours sincerely

THE HON MARK DREYFUS KC MP
30 / 9 /2024

Encl. *Response to the Committee's questions on the Bill*

Attorney-General

Senate Standing Committee for the Scrutiny of Bills
Ministerial Response to Scrutiny Digest 12 of 2024
Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024

Significant matters in delegated legislation

Schedule 5 to the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024 (the Bill), seeks to replace the list of specified Commonwealth, State or Territory agencies, authorities, bodies and organisations authorised to disclose AUSTRAC information to foreign governments and agencies under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act) with a power for the Commonwealth, State or Territory agency to be prescribed by the Anti-Money Laundering and Counter-Terrorism Financing Rules (the AML/CTF Rules).

In *Scrutiny Digest 12 of 2024*, the Senate Standing Committee for the Scrutiny of Bills (the Committee) requested the Attorney-General's advice as to why it is considered necessary and appropriate to leave the designation of Commonwealth, State and Territory entities who can disclose AUSTRAC information to foreign governments to delegated legislation.

Attorney-General's response

Following the machinery of government changes in 2022, responsibility for administering the AML/CTF Act transferred from the Minister for Home Affairs to the Attorney-General. An issue arose whereby the Attorney-General's Department is currently inadvertently listed twice in subsection 127(3) of the AML/CTF Act as both 'the Department' in paragraph (a) and the Attorney-General's Department in paragraph (b). This change also meant that the Department of Home Affairs, which would have previously been covered by 'the Department' at paragraph (a), was no longer covered by subsection 127(3) at all.

The proposed amendments are intended to enable a greater degree of flexibility and efficiency to account for potential machinery of government changes or changes to agency names in the future. The ability to share information related to financial crime quickly to international partners is vital to allow law enforcement and other agencies to address money laundering, terrorism financing and other serious crimes efficiently. Appropriate safeguards around the sharing of such information are contained in subsection 127(2) of the AML/CTF Act. This includes requiring that the head of an agency to be satisfied the information will be appropriately protected and used only for the purpose for which it was disclosed. Moving the list of agency names in the AML/CTF Rules would allow administrative issues to be adjusted without delay, and will ensure provisions do not easily become outdated which would require legislative amendments to correct. This allows for more efficient use of Parliamentary resources.

The AML/CTF Rules are legislative instruments within the meaning of section 8 of the *Legislation Act 2003*. Accordingly, AML/CTF Rules must be tabled in Parliament, and are subject to appropriate Parliamentary oversight, scrutiny and disallowance by either House. Further, the proposed amendments limit the power to disclose AUSTRAC information internationally to Commonwealth, State or Territory agencies.

The proposed amendments would move the list of agencies into the AML/CTF Rules when they are remade, building on the existing power of the AUSTRAC Chief Executive Officer CEO under paragraph 127(3)(o) of the AML/CTF Act to prescribe any other agency, authority, body or organisation of the Commonwealth in the AML/CTF Rules. While this currently allows for new agencies to be prescribed in the AML/CTF Rules, it does not provide the AUSTRAC CEO with the power to correct the names of existing agencies in the AML/CTF Act.

Abrogation of privilege against self-incrimination

Schedule 9 to the Bill would amend section 169 of the AML/CTF Act in relation to information or documents relevant to the operation of the AML/CTF Act, regulations or AML/CTF Rules provided to an authorised officer. Section 169 currently provides that the information or document is not admissible in evidence against the person in most civil or criminal proceedings, other than proceedings under the AML/CTF Act, or the *Proceeds of Crime Act 2002* or *Criminal Code* (Cth) that relate to the AML/CTF Act. This is known as a 'use immunity'. The Bill would expand the proceedings where no use immunity applies to include proceedings for an offence against a provision covered by the definitions of money laundering, the financing of terrorism, and proliferation financing in section 5 of the AML/CTF Act.

In addition, proposed section 172K provides that it is not a reasonable excuse for an individual to refuse or fail to answer a question, produce a document or sign a record in accordance with a requirement made under the provisions in Schedule 9 on the ground that doing so might incriminate them or expose them to a penalty. Derivative use immunity is not provided. This means that self-incriminatory material may still be used to obtain other evidence that would be admissible against the person.

In *Scrutiny Digest 12 of 2024*, the Committee requested the Attorney-General's advice as to:

- why it is necessary and appropriate to expand the abrogation of the privilege against self-incrimination in relation to all offences against a provision covered by the definitions of money laundering, the financing of terrorism, and proliferation financing
- why is it necessary and appropriate not to provide for any use or derivative use immunity in this context, and
- why no derivative use immunity has been provided in proposed section 172K.

Attorney-General's response

Abrogation of the privilege against self-incrimination
The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide) states that the privilege against self-incrimination can be overridden by legislation, however there must be clear policy justification for doing so. The Committee has previously recognised that the privilege can be overridden where there is a public benefit in the removal of the principle that outweighs the loss.

The proposed expansion of the abrogation of the privilege against self-incrimination in section 169 is necessary to ensure information provided to an authorised officer in response to a notice issued under section 167 of the AML/CTF Act can also be used in criminal proceedings for an offence relevant to the definitions of money laundering, financing of terrorism and proliferation financing in section 5 of the AML/CTF Act. This would allow for information or documents to be used in proceedings relating to offences against state or territory laws that relate to money laundering, financing of terrorism or proliferation financing where information collected by AUSTRAC is relevant to the prosecution of those offences.

This expansion is necessary to ensure the effective investigation and prosecution of serious criminal offences that relate to money laundering, financing of terrorism, and proliferation financing. The expansion balances the additional public benefit that would be provided by ensuring AUSTRAC can be more effective as Australia's AML/CTF regulator in monitoring and ensuring compliance with the AML/CTF regime.

Use or derivative use immunities

The Guide states that when removing the privilege against self-incrimination it is usual to provide some degree of protection by including a 'use' immunity or a 'use and derivative use' immunity provision. The Committee has reported positively on legislation that provides a 'use' immunity and not also a 'derivative use' immunity in limited circumstances only – generally where the offences for which the evidence would be used are very serious and where providing a 'derivative use' immunity would significantly undermine investigatory functions of the relevant legislation.

More circumscribed immunities have also been accepted for legislation governing Australian regulators, including the Australian Securities and Investments Commission (ASIC), the Australian Competition and Consumer Commission and the Australian Prudential Regulation Authority, who regulate the activities of bodies corporate but exercise information gathering powers against natural persons. Generally, the information-gathering powers conferred on these agencies remove the privilege against self-incrimination, make no provision for derivative use immunity and only provide for use immunity in some circumstances.

Similarly, to those limited immunities, the inclusion of a 'use' immunity or 'use and derivative use' immunity provision in section 169 would unacceptably fetter the investigation of AML/CTF offences and enforcement of the AML/CTF regime.

The proposed amendments to section 169 enhance AUSTRAC's ability to fulfil its statutory role as Australia's AML/CTF regulator and financial intelligence unit. In particular, the amendments allow AUSTRAC to use relevant information to sanction breaches of criminal offences relating to money laundering, financing of terrorism or proliferation financing outside of the AML/CTF regime.

The current scope of section 169 creates constraints on the prosecution of serious offences in state and territory legislation. For example, where AUSTRAC uncovers pertinent material relating to criminal conduct through the ordinary exercise of its section 167 notice power, that evidence cannot be adduced in later proceedings to prosecute money laundering or financing of terrorism offences outside of the AML/CTF Act and Criminal Code. For example, evidence related to unregistered remittance services can also be evidence of money laundering offences, but without the benefit of the proposed reforms, this evidence would be unable to be adduced for prosecutorial purposes.

Given the significant threat posed to the Australian community by money laundering and terrorism financing, the proposed amendments fulfil a legitimate objective of the AML/CTF Act and regime by closing an operational gap.

As noted by the Committee, proposed section 172K provides that it is not a reasonable excuse for an individual to refuse or fail to answer a question, produce a document or sign a record in accordance with a requirement made under the provisions in Schedule 9 on the ground that doing so might incriminate them or expose them to a penalty. Subsection 172K(3) provides a 'use' immunity for a person who, before answering a question or producing a document, claims that it might tend to incriminate them, or make them liable to a penalty.

This type of immunity prevents self-incriminating information from being used directly as evidence against the person who provided it. The use immunity applies to criminal proceedings and proceedings for the imposition of a penalty, other than proceedings relating to giving false evidence.

The Guide indicates that where a law excludes the privilege against self-incrimination as in section 172K, it is 'usual to include a use immunity or a derivative use immunity provision'. The inclusion of a derivative use immunity provision is not appropriate in this circumstance as it would unreasonably fetter the investigation and potential prosecution of serious money laundering, terrorism financing, or proliferation financing offences. It would also significantly undermine AUSTRAC's ability to monitor and enforce compliance with Australia's AML/CTF regime.

Reversal of the evidential burden of proof
Significant matters in delegated legislation

Schedule 5 to the Bill inserts a new offence of 'tipping off' into the AML/CTF Act where disclosure of specified information would, or reasonably could, prejudice an investigation of a Commonwealth offence, or one being undertaken under the Proceeds of Crime Act 2002 or equivalent state or territory laws. There are two exceptions to the offence included in the Bill, which reverse the evidential burden of proof.

In *Scrutiny Digest 12 of 2024*, the Committee requested an addendum to the explanatory memorandum for the Bill containing a justification for the reverse burden of proof provisions in Schedule 5 of the Bill to be tabled in Parliament.

Attorney-General's response

Subsection 123(4) creates an exception to the tipping off offence at section 123 of the AML/CTF Act, which allows legal practitioners, qualified accountants or a person specified in the AML/CTF Rules to disclose suspicious matter report (SMR) related information where it relates to the affairs of a customer of the reporting entity. The disclosure must be made in good faith and for the purposes of dissuading the customer from engaging in conduct that constitutes, or could constitute, an offence against a law of the Commonwealth or of a State or Territory.

Subsection 123(5) creates an exception to the tipping off offence at section 123 of the AML/CTF Act, which provides that the tipping off offence does not apply to the disclosure of information where the disclosure is in line with the regulations, the information is shared between reporting entities and is made for the purpose of detecting, deterring, or disrupting money laundering, the financing of terrorism, proliferation financing, or other serious crimes.

The notes under subsections 123(4) and (5) provide that the accused bears the evidential burden of proof in order to rely on these exceptions. It is an evidential burden as the accused may lead evidence to adduce or point to evidence that suggests a reasonable possibility that the matter exists or does not exist. If the evidence is put in issue, the legal burden of proof remains with the prosecution. Providing that the defendant bears the evidential burden of proof is consistent with 4.3.2 of the Guide which provides that "words of exception, exemption, excuse, qualification or justification will place an evidential burden of proof on the defendant".

The reversal of the burden of proof is appropriate, as evidence regarding the accused's intention of disclosing the information in good faith and for the purposes of dissuading the prohibited conduct, or for the purposes of detecting, deterring, or disrupting money laundering, the financing of terrorism, proliferation financing, or other serious crimes is particularly within the defendant's knowledge, and would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter. It follows then that evidence to this effect could be readily and more easily provided by the accused.

An addendum to the explanatory memorandum containing this justification will be tabled in the Parliament as soon as practicable.

Strict liability offences

Schedule 9 of the Bill provides that persons required to appear for examination in accordance with a notice may be required to take an oath or give an affirmation that the statements made will be true. The Bill provides that non-compliance with this requirement is an offence of strict liability which carries a sentence of up to three months' imprisonment. A strict liability offence removes the requirement for the prosecution to prove the defendant's fault.

In *Scrutiny Digest 12 of 2024*, the Committee requested a detailed justification from the Attorney-General for the proposed strict liability offence in section 172C of the Bill with reference to the principles set out in the Guide, and in particular why it is considered necessary and appropriate to impose a period of imprisonment in relation to a strict liability offence.

Attorney-General's response

The Government considers that criminal liability should generally only be imposed on individuals where they are aware of the consequences of their actions, and that they may be liable to penalty as a result of these actions. As a result, offences of strict liability should only be imposed where it is necessary to do so.

The Bill would insert a new subsection 172C(3) which imposes a strict liability offence where a person refuses or fails to comply with subsection 172C(1). Subsection 172C(1) provides that if a person is required to appear for examination as required by a notice under subsection 172A(2), the examiner may require the person to take an oath or make an affirmation. The imposition of strict liability to this offence removes the fault element, so that the prosecution will not have to prove that the defendant intended to breach the law in question.

As noted in the explanatory memorandum to the Bill, information that would be obtained through an examination will be critical to AUSTRAC's ability to monitor compliance with the AML/CTF regime, by enabling AUSTRAC to effectively collect information that will assist in detecting, deterring and disrupting money laundering, the financing of terrorism, and other serious offences.

The Attorney-General's Department referred to the Guide in considering whether the inclusion of strict liability for this offence is appropriate. The Guide provides that generally where all elements of an offence are subject to strict or absolute liability, then the offence should meet the following criteria:

- The offence is not punishable by imprisonment and the offence is punishable by a fine of up to 60 penalty units for an individual or 300 for a body corporate, in the case of strict liability.
- The punishment of offences not involving fault is likely to significantly enhance the effectiveness of the enforcement regime in deterring certain conduct.

- There are legitimate grounds for penalising the persons lacking fault – for example, because they will be notified so that they may guard against the possibility of contravention.

While the offence is punishable by a maximum of three months in prison, this is appropriately balanced against the importance of the relevant provisions to AUSTRAC's ability to enforce the AML/CTF regime. Requiring AUSTRAC in its prosecution to respond where a person raises a defence to a fault element in relation to subsection 172C(3) would impose an unnecessary burden on the regulator in conducting its enforcement investigations under the regime, and may also impose an unnecessary burden on the relevant courts by protracting proceedings. While the strict liability offence does impose a potential prison term, the maximum possible sentence of three months is appropriately brief.

Subsection 4B(2) of the *Crimes Act 1914* provides a formula for converting a term of imprisonment to penalty units. Using this formula, 12 months imprisonment equals to 60 penalty units and 3 months imprisonment equals to 15 penalty units. The penalty of 3 months imprisonment (15 penalty units), therefore, sits comfortably below the 60 penalty units threshold for a strict liability offence.

The strict liability offence is straightforward and limited in its application to situations in which a person refuses or fails to comply with the requirement to take an oath or make an affirmation in circumstances where they have appeared for examination in accordance with notices given under section 172A(2). Due to the limited circumstances in which this situation is likely to arise, it is appropriate that strict liability be imposed in these circumstances. The application of strict liability also recognises the significant resources for AUSTRAC involved in arranging for a person or persons to appear for examination, and it imposes an appropriately balanced penalty for refusing to take an oath or affirmation in such circumstances, regardless of the intent of the person.

In relation to the second point included in the Guide, as noted above, the ability for AUSTRAC to efficiently gather and assess evidence is essential to AUSTRAC's role as the AML/CTF regulator, and its ability to investigate and enforce breaches of Australia's AML/CTF regime.

Regarding the third point, the offence in question would only occur where there are legitimate grounds for penalising the person without establishing fault, and that in such circumstances they will be so notified as to the outcome of any contravention, whether they are at fault or not. As noted above, contraventions of this offence will occur in a controlled environment, including electronic recording of the proceedings, where AUSTRAC or other officials will be able to explain to the persons in question the consequences of any breach of the strict liability offence at section 172C(3). Persons breaching this offence will do so with the knowledge that such an offence may result in a prison sentence. As a result, it is appropriate to confer strict liability under these conditions.

Further, subsection 172C(3) is consistent with similar strict liability offences punishable by imprisonment in the legislation outlining the examination functions and powers of other regulators such as ASIC. Sections 21(1) and (1A) of the *Australian Securities and Investments Commission Act 2001* provides that the failure of an examinee to either take an oath or make an affirmation is an offence of strict liability and section 63(3) imposes a penalty of 3 months imprisonment.

The Hon Jason Clare MP
Minister for Education

Reference: MC24-009012

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

By email: scrutiny.sen@aph.gov.au

Dear Chair

Thank you for your correspondence of 19 September 2024 regarding the Senate Standing Committee for the Scrutiny of Bills' (the Committee) request for information on matters identified in *Scrutiny Digest 12 of 2024* in relation to the Wage Justice for Early Childhood Education and Care Workers (Special Account) Bill 2024 (the Bill).

Use of non-legislative guidance

The Committee has requested my advice on why it is necessary and appropriate for the eligibility criteria for decisions to grant remuneration made under clause 10 of the Bill to be left to non-legislative guidance.

The Bill establishes a special account to fund grants that support a remuneration increase for workers in the early childhood education and care (ECEC) sector.

Consistent with the fact that these grants will be administered in accordance with the Commonwealth grants policy framework as established through the Commonwealth Grants Rules and Guidelines 2017 (and the Commonwealth Grants Rules and Principles 2024 from 1 October 2024), the eligibility criteria to support the making of the grants will be set out in Grant Opportunity Guidelines (Guidelines), which will be made available shortly. The Guidelines will outline both the categories of ECEC workers that are intended to benefit from the remuneration increase and who will be able to apply for a grant.

It is common practice for grant eligibility criteria to be left to non-legislative guidance when establishing a special account to fund grants. See for example Part 3, Division 2 of the *Housing Australia Future Fund Act 2023.*

In this case, it is appropriate that the eligibility criteria for grants are not contained within legislation, as this provides the necessary flexibility to adjust eligibility if required. For example, should eligibility criteria need to be amended to extend support to other parts of the ECEC sector, following consultation with relevant stakeholders, the Guidelines could be promptly amended.

Grants to support remuneration increases to ECEC workers will initially be made under section 85GA of the *A New Tax System (Family Assistance) Act 1999*. That Act does not provide guidance as to the eligibility criteria for grants made under section 85GA. For consistency, it is appropriate for the Bill to adopt a similar approach.

Eligibility criteria

The Committee has also sought my advice as to the eligibility criteria for decisions made under clause 10 of the Bill.

Grants will be made available to cover eligible ECEC workers who:

- work at an eligible Child Care Subsidy (CCS) approved Centre-Based Day Care (CBDC) or Outside School Hours Care (OSHC) service that opts in to the payment, and
- are covered by either the *Children's Services Award 2010*, the *Educational Services (Teachers) Award 2020* or a state-based ECEC award, or
- undertake the duties included in the *Children's Services Award 2010* and the *Educational Services (Teachers) Award 2020*.

To be eligible to apply for a grant, you must:

- be a legal entity that provides CBDC or OSHC services (a Provider). One Provider may apply in relation to one or multiple service locations (Services).

The Provider must be:

- an incorporated or unincorporated body or association, or
- a private or public company, or
- a registered co-operative, or
- a state/territory government body, or
- a local council, or
- an Indigenous corporation, or
- a sole trader, or
- a partnership.

The Provider must for each Service on the application:

- have a valid Australian Business Number
- meet and maintain all eligibility requirements of continued CCS approval for the duration of the grant
- employ eligible ECEC workers under a legally enforceable workplace instrument that meets specified conditions, including an obligation to pay workers either at or above the relevant minimum rates set out in the grant Guidelines
- not increase their Service fees by more than 4.4% in the 12 months from 8 August 2024 to 7 August 2025 and for each subsequent 12 month period, by more than the amount equivalent to the growth rate as specified in the new Australian Bureau of Statistics input cost index which will be developed specifically for the ECEC sector or such other fee growth percentage caps as determined by the Department of Education.

Whether the Bill can be amended

Finally, the Committee has sought my advice as to whether the Bill can be amended to include additional guidance on the exercise of the power on the face of the primary legislation.

For the reasons given above, specifically the need to ensure flexibility to allow for adjustments to eligibility requirements and consistency with the making of grants under section 85G of the *A New Tax System (Family Assistance) Act 1999*, I do not consider it is necessary to include additional guidance on the exercise of the power on the face of the primary legislation.

I trust this information is of assistance.

Yours sincerely

JASON CLARE

3 / 10 / 2024

Attorney-General

Reference: MC24-050796

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

By email: scrutiny.sen@aph.gov.au

Dear Chair

Thank you for your correspondence of 19 September 2024 regarding the Criminal Code Amendment (Hate Crimes) Bill 2024 (the Bill).

I appreciate the time the Committee has taken to review the Bill. Please find enclosed my response to the Committee's questions in *Scrutiny Digest 12 of 2024*.

I trust this information is of assistance.

Yours sincerely

THE HON MARK DREYFUS KC MP
8 /10 /2024

Encl: *Response to Senate Standing Committee on the Scrutiny of Bills Scrutiny Digest 12 of 2024*

Response to Senate Standing Committee on the Scrutiny of Bills
Scrutiny Digest 12 of 2024

The Senate Standing Committee on the Scrutiny of Bills (the Committee) has requested the Attorney-General's further advice in relation to a number of matters in the Criminal Code Amendment (Hate Crimes) Bill 2024 (the Bill). These matters are set out in the Scrutiny Digest 12 of 2024. The following information is provided in response to the Committee's request for further advice on the Bill.

Broad scope of offence provisions—Freedom of expression

1.40 The committee considers further information is required to fully assess the appropriateness of removing existing defences, the effect of which may mean the overly broad criminalisation of certain speech. The committee therefore seeks the Attorney-General's advice as to:

- **why is it necessary to seek to remove the application of the good faith defences in section 80.3 to these offences (noting the explanatory materials provide that no relevant speech could ever be made in good faith);**
- **why it is proposed to remove the defences in section 80.3 entirely without implementing the other part of the ALRC recommendation to reframe the criminal offences so that the court, in determining whether a person intends the urged force or violence will occur, must have regard to the context in which the circumstance occurred;**
- **what conduct would 'use of force' include and would it include use of force against property; and**
- **what type of groups or members of a group would be captured by the attribute of 'political opinion', and why the inclusion of this attribute is appropriate in the context of freedom of expression.**

Removal of the good faith defence and consideration of the context in which relevant conduct occurred

The offences have been carefully crafted to target the most serious forms of hate speech, namely the urging or threatening of force or violence against individuals, groups and the broader Australian community. Urging and threatening force or violence undermines community respect and understanding, and erodes Australia's shared values. There are no circumstances where urging or threatening force or violence is appropriate. The removal of the good faith defence in section 80.3 reflects the Government's view that threatening and urging violence are not part of good faith discourse.

The context in which relevant conduct occurred will be considered by the courts in determining whether an offence has been committed. The urging violence offences require it to be proven that the person intended to urge force or violence. In the absence of direct evidence in the form of an admission by the accused, the requisite intent would need to be proved as a matter of inference from the facts and surrounding circumstances.[1] This would require consideration of the context of the conduct.

---

[1] See eg *Kural v R* (1987) 162 CLR 502, 504 (Mason CJ, Deane and Dawson JJ), applied by the Court in *Smith v R; R v Afford* (2017) 259 CLR 291.

As amended, the urging violence offence would also require it to be proven that the person was reckless as to whether that force or violence will occur. Section 5.4 of the *Criminal Code Act 1995* provides that a person is reckless with respect to a result if they are aware of a substantial risk that the result will occur and, having regard to the circumstances known to them, it is unjustifiable to take the risk. As such, establishing whether a person is reckless as to whether their conduct will result in force or violence will necessarily require consideration of the context in which that conduct occurred.

Meaning of 'use of force'

The term 'force or violence' is not defined in the *Criminal Code Act 1995*. It is intended to take its ordinary meaning. The Macquarie Dictionary definition of 'force' includes strength or power exerted upon an object and physical coercion. 'Violence' includes rough force in action, rough or injurious action or treatment, and any unjust or unwarranted exertion of force or power.

Notably, the offences in the Bill apply where a person urges or threatens force or violence *against a group or a member of a group*.[2] This is intended to require that the violence or force is against persons who are a part of the group. It is not intended to apply to threatening or urging damage to property, except where that damage to property would also involve violence or force against a person.

Inclusion of 'political opinion' as a protected attribute

The term 'political opinion' is not defined and is intended to take its ordinary meaning. The Macquarie Dictionary definition of 'political' includes things that relate to the governing of a nation, state, municipality etc; exercising or seeking power in government or public affairs; and a political party or its principles, aims, activities. The definition of 'opinion' includes a judgement or belief resting on grounds insufficient to produce certainty; a personal view, attitude or estimation; and the expression of a personal view, estimation or judgement. Having regard to those definitions, 'political opinion' could include beliefs, judgements, attitudes and views that relate to government, governance, and political parties.

By including 'political opinion' as a protected attribute, the offences in the Bill would promote the right to hold opinions without interference.[3] The urging and threatening violence offences would assist individuals and groups to express their political opinions without fear of force or violence. The offences are also consistent with rights to freedom from discrimination on the basis of political opinion contained in the International Covenant on Civil and Political Rights (ICCPR)[4] and the Universal Declaration of Human Rights.[5]

The amended urging violence offences and new threatening violence offences would limit the right to freedom of expression as provided for in the ICCPR[6] in that they would limit the public communication of information and ideas, where the communication amounts to urging or threatening force or violence against a targeted group or its members, the person is

---

[2] Sections 80.2A(1)(a), 80.2A(2)(a), 80.2B(1)(a), 80.2B(2)(a), 80.2BA(1)(a), 80.2BA(2)(a), 80.2BB(1)(a), 80.2BB(2)(a) in the Criminal Code Act 1995, and Criminal Code Amendment (Hate Crimes) Bill 2024

[3] See Article 19(1) of the International Covenant on Civil and Political Rights (ICCPR).

[4] See Article 26 of the ICCPR.

[5] See Article 2 of the Universal Declaration of Human Rights.

[6] See Article 19(2) of the ICCPR.

reckless as to whether or not the communication would result in force or violence occurring, and the targeted group is distinguished by a listed protected attribute or the person believes the targeted person is a member of a group distinguished by a listed protected attribute, including political opinion.

The right to freedom of expression under international law is not absolute and may be subject to limitation for specified purposes, including respect for the rights or reputations of others; and for the protection of national security or public order where such limitation is provided by law and is reasonable, necessary and proportionate to a legitimate objective.[7] The limitations which the amended offences place on this right are provided for by law and are necessary and proportionate to promote respect of the rights of others and the protection of public order.[8]

The limitation is necessary to respect the rights of others to hold opinions without interference, by assisting other Australians to freely express their political views without fear of force or violence. The limitation is also necessary to protect the Australian community from conduct that causes significant harm to its members in the form of force or violence and to prevent the compromise of national security and public order, as conduct of this sort can increase the likelihood that force or violence will be perpetrated.

The limitation is proportionate as the offences in the Bill target only the most serious forms of harmful hate speech against groups distinguished by political opinion, namely urging or threatening force or violence. Australians can, and do, hold strong political views, and the ability to express these is an important aspect of our democracy. Views could continue to be expressed so long as they do not urge or threaten force or violence against a targeted group or its members.

---

[7] See Article 19(3) of the ICCPR.

[8] See Article 19(3) of the ICCPR.

The Hon Anika Wells MP
Minister for Aged Care
Minister for Sport
Member for Lilley

Ref No: MC24-015669

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Parliament House
CANBERRA ACT 2600
Scrutiny.Sen@aph.gov.au

Dear Chair

Thank you for your correspondence of 10 October 2024 on behalf of the Senate Scrutiny of Bills Committee (Committee), regarding the Aged Care Bill 2024 (Bill).

I thank the Committee for its consideration of the Bill in Scrutiny Digest 13 of 2024. I welcome the opportunity to respond to the Committee's questions.

Please find enclosed my response to questions raised.

I thank the Committee for raising these issues, and trust that my response will be of assistance.

Yours sincerely

Anika Wells

24 October 2024

Encl (1)

cc: The Hon Mark Butler MP, Minister for Health and Aged Care

Aged Care Bill 2024
Responses to queries from Senate Scrutiny of Bills Committee
October 2024

Question	Response

Undue trespass on rights and liberties
Significant matters in delegated legislation
Broad discretionary powers
Immunity from civil and criminal liability
 	
1.18 Noting the potential for the use of restrictive practices to impact on personal rights and liberties, the committee requests the minister's advice as to:
 	
• **why it is considered necessary and appropriate to leave the details of when restrictive practices can be used in an aged care setting to delegated legislation;**
 	
• **whether the bill could be amended to include additional high-level guidance about when restrictive practices can be used on the face of the primary legislation; and**
 	
• **whether the bill could be amended to include:**
 	
  • **at least a broad definition of 'emergency'; and**
 	
  • **limits around which considerations set out in clause 18 can be overridden in an emergency.**
	The Aged Care Bill 2024 (Bill), as is the case with the current *Aged Care Act 1997* (current Act), includes significant safeguards in relation to the use of restrictive practices. Clause 18 provides details of requirements that must be included in the rules in regard to the use of restrictive practices. This provision specifies that the rules must require restrictive practices to only be used:
	• as a last resort and after consideration of the likely impact of the use on the individual;
	• only to the extent that is necessary for the shortest time; and
	• in the least restrictive form, to prevent harm to the individual or others.
	
	The rules must also:
	• require alternative strategies be used before a restrictive practice is used;
	• require informed consent be given to the use of a restrictive practice; and
	• make provision for monitoring and review of the use of a restrictive practice.
	
	As is currently the case, the rules will also require that the use of a restrictive practice complies with a care recipient's behaviour support plan. The behaviour support plan captures any assessment of the care recipient that is relevant to understanding the care recipient's behaviour, as well as information about behaviours of concern for which the care recipient may need support. This reduces the incidence of emergencies.
	
	It is necessary and appropriate that these matters continue to be dealt with in delegated legislation as they will deal with operational details, which intersect with state and territory legislative frameworks. Including these matters in delegated legislation will provide flexibility for prompt modifications if the arrangements have any unintended consequences that may impact the health, safety and wellbeing of individuals receiving aged care services.

	Subclause 18(3) provides that the delegated legislation may provide that a requirement specified in the rules does not apply if the use of a restrictive practice in relation to an individual receiving aged care services is necessary in an emergency. This replicates the provision in the current Act. The rules regarding the emergency use of restrictive practices will reflect the current requirements in the *Quality of Care Principles 2014.* These requirements include that the emergency use of restrictive practice only applies while the emergency persists. Situations where restrictive practices are required in residential aged care in the event of an emergency should be rare and limited to serious or dangerous situations that are unanticipated or unforeseen and require immediate action. Further, as is currently the case, the rules will specify that as soon as practicable following the use of restrictive practices in an emergency: • if the recipient lacked capacity to consent, the provider must also inform their restrictive practices substitute decision maker about the use of the restrictive practice; • the provider documents the certain matters about the use of the restrictive practice in the behaviour support plan, including: reasons for the restrictive practice; the alternative strategies that were considered or used before the use of the restrictive practice; the reasons the use of the restrictive practice was necessary; and the care to be provided to the care recipient in relation to the care recipient's behaviour; • the provider ensures that any assessment(s) undertaken prior to the use of the restrictive practice is properly documented in the behaviour support plan. Within this context, by utilising the ordinary meaning of an 'emergency', providers can take appropriate urgent action where there is an immediate risk or harm to a care recipient or other person, and only during that period. The above safeguards ensure there is transparency in the use of the emergency provision for the use of a restrictive practice.

Undue trespass on rights and liberties **No invalidity clause** **1.28 The committee seeks the minister's advice as to:** **• whether a complaint could be made to the Complaints Commissioner for a breach of all aspects of the Statement of Rights (or would it be required to be linked to a violation of the Code of Conduct or Aged Care Quality Standards), and if not, why it is not appropriate to amend the bill to allow for this;** **• how subclauses 26(1) and (3) interact, and whether clause 26 of the bill can be amended to require consideration of the Statement of Principles when making a decision as a condition of validity.**	The functions of the Complaints Commissioner under the Bill include to uphold the rights under the Statement of Rights by maintaining processes for making complaints about a registered provider acting in a way that is incompatible with the Statement of Rights (subparagraph 358(a)(ii)). This is further supported by clause 361, which provides that the rules made in relation to the Complaints Commissioner dealing with complaints or feedback may make provision in relation to how complaints can be made about a registered provider acting in a way that is incompatible with the Statement of Rights (subparagraph 361(2)(a)(ii)). These rules will allow for complaints to be made to the Complaints Commissioner consistent with all subparagraphs under paragraph 358(a), including subparagraph 358(a)(ii). This will allow complainants to raise any behaviour by a provider which is incompatible with the Statement of Rights with the Complaints Commissioner, regardless of whether it can be directly linked to a violation of the Code of Conduct, the Aged Care Quality Standards, or another provision of the Bill. Subclause 26(3) does not negate those bodies bound by the Statement of Principles in subclause 26(1) from having to have regard to the Principles when performing functions and exercising powers, but rather reflects the broad scope and guiding nature of the statement. Including a 'no invalidity' clause in the Bill will not exclude judicial review under paragraph 75(v) of the Constitution and section 39B of the *Judiciary Act 1903* where a failure to meet procedural requirements would amount to a jurisdictional error. It would not inoculate a decision against broader failures such as fraud, bribery, dishonesty or other forms of conscious maladministration. I appreciate the Committee's raising this issue, but I do not consider that an amendment to this provision is appropriate. Anyone performing functions or exercising powers under the Bill must have regard to the Principles. However, there may be issues outside of the control of those persons that require them to make a decision that is not wholly in line with each and every Principle, but is in line with the Bill or other legislation.

Tabling of documents in Parliament **1.47 Noting the impact on parliamentary scrutiny, the committee requests the minister's advice as to why the bill does not provide for reports produced under clauses 342, 373 and 374 to be tabled in the Parliament.**	Clauses 373 and 374 are drafted in line with section 58 of the *Aged Care Quality and Safety Commission Act 2018* and, similar to that section, are intended to be used to obtain reports from the Commissioner or Complaints Commissioner concerning specific matters of concern relevant to the functions of the Commissioner or Complaints Commissioner. As these reports may contain sensitive information concerning relevant persons, it is not considered that it would be appropriate for the reports to be tabled in the Parliament. Similarly, clause 342 relates to coroner's reports, which may contain sensitive information concerning deceased persons and their family members, it is not considered that it would be appropriate for the reports to be tabled in the Parliament. I note that under subclause 341(2), the published register includes matters covered in clause 342 subject to the exclusions outlined in subclauses 341(4) and 341(5).
Coercive powers **1.56 In light of the above, the committee requests the minister's advice as to:** **• why it is necessary and appropriate that clauses 436 and 437 allow for an authorised person, or a person assisting an authorised person, to move things to determine if they may be seized, and then seize a thing or data contained in the thing without a warrant;** **• why it is necessary and appropriate for clauses 436 and 437 to confer powers that are beyond what is already provided for by Part 3 of the Regulatory Powers (Standard Provisions) Act 2014;** **• whether section 66 of the Regulatory Powers (Standard Provisions) Act 2014 is taken to apply to these provisions;** **• why there currently is no statutory limit on the number of times an extension may be applied for in order to retain a thing that has been moved to another location to be examined; and**	The additional powers are necessary and appropriate to ensure that electronic equipment may be examined thoroughly for evidential material, whether on site or elsewhere in certain circumstances, and by an expert user where required to ensure integrity of evidence is maintained and data is not damaged or corrupted. The Committee's concerns are noted and I will consider amending provisions to constrain the operation of these additional powers to only where an investigation warrant has been issued. This approach aligns to that within the *National Disability Insurance Scheme Act 2013* and supports harmonisation of the regulatory approach adopted by regulators across the care sector. If the operation of the powers are confined in this way, the *Regulatory Powers (Standard Provisions) Act 2014* will apply to the exercise of these powers as it does to all the other powers related to investigation and seizure of evidential material under warrant, including the obligations to return seized items and limits on extensions to hold such items.

• why the bill does not contain a requirement that a thing that has been moved or seized must be returned after a certain period or once it is no longer required for evidential purposes.	
Procedural fairness **Privacy** **Significant matters in delegated legislation** **1.68 In light of the above, the committee requests the minister's advice as to:** • **why it is necessary and appropriate to allow a final banning order to be made against a person in emergency circumstances, noting that this will result in a banning order being made against the individual without providing a chance to make submissions, and whether the bill could be amended to instead provide for the making of an interim banning order and allow submissions to be made before a final banning order is made;** • **how the register of banning orders will be published, including who will have access to this register, and, if it will be published in full on a public website, why this is necessary and appropriate;** • **why it is necessary and appropriate that information relating to banning orders that have ceased remain published;** • **why it is necessary and appropriate to include matters in relation to information that can be included on these registers and in relation to the administration and operation of the registers in delegated legislation; and** • **whether the bill can be amended to provide further guidance as to the types of matters the rules may make provision for in relation to the registers.**	The provisions within the Bill seek to maintain the existing framework for the Commissioner to making banning orders and to establish and maintain a register of those banning orders. The framework within the Bill is aligned not only to that currently in operation within the aged care system but also aligns to the banning order framework within the *National Disability Insurance Scheme Act 2013* to ensure harmonisation across the care sector. It is anticipated that the register of banning orders will continue to be published on the Aged Care Quality and Safety Commission's website subject to similar requirements being established under the rules to those under the existing Aged Care Quality and Safety Commission Rules 2018, which provide that the Commissioner must not publish a part of the register of banning orders if publication is contrary to public interest or the interests of one or more care recipients (section 23CG(3)). The publication of the banning orders register enables providers of aged care services to meet their workforce obligations by ensuring that a person who is subject to a banning order is not engaged in the delivery of funded aged care services. Significantly, the register's publication facilitates harmonisation across the care sector by enabling providers and recipients of services under the NDIS to ensure that a person banned from being involved in the delivery of aged care services cannot simply move to another arm of the care services sector and continue to engage in behaviours or conduct which has warranted regulatory action of this nature.

Immunity from civil liability **1.74 The committee requests the minister's advice as to what recourse is available for affected individuals, other than demonstrating a lack of good faith, for actions taken by authorised persons, persons assisting authorised persons and the System Governor.**	Clause 533 is intended to protect authorised officers, and persons acting under their direction or authority, against personal civil liability where they are performing or exercising legislated requirements in good faith. This would ensure that they are free to perform their functions without concern that their personal interests would be at risk. These immunities relate to individuals, but not the Commonwealth, and therefore an affected person could seek a remedy from the Commonwealth despite being unable to seek a remedy from a protected individual who has acted in good faith. Further, the conferral of immunity from civil liability when performing functions and powers in good faith prevents civil proceedings being used to undermine or put at risk legitimate actions undertaken by protected persons. Remedies would also be available to an affected person under the Scheme for Compensation for Detriment caused by Defective Administration (known as the CDDA Scheme) where appropriate. Nothing in the Bill would prevent the pursuit of a remedy under this scheme. Similarly, clauses 536 and 541 are intended to protect persons from civil liability (and 536 clarifies that a person is not subject to any criminal liability under any other Commonwealth Act) where making a disclosure in accordance with Division 2 of Part 2 in Chapter 7. The immunity is necessary to enable an individual to perform their function or undertake an action authorised by the legislation, appropriately and without concern that their personal interests would be at risk. The scope of the immunity is limited to the act of the disclosure itself, with any actions disclosed by the person and their liability for those actions remaining unaffected by the immunity as outlined in clauses 536 and 541.
Privacy **1.91 Noting the impact on privacy of broad authorisations for the use or disclosure of personal information, the committee requests the minister's advice as to:**	The authorisations set out in clauses 538 and 539 have been drafted in line with a framework that is consistent across the Commonwealth, and with consideration of the recent review of secrecy provisions undertaken by the Attorney-General's Department. The authorisation in subclause 538(1) provides for disclosures of relevant information to the Minister for the performance of the Minister's functions.

• **why each of the broad exceptions from privacy protections in clauses 538 and 539 are necessary and appropriate, in particular subclauses 538(1) and (4) and 539(4), (7), (10) and (11);** • **whether the bill could be amended to require a person who is disclosing information for the same purpose for which it was disclosed to them (under subclause 538(9)) to de-identify the information where appropriate;** • **whether the bill can be amended to require information disclosed for research purposes to be either de-identified or only shared with consent; and** • **examples or guidance as to what would constitute a public interest reason for the System Governor to disclose information.**	However, subclause 538(2) provides that where the performance of functions can be achieved by the disclosure of information that has been de-identified, disclosure of identified information would not be authorised. This provides an additional privacy protection measure, and otherwise the disclosure is considered necessary and appropriate for government functionality. In relation to the particular concerns raised about the Minister responding publicly to adverse claims in the media where it is necessary to provide personal information about the individual who has made the adverse claims to the Minister, this would not be a broader use or disclosure of personal information than that which is permitted under the *Privacy Act 1988* (see paragraph 6.22 of the Office of the Australian Information Commissioner (OAIC)'s Australian Privacy Principle (APP) Guidelines). Subclause 538(4) similarly allows for effective administration of the aged care system, whereby relevant information is permitted to be disclosed by entrusted persons (noting that is a limited cohort) to enable the delivery of funded aged care services or other community, health or social services to the individual, the assessment of an individuals' needs, or assessment of the level of care needs as against other individuals. This last element is important, particularly where individuals may not have necessarily consented to their information being used for a purpose that relates to aged care services provided to others, to ensure there is no delay in the provision of those services and prioritisation of services in line with Chapter 2 of the Bill. In addition, the intention of this clause is to authorise disclosures made to relevant bodies to facilitate providing important services to an individual where there is a need for this. For example, this is intended to facilitate disclosure to state and territory bodies that provide services in relation to potential family violence or elder abuse concerns, where consent to such disclosures is not always practicable. Clause 539 sets out situations where a disclosure of relevant information by the System Governor and an Appointed Commissioner may be authorised. These authorisations provide a basis for sharing information in a manner that is lawful as well as reasonable, necessary and proportionate to achieve a legitimate objective.

	Subclause 539(4) lists out the relevant Commonwealth bodies to whom information can be disclosed to facilitate the performance or functions of the body, including, for example, the Inspector-General of Aged Care. The intent of this provision is to ensure consistency of information and data across Government, so that information does not become siloed, frustrating the functions of the listed Commonwealth agencies. A key theme from the Aged Care Quality and Safety Royal Commission was the interoperability of information and communications systems to enable the sharing of data and information about people receiving care between aged care and health care providers and relevant government agencies. In addition to the amendments made to information management provisions of the current Act by the *Aged Care and Other Legislation Amendment (Royal Commission Response) Act 2022* (Cth), subclause 539(4) is in line with this theme, and in particular facilitates greater information sharing between Commonwealth bodies that have functions and powers relating to aged care, veterans' care, social security and disability support, as well as bodies that have oversight and safeguarding functions (such as the Commonwealth Ombudsman). Subclause 539(7) provides that relevant information may be disclosed for the purposes of research into funded aged care services if conducted on behalf of the Commonwealth. The disclosure of personal information for this purpose is only considered necessary if the research cannot be conducted if the information were to be de-identified. To amend the provision as proposed would significantly alter the intended operation of this provision and result in no authorisation being available to allow relevant research that requires information about identified or reasonably identifiable individuals. We note some important research projects may involve linkage with other data sets where it is not possible to remove all risk of re-identification. Further, obtaining informed consent at the time of collecting the information is not practicable, as it would not be known at that time what future research may be proposed. To obtain consent at the time of each new research proposal would also not be practicable as it could limit the value of the research where consent was not obtained, or responses not provided. Research into funded aged care services is of significant import to enable a sustainable aged care system.

	Subclauses 539(10) and 539(11) provide that relevant information may be used or disclosed by the System Governor or an Appointed Commissioner where they have certified its use or disclosure for the purpose specified is in the public interest. Examples of what may constitute a public interest reason for the System Governor to disclose information (and therefore provide justification for the inclusion of such a clause) include: • health and safety concerns: disclosures that directly address potential risks to the health and safety of individuals accessing aged care, such as cases of neglect or abuse, can be justified in the public interest (where the requirements of subclause 537(8) are not met). • emergency management: emergencies such as disease outbreaks, disclosing information can facilitate rapid response measures to protect vulnerable populations (where the requirements of subclause 537(8) are not met). • transparency and accountability: disclosing information for the purposes of enhancing public trust and accountability in the aged care system, particularly in relation to government oversight. Assuming the Committee is referencing subclause 537(9), I will consider an amendment to require a person who is disclosing information for the same purpose for which it was disclosed to them (under subclause 537(9)) to de-identify the information where appropriate.
Broad delegation of administrative powers and functions **1.95 The committee requests the minister's advice as to why it is considered necessary and appropriate to allow for the delegation of any or all of the Commissioner's powers and functions under clause 575, and whether the bill can be amended to provide some legislative guidance as to the scope of powers that might be delegated, or the categories of people to whom those powers might be delegated.**	Clause 575 provides for the delegation of functions by the Aged Care Quality and Safety Commissioner to the ministerially appointed Complaints Commissioner. The scope of functions and powers which may be delegated to the Complaints Commissioner is broad due to the potential overlap of skills and experience of Commission staff in exercising complaints functions and other Commissioner functions, for example reportable incidents under clause 349. This is intended to allow for the effective administration and allocation of Commission resources. Noting the concerns of the Committee, I will consider an amendment to subclause 572(2) as suggested to limit the categories of people to whom those powers might be delegated, in line with other subdelegation provisions.

	The Complaints Commissioner may otherwise delegate their functions or powers under the Bill, other than Parts 2 to 9 of Chapter 6 (regulatory mechanisms), to a member of staff of the Commission in accordance with Division 3, Part 3 of Chapter 8.
Automated decision-making **1.103 The committee requests the minister's advice as to:** • **why each of the decisions included within the definition of 'relevant administrative decisions' are considered appropriate for automation and whether any are discretionary in nature; and** • **whether the Attorney-General's Department was consulted to ensure a consistent legal framework regarding automated decision-making (as per recommendations 17.1 and 17.2 of the Royal Commission into the Robodebt Scheme).**	The Department referred the provisions at clauses 582 and 583 to the Attorney-General's Department to ensure a consistent legal framework regarding automated decision-making (as per recommendations 17.1 and 17.2 of the Royal Commission into the Robodebt Scheme). The Attorney-General's Department supported these provisions as they are consistent with the precedent provision on the use of automated decision-making. None of the administrative actions listed at clause 582 are discretionary in nature. Decisions made under subclause 78(1) (which deals with classification levels) and subclause 86(1) (which deals with priority category decisions) may use a computer program, after the assessment is undertaken by an approved assessor. The input is recorded and run through the computer program. There is no discretion in the decision once it is input to the computer program. Decisions made under subclause 92(1) (which deals with allocation of places to individuals) and subclause 93(1) (which deals with deciding the order of allocation of places to individuals) may use a computer program. Clause 91 would be a discretionary decision until rules for the purposes of 93(2) providing for a method or procedure of allocating places are made. The Attorney's General Department confirmed there were no concerns if this decision were not be automated until rules are made. The rules for subclause 93(2) would effectively remove the System Governor's discretion, which renders clause 93 a mandatory decision based on objectively ascertainable matters.

	Giving a notice under subclauses 79(1), 88(1) or 92(3) and doing, or refusing or failing to do, anything related to making a decision under subclauses 78(1), 86(1), 92(1) or 93(1) are appropriately limited to mandatory decisions based on objectively ascertainable matters.
Standing appropriation **1.107 The committee therefore requests the minister's advice as to what mechanisms are in place to report to the Parliament on any expenditure authorised by the standing appropriation.**	The appropriation provisions in the Aged Care Bill 2024 (Bill) mirror the appropriation provisions in the *Aged Care Act 1997,* for which is the Bill is intended as a replacement. It is not intended for the Bill to change the current mechanisms in place to report to the Parliament on any expenditure authorised by the standing appropriation. Clause 599 of the Bill requires the System Governor to give the Minister, for presentation to each House of the Parliament, a report on the performance of the System Governor's functions during each financial year. This report must include: a) the extent of unmet demand for funded aged care services; b) the duration of waiting periods for funded aged care services; c) the number of registered providers entering and exiting the market for the delivery of funded aged care services; d) the financial viability of registered providers in that market; e) usage of the bond guarantee scheme; f) the amounts of contributions paid; g) the amounts of those contributions paid as refundable deposits; h) the extent of building, upgrading and refurbishment of residential care homes.

The Hon Michelle Rowland MP

Minister for Communications
Federal Member for Greenway

MC24-017812

Senator Dean Smith
Chair
Senate Standing Committee for the Scrutiny of Bills
Suite 1.111
Parliament House
Canberra ACT 2600

scrutiny.sen@aph.gov.au

Dear Senator Smith

Thank you for your email of 10 October 2024 regarding the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024.

As requested by the Committee, please find enclosed my responses to the Committee's request for information as set out in its Scrutiny Digest 13 of 2024.

Thank you for taking the time to write to me on this matter. I trust that the attached information is of assistance.

Yours sincerely

Michelle Rowland MP

24 /10 /2024

Encl. Response to the Committee's questions in relation to the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024

Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024
Responses to queries from the Senate Standing Committee for the Scrutiny of Bills
October 2024

Question	Response
1.115 The committee therefore seeks the minister's advice as to:	
• **why it is considered necessary and appropriate to leave to the rules all detail regarding risk management, media literacy plans and complaints;** • **whether further detail could be included on the face of the primary legislation, noting the importance of parliamentary scrutiny;** • **why there is no requirement to make digital platform rules regarding complaints and dispute handling processes for misinformation complaints;**	# Risk Management ## Key points The Bill provides the appropriate balance between matters relating to risk assessments specified in the Bill and matters which may be dealt with by legislative instrument. • The Bill will impose a requirement on digital communications platform providers to publish a *risk assessment*, that is an assessment of the risks of misinformation and disinformation on the platform, which must include risks arising from both the design or functioning of the platform and the use of the platform by end-users. • The obligation to publish a *risk assessment* will arise directly under cl.17. However, the Bill provides that digital platform rules may specify matters which must be included in the risk assessment and specify when risk assessments must be updated. • In addition, the digital platform rules may require a provider to have a management plan for risks relating to misinformation and disinformation on digital communications platforms (*risk management plan*) and specify when such a plan must be prepared. The rules may also require those risk management plans to state the steps (if any) being taken by providers in relation to specified risks. • The matters which may be provided for in rules are not appropriate to be specified in the primary legislation: o the need for such rules can be better identified as the Australian Communications and Media Authority (ACMA) obtains further information through the digital platform providers' reporting and publication obligations and the ACMA's information gathering powers (arising under Schedule 9 directly or through digital platform rules);

Question	Response
	○ the need for such rules may also depend on the timing and nature of external events that would be impossible to predict (e.g. a future natural disaster, violent attacks, coordinated bot or troll farm actions or emergency events that might trigger a wave of misinformation and disinformation); ○ platforms differ significantly in the nature of their user-interfaces, their users, and the content which is shared—this means that the risks and the measures to address these through rules may also differ significantly and factors that underpin rules may change quite rapidly with changes in technology, and new service offerings; and ○ to ensure there is no undue regulatory burden on low-risk platforms, it might be appropriate to make rules for only some classes of providers where the risks are greater. Relevant provisions The Bill proposes a requirement for a digital communications platform provider to publish a *report…on the outcomes of an assessment by the provider of risks relating to misinformation and disinformation on its platform* (cl.17(1)(a)). This risk assessment must include: • risks arising from the design or functioning of the platform (cl.17(1)(a)(i)); and • risks arising from the use of the platform by end-users (cl.17(1)(a)(ii)). The report must meet *the requirements (if any) prescribed by the digital platform rules* (cl.17(1)(a)). The digital platform rules may provide for the *risk assessments to cover specified matters* (cl.19(b)).

Question	Response
	The EM (p.76) highlights the limited scope of this rule-making power related to risk assessments: *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.* It can be seen that the obligation to publish a risk assessment arises directly under cl.17(1)(a). The digital platform rules contemplated under cl.19 may specify matters which must be included in the assessment and specify when risk assessments must be updated. A risk assessment will need to consider the characteristics of the relevant digital communications platform. Platforms differ significantly in the nature of their user-interfaces, their users, and the content which is shared. Moreover, all of these factors can change quite rapidly with changes in technology, and new service offerings. The nature and features of digital communications platforms are constantly and rapidly evolving, including through new generative artificial intelligence technology. In addition to the *risk assessment* required by cl.17(1)(a) (including as supplemented by matters specified in a digital platform rule (if any) made under that subclause), the digital platform rules made under cl.19 may require providers to *have management plans for risks relating to misinformation and disinformation on digital communications platforms* (cl.19(c)). The Bill also provides for rules to be made specifying when risk management plans must be prepared (cl.19(d)).

Question	Response
	The rules may also require those risk management plans to *state the steps (if any) being taken by digital communications platform providers in relation to risks identified by providers or specified in the rules* (cl.19(e)). The EM (p.76) further elaborates that the *risk management plan* is intended to comprise: *…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 EM (pp 76-77) confirms that the power to make rules with respect to risk management plans does not extend to the power to require the provider to take particular action in relation to the management of particular risks: *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.* The EM (p.76) states that the ACMA could target the application of such rules to certain digital communications platform providers only (see *Acts Interpretation Act 1901* s33(3A)) where, for example, certain sections of the digital platform industry pose a higher risk due to the nature of their services or their features, and/or having regard to the numbers of end-users of such services.

Question	Response
	As noted above, platforms differ significantly in the nature of their user-interfaces, their users, and the content which is shared—and none of these aspects remain static. The flexibility to impose specific requirements for risk management plans by means of legislative instrument is necessary to be able to impose such requirements where needed to address significant risks (consistent with the objective of avoiding unnecessary regulation) and to impose, vary or remove requirements promptly to address current needs in a rapidly evolving industry. Flexibility through rules is also required in response to external events, the timing of which cannot be predicted. ## Media Literacy ### Key points The Bill provides the appropriate balance between matters relating to media literacy plans specified in the Bill and matters which may be dealt with by legislative instrument: • The Bill will impose a requirement to publish a *current media literacy plan*. • The Bill contains a definition of *media literacy plan*, which requires it to set out measures the provider will take to enable end-users to better identify misinformation and disinformation on the platform. • The EM gives examples of the kinds of measures that might be included in a plan, but notes that appropriate measures will differ between platforms. • The Bill does not confer power to make digital platform rules that require a specific measure be included in a media literacy plan—rather, the rules may require that the plan identify measures (*media literacy tools*) that are being used by the provider and also to provide an assessment of their effectiveness. The rules may also impose requirements to update a media literacy plan.

Question	Response
	• The matters which may be provided for in rules are not appropriate to be specified in the primary legislation as: ▪ the need for such rules can be better identified as the ACMA obtains further information by means of the platforms' reporting and publication obligations and the ACMA's information gathering powers provided for in the Bill; ▪ platforms differ significantly in the nature of their user-interfaces, their users, and the content which is shared—this means that the risks and the measures to address these may also differ significantly and factors that may underpin rules may change quite rapidly with changes in technology, and new service offerings; and ▪ to ensure there is no undue regulatory burden on low-risk platforms, it might be appropriate to make rules for only for some classes of providers where the risks are greater. Relevant provisions The Bill proposes a requirement for a digital communications platform provider to publish its *current media literacy plan* (cl.17(1)(c)). The Bill (cl.2) defines a 'media literacy plan' to mean: *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).*

Question	Response
	The EM (p.69) gives examples of the kinds of measures that could be included in a media literacy plan: *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.* However, each media literacy plan will need to be tailored to some extent for that particular digital communications platform. Platforms differ significantly in the nature of their user-interfaces, their users, and the content which is shared (see EM pp 69, 78-79). Moreover, all of these factors can change quite rapidly with changes in technology, and new service offerings. The Bill provides for the obligations to publish a media literacy plan to be augmented by digital platform rules, made by legislative instrument by the ACMA. These are limited to the following matters (cl.22): • requirements to update media literacy plans • requirements for plans to identify the media literacy tools being used in relation to risks of misinformation and disinformation (see also cl.19(e))

Question	Response
	• requirements to provide assessments of the effectiveness of media literacy tools mentioned in their media literacy plan. The EM (p.78) gives examples of media literacy tools: *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.* As for the rule-making power in relation to risk management, the purpose of these rule-making powers is **not** to empower the ACMA to require the digital communications platform provider to take particular action in relation to specified risks—in this case by requiring use of a specified media literacy tool—but simply to require the provider to specify what action it is taking in that regard. The EM (pp 78-79) notes it is likely to be the case that not all digital communications platform providers will be subject to the same rules: *For example,* [the ACMA] *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 need for such rules will be informed by the information that the ACMA is able to obtain pursuant to various measures in the Bill once enacted (see cl.17 (digital communications

Question	Response
	platform provider must publish information) and Subdivision B of Division 3 of Part 2 (Information gathering)), having regard to the current risks of misinformation and disinformation on particular kinds of platform. ## Complaints and dispute handling processes ### Key points To include, at this time, baseline requirements for complaints and dispute processes in the Bill itself risks overregulation and inflexibility in dealing with the evolving digital communications platform industry. Any further regulation should: • be informed by the information that the ACMA is able to obtain once the Bill is enacted • allow for differing measures taking into account differences in user-interfaces, typical characteristics of end-users, and in the content shared • retain flexibility to make changes to respond to how the system is operating in practice and to the evolving risk landscape • be informed by the ongoing process to define a voluntary internal dispute resolution code, on which the Government is currently working with the digital platforms industry to develop following on from recommendations in the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry Final Report* and *Digital Platform Services Inquiry Interim Report No. 5*. The power to make rules requiring digital communications platform providers to implement and maintain complaints and dispute handling processes needs to be viewed in the context of the publication requirements contained in the Bill itself—in particular, the requirements on providers to publish their policies or policy approach in relation to misinformation and disinformation on

Question	Response
	the platform. In other words, these publication requirements may inform whether particular digital communication platform providers have existing complaints and dispute mechanisms, and the nature of these mechanisms. This in turn will inform the nature of rules that could potentially be made, and the classes of providers who they could apply to, for example. Relevant provisions There is no express requirement in the Bill for a digital communications platform provider to publish the particulars of its complaints and dispute handling processes. However, where a provider has such processes, that is likely to engage the requirement for the provider to publish its *policy*, or *policy approach*, in relation to misinformation and disinformation on the platform (cl.17(1)(b)). The information published is envisaged to inform the ACMA regarding the need to make any digital platform rules relating to complaints and dispute handling. This is explained in greater detail in the EM (p.68 emphasis added): *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*

Question	Response
	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****.* The relevant rule-making power relates to complaints and dispute handling processes for *misinformation complaints* (cl.25(1)). The Bill defines (cl.2) a *misinformation complaint* as a complaint in relation to either: • misinformation or disinformation (or dissemination that is potentially 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.

Question	Response

	The Bill expressly authorises the making of rules to require providers to do the following in relation to *misinformation complaints*:
	• implement and maintain complaints and dispute handling processes (cl.25(2)(a));
	• ensure complaints and dispute handling processes comply with minimum standards (cl.25(2)(b));
	• publish, or provide to the ACMA, information regarding:
	  ○ complaints and dispute handling processes; and
	  ○ misinformation complaints; and
	  ○ responses to misinformation complaints (cl.25(2)(c)).
	
	While it might be possible to develop a set of baseline requirements for complaints and dispute handling under the Bill itself, this is fraught with risks of overregulation and inflexibility on the digital communications platform industry, particularly prior to the ACMA gaining a more thorough understanding of the sector through its information gathering powers.
	
	Various passages from the EM explain the need that any further regulation must:
	• be informed by the information that the ACMA is able to obtain pursuant to various measures in the Bill once enacted (see s.17 (digital communications platform provider must publish information) and Subdivision B of Division 3 of Part 2 (Information gathering)
	• address appropriate measures to different classes of providers taking into account the significant differences in platforms with respect to the nature of their user-interfaces, their users, and the content which is shared
	• retain the flexibility to consider how the system is operating in practice and to respond to the evolving risk landscape.

Question	Response
	Moreover, the rules provide flexibility for the requirements in relation to complaints and dispute handling to be informed by the voluntary internal dispute resolution code that the Government is currently working with digital platforms industry to develop in response to successive digital platform inquiry report recommendations from the Australian Competition and Consumer Commission (ACCC).
• **whether the bill could provide that all ACMA's decisions made under the rules are subject to merits review, unless ACMA specifically excludes merits review in individual cases.**	## Decisions subject to merits review ### Key points It is not appropriate for the Bill to provide that 'all decisions' made by the ACMA under the rules are subject to merits review, unless specifically excluded by the rules: • the measure providing for decisions subject to review is in the same form as used elsewhere in the Bill. • it can be expected that the ACMA will specify in the rules the administrative decisions where merits review will lie, acting in accordance with the general polices and guidelines as to the kinds of decisions which should be subject to merits review. • the rules will be subject to parliamentary scrutiny and disallowance. • if the rules do not reflect those policies, the failure to do so will need to be explained to the Senate Standing Committee for the Scrutiny of Delegated Legislation. Failure to provide an adequate explanation could lead to disallowance of the rules. • it is not always clear whether a particular administrative action taken under a legislative scheme will be held to be a 'decision' for the purposes of the relevant legislation. • it is impractical to require the rules to specify every action that might conceivably be held to be a 'decision' unless specifically excluded.

Question	Response
	• there is a real risk that a provision of this kind could be gamed by a well-resourced, litigious, digital communications platform provider to frustrate the finalisation of an administrative decision-making process. Relevant Provisions The Bill provides for merits review of administrative decisions provided for by the rules where these are specified in the digital platform rules (see proposed s.204(4A) of the *Broadcasting Services Act 1992* (BSA) to be inserted by item 15 of Schedule 2 of the Bill). This measure is in the same form as existing measures in the BSA which confer merits review rights for decisions made under other specified legislative instruments (BSA ss 204(3), 204(4)). The same is done for administrative decisions provided for in the Bill itself: specific provisions subject to merits review are specified under Schedule 2, Item 14 as additions to s.204(1) of the BSA. Digital platform rules must be made by legislative instrument, subject to scrutiny and potential disallowance by both Houses of Parliament in accordance with the *Legislation Act 2003* (see further EM at p.131). It can be expected that the ACMA would provide for merits review where a substantive decision would affect the interests of a person and does not fall within the recognised classes of administrative decisions unsuitable for merits review[1]. Should the ACMA fail to do so, the Senate Standing Committee for the Scrutiny of Delegated Legislation will identify this and require an explanation.

[1] For example, see Administrative Review Council 1999 *What decisions should be subject to merit review?* at What decisions should be subject to merit review? 1999 | Attorney-General's Department (ag.gov.au) (accessed 14 October 2024).

Question	Response
	To provide in the Bill that **all** *decisions* taken by the ACMA are subject to merits review—unless specifically excluded— in practice would require the rules to identify each administrative action of a procedural or preliminary character, or that is otherwise not suitable for merits review, that might arguably be characterised as a 'decision'. The history of litigation on the question of when administrative action constitutes a reviewable 'decision' under the *Administrative Decisions (Judicial Review) Act 1977*[2] demonstrates that there is much scope for difference of views on these issues. The objectives of the legislation are likely to be frustrated if a platform is able to interrupt a decision-making process by making applications for merits review of various actions taken by the ACMA on the basis that each such action constitutes a 'decision'. Such applications might not ultimately be granted, but nevertheless might lead to significant delay until the application is determined by a Tribunal member. In this regard it is relevant to note that the decisions which the ACMA might be empowered to make under digital platform rules will operate to impose obligations upon digital communications platform providers. In practice, those providers impacted by potential rules will be extremely large corporations, with ample resources to use litigation to delay administrative processes where it is in their interests to do so.[3]

[2] For example, see Aronsen, Groves & Weeks (2022) *Judicial Review of Administrative Action and Government Liability* (7th ed) paras [2.280]-[2.450]
[3] For example, see *Australian Broadcasting Tribunal v Bond* [1990] HCA 33 at [2]-[35]

Question	Response
1.123 The committee seeks the minister's advice as to:	
• **why it is considered necessary and appropriate to leave to the rules all details regarding record keeping relating to misinformation or disinformation**	## Record Keeping Rules ### Key Points These rule-making powers are expected to be used to make different provisions for different classes of digital communications platform provider, taking into account: • the differing characteristics of platform providers, their user-interfaces, their users and the content shared; • the consequent differences in misinformation risks and the measures appropriate to address these risks; and • the contemporary environment noting factors can change quite rapidly with changes in technology, and new service offerings. As such, it is impracticable to develop appropriately-targeted baseline requirements for record keeping rules to be included in the current Bill. ### Relevant Provisions The power to make digital platform rules about the keeping of records by digital communications platform providers is modelled on the powers of the ACMA to make record keeping rules for carriers and carriage service providers under *Telecommunications Act 1997* s.529 (see EM p.85). It is clear from the terms of s.529 that it was intended that different record keeping obligations might apply to a particular carrier or service provider or class of carrier or service provider.

Question	Response
	Similar scope to make different arrangements for different providers is intended for cl.30. The EM (p.85) draws attention to the general operation of the *Acts Interpretation Act 1901* s.33(3A) (and see also s.33(3AC)) and notes the following: *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.* Accordingly, the absence of any 'baseline' record keeping obligations in the Bill serves a number of objectives of better regulatory practice: • it removes the risk of 'regulatory overreach' due to an initial imposition of a set of uniform record keeping obligations; • it enables regulation to be better tailored to areas of greater risk of harms, having regard to the particular features of different kinds of platform; and • it enables regulation to respond more rapidly to emerging risks and to withdraw regulatory requirements where these no longer achieve any significant objective.
• **why privacy protections specified in the explanatory memorandum are not included in the bill itself, such as in relation to de-identification and that records should only be retained for as long as is reasonably necessary; and**	## Specific Privacy Measures ### Key Points • The EM refers to these as examples of potential privacy protections that the ACMA, in making rules about record keeping by providers, might consider in identifying whether those rules will be a necessary and reasonable means to achieve the regulatory objectives of the Bill.

Question	Response
	• Having regard to the differences between platforms and the particular risks of misinformation or disinformation, it is clear that the examples mentioned will not be feasible in every case. • Accordingly, it would not be possible for the Bill to provide that the rules must include requirements for de-identification and time limits on record retention. Relevant Provisions This issue relates to the question of what further restrictions or requirements might be added to the provisions requiring the ACMA to consider certain things before making a *digital platform rule* requiring digital platform providers to make and retain records relating to misinformation and disinformation, and/or measures they have taken to respond to these (cl.30). • The *digital platform rules* will be *legislative instruments* (cl.82), subject to tabling and parliamentary scrutiny and disallowance provisions of the *Legislation Act 2003*. • Before making such a rule, the ACMA is required to consider the privacy of relevant end-users (cl.30(2)(a)) and whether the rule is required for the performance of a relevant ACMA function (cl.30(2)(b)). • The ACMA may not make rules which require a provider to make and retain records of the content of *private messages* or *VOIP communications* (cl.30(3)). The EM (p.87) relating to these provisions explains their effect and intended operation as follows: *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*

Question	Response
	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)...). In addition, the ACMA must comply with the requirements of the Privacy Act when dealing with personal information… As the EM notes, in making any such rules about records that might impact on the privacy of end-users, the ACMA is expected to consider the extent to which those records are a necessary and reasonable means to achieve the regulatory objectives contemplated under the Bill. This is likely to be a question posed as part of the delegated legislation scrutiny process when the particular rules are put before Parliament. The EM gives specific examples of measures which would limit the impact on privacy (de-identification and time limits on record retention). However, it is clear there is no expectation that such measures will be suitable in every case: the EM simply suggests that the ACMA will consider the extent to which these may be feasible. The response to the previous question noted the expectation that rules about record keeping made under cl.30 would need to be adapted to the particular circumstances of different classes of platform provider. These include their user-interfaces, their users and the content shared and the consequent differences in misinformation risks and the measures appropriate to address these risks.

Question	Response
	In these circumstances it would not be possible for the Bill to provide that the rules must include requirements for de-identification and time limits on record retention in all cases.
• **why the bill does not contain a minimum number of end-users as to what constitutes a 'private message' (noting that if the rules set a low number, important privacy protections would not apply to such messages).**	## Definition of private message ### Key points Any legislative instrument to determine a different maximum number of private recipients of a private message will need to be informed by information made available to the ACMA pursuant to the operation of other provisions in BSA Schedule 9. The reasons for that determination of a number will need to be justified by the ACMA to Parliament, having regard to its potential human rights impacts. ### Relevant Provisions The Bill (cl.2) defines *private message* as follows: ***private message*** *means a message sent using a digital communications platform from an end-user:* *(a) to another end-user; or* *(b) at the same time to a number of end-users that does not exceed:* *(i) the number specified in the digital platform rules; or* *(ii) if no number is specified in the digital platform rules— 1,000.* Note that the definition of a *private message* contained in paragraph (a) of the definition cannot be altered by digital platform rules: a message sent by an end-user to a single other end-user will always constitute a *private message*.

Question	Response
	A digital platform rule may only affect the application of the definition where a message is sent by an end-user to more than one person at the same time (paragraph (b) of the definition). The EM (p.27) notes the reason for the initial selection of the number 1,000: *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.* *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.* The EM further notes at p.27 that allowing the maximum number to be specified in the digital platform rules *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*. If the ACMA makes a legislative instrument to specify a relevant number lower than the present number, it will be need to provide a justification at that time as to why such messages need to be brought within scope of BSA Schedule 9. This is noted in the EM (p.27): *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*

Question	Response
	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.
1.142 Noting the above comments, the committee seeks the minister's advice as to:	
• **whether the definition of 'professional news content' is overly narrow in requiring that the person producing the content be bound by specific editorial standards, and how this is likely to operate in practice in relation to journalists producing content in countries that may not have analogous standards;**	## Professional news content ### Key points The Bill has aligned its definitions of journalism around the requirements of the *professional standards test* set out in section 52P of the *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021*. This contemplates journalism as a line of work subject to codes of practice or professional standards that relate to the provision of quality journalism. • There is no settled or understood meaning of who might be a 'journalist', where producing content in a country that may not have analogous rules or standards (for example, cl. 16(2)(b)(iv)). • It is inconsistent with the policy intention behind the exclusion that it might potentially operate to exclude from the scope of the legislation dissemination of content by a person who might simply call themselves a 'journalist'. • Exclusion from the operation of the Bill of *professional news content* reflects considered policy judgements about the objective misinformation and disinformation risks posed by content originating from recognised media formats where generally:

Question	Response
	▪ material is produced in circumstances which help ensure quality, arm's-length journalism; and ▪ there are established complaint resolution processes – e.g. correction notices. • There is greater potential for harm from the spread of content from self-described 'journalists' whose activities are not subject to any professional standards of conduct, oversight or accountability mechanisms. • In addition, any expanded definition of journalism risks inadvertently covering activities of foreign interference operations driven by state-based actors that masquerade as producers of legitimate journalism. Relevant provisions The operative provisions of the Bill apply in relation to *misinformation* or *disinformation*. This is relevantly defined (cl.13) as the dissemination of content using a digital service if: • the content contains information that is reasonably verifiable as false, misleading or deceptive; and • the content is provided on the digital service to one or more end-users in Australia; and • the provision of the content on the digital service is reasonably likely to cause or contribute to serious harm; and • the dissemination is not *excluded dissemination*. Where dissemination of content is *excluded dissemination*, it is effectively entirely outside the scope of the measures contained in the Bill intended to address concerns regarding the dissemination of false, misleading or deceptive information reasonably likely to cause or contribute to *serious harm* as defined in cl.14.

Question	Response
	In other words, the effect of extending the definition takes such disseminations of information outside the scope of the Bill for all purposes. This would put it beyond the scope of information and reporting on instances of misinformation or disinformation, for example, not simply measures aimed at preventing dissemination of misinformation or disinformation. The dissemination of *professional news content* is one of the categories of *excluded dissemination* (cl.16(1)(b)). The *professional news content* exclusion will apply to the *dissemination of content* by a person: • who produces, and publishes online • *news content* (cl.16(3)) in one of the formats specified in cl.16(2)(a) • where that person is *subject to* the rules of an Australian standard or code of practice analogous to those specified in subparagraphs (i), (ii) or (iii) of cl.16(2)(b). The *professional news content* exclusion can also apply to a person who produces, and publishes online, *news content* in like circumstances provided that person is *subject to* either: • *rules or internal editorial standards* that are *analogous* to the Australian rules specified 'to the extent that they relate to the provision of quality journalism' (cl.16(2)(b)(iv)); or • rules specified for these purposes in digital platform rules (cl.16(2)(b)(v)). The EM (pp 62-63) explains the rationale for the *professional news content* exclusion: *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 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.*

Question	Response
	In such circumstances, where anyone who chooses to call themselves a 'journalist'—e.g. a blogger with a smart phone—could be permitted to rely on the exclusion contemplated under cl.16, that provision would be unfeasibly broad and indeterminate, greatly reducing the efficacy of the Bill. Exclusion from the operation of the Bill of *professional news content* reflects considered policy, operational and regulatory judgements about the objective misinformation and disinformation risks posed by content originating from the sources of information listed in cl.16(2). Specifically, where content originates from a person covered by the criteria set out in cls 16(2)(b) and (c), that material is produced in circumstances which help ensure quality, arm's-length journalism where the potential for intentionally false or misleading material is low or negligible. In addition, where content originates from such a person, there are generally established complaint resolution processes that may address harms arising from the circulation of that material—for example, the issue of correction notices in relation to material found to be factually inaccurate or not prepared in accordance with fair and accepted standards of investigating or reporting. There also may be additional commercial or regulatory levers that ensure high quality journalism for bodies captured by this exemption class. Accordingly, there is greater potential for harm from the spread of content from self-described 'journalists' whose activities are not subject to any professional standards of conduct. However, it should be kept in mind that dissemination from such persons on a digital service will not come within the scope of the Bill unless it also meets the *false, misleading or deceptive* and *serious harm* requirements of the Bill. It should also be noted that permitting self-described 'journalists' to be exempted from the Bill risks inadvertently excluding the activities of foreign influence operations by state-based actors

Question	Response
	that masquerade as producers of legitimate journalism and greatly reducing the efficacy of the Bill.
• **why it is considered necessary and appropriate to leave to codes and standards all processes by which participants in a digital platform industry are to prevent or respond to misinformation or disinformation, including why there is no requirement as to what such a code or standard must contain; and**	## Codes and Standards: mandatory content requirement ### Key Points • The legislative scheme of the Bill reflects the principle that regulation should be imposed on industry only to the extent necessary to address a perceived harm that is not being adequately mitigated by industry self-regulation. • The Bill does not set out all the matters which must be in a code, as the nature of the risk and the appropriate measures will depend on the relevant industry sector and class of digital communication platform provider. • The power to enact a misinformation standard is also more comprehensively precluded by requirements such as the ACMA being satisfied that it is *necessary* to deal with that matter to provide adequate protection from *serious harm*, or codes having partially or totally failed. • Given that a code need not address all matters which potentially could be addressed—and in practice a standard is highly unlikely ever to do so—it is not possible to specify the matters that a code or standard *must* contain without reducing the flexibility with which industry or the regulator might operate. ### Relevant provisions Following the model commonly used in legislation in the Communications portfolio[4], the statutory scheme in the Bill provides for codes of practice to be developed by industry bodies,

[4] See for example *Telecommunications Act 1997* Part 6; *Broadcasting Services Act 1992* Part 9; *Online Safety Act 2021* Part 9 Division 7

Question	Response
	which may be submitted to the regulator for approval under the legislation (new Division 4 of Part 2, BSA Schedule 9). Where approved, that code has legal effect (cls 47, 52). The ACMA may also request codes in certain circumstances (cl.48). Although the use of the term 'code' might suggest otherwise, it is not intended that a code need be in force which deals with every matter which could be included in a code for the purposes of the Bill. • The Bill allows for the possibility that the ACMA may approve only a part of a code that was submitted to it (cl.47(5)). This may occur where the ACMA is dissatisfied with some provisions of a draft code, but is satisfied with the rest of the provisions (EM p.107). • Similarly, where the ACMA requests an industry body to develop a code, it must specify one or more matters relating to the operations of the relevant platforms to which the code is to apply (cl.48(1)(a). The scope of the power for the ACMA to make a standard is even more clearly circumscribed and subject to preconditions. Before it can make a standard in respect of a matter, the ACMA must be satisfied that it is *necessary… to provide adequate protection for the Australian community from serious harm caused or contributed to by misinformation or disinformation* (cls 55(1)(c), 56(1)(e), 57(1)(d), 58(1)(e), 59(1), for example. The scheme of the Bill makes it clear that: • a code need not address all matters which potentially could be addressed; and • a standard is highly unlikely ever to address all matters which potentially could be addressed.

Question	Response
	It follows that it is not possible or appropriate for the Bill to specify the matters that either a code or a standard must contain.
• **whether the bill could be amended to require the ACMA to be satisfied that a misinformation code or standard appropriately balances the importance of protecting the community from serious harm with the right to freedom of expression.**	## Codes and Standards: statutory balancing requirement ### Key Points • Where it approves a misinformation code or determines a misinformation standard, the ACMA will have a legal obligation to prepare a statement of compatibility with Australia's international human rights obligations. • In practice, this means that the ACMA will need to consider Australia's international human rights obligations, including those relating to freedom of expression, in deciding whether to approve a code or make a standard. • In the context of this legislation, any attempt to codify some aspects of that consideration, with reference a specified human right, is likely to create legal uncertainty, with real risks of legal challenges and unintended consequences. • Codes and standards are also subject to parliamentary scrutiny and disallowance. ### Relevant provisions The Bill provides for a misinformation code to be developed by a body or association that represents a particular section of the digital platform industry and submitted to the ACMA for its approval (cls 47, 50). In various circumstances specified in the Bill, the ACMA may make or vary a misinformation standard (cls 55-60). • A misinformation code approved by the ACMA is a legislative instrument (cl.47(6)). • For the purposes of the *Legislation Act 2003*, the ACMA is the rule-maker for the approved misinformation code (cl.47(7)).

Question	Response
	• Where the ACMA approves a draft variation of a code submitted by a body or association, it is required, by legislative instrument, to vary the code accordingly (cl.50(5)). • Where the ACMA makes, or varies, a misinformation standard, it does so by means of a legislative instrument (cls 55(2), 56(2), 57(3), 58(3), 59(2), 60(1)). As the Bill provides that approved codes and standards are legislative instruments (and the ACMA the rule maker), the ACMA is required to prepare a statement of compatibility for the instrument under s.9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* (*Legislation Act 2003* s15J(2)(f)). A statement of compatibility must include an assessment of whether the legislative instrument is compatible with *human rights* (*Human Rights (Parliamentary Scrutiny) Act 2011* s.9(2)). Subsection 3(1) of that Act defines *human rights* for the purposes of that Act as follows: ***human rights*** *means the rights and freedoms recognised or declared by the following international instruments:* *(a) the International Convention on the Elimination of all Forms of Racial Discrimination done at New York on 21 December 1965 ([1975] ATS 40);* *(b) the International Covenant on Economic, Social and Cultural Rights done at New York on 16 December 1966 ([1976] ATS 5);* *(c) the International Covenant on Civil and Political Rights done at New York on 16 December 1966 ([1980] ATS 23);* *(d) the Convention on the Elimination of All Forms of Discrimination Against Women done at New York on 18 December 1979 ([1983] ATS 9);* *(e) the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment done at New York on 10 December 1984 ([1989] ATS 21);*

Question	Response
	(f) the Convention on the Rights of the Child done at New York on 20 November 1989 ([1991] ATS 4); *(g) the Convention on the Rights of Persons with Disabilities done at New York on 13 December 2006 ([2008] ATS 12).* In practice the requirement to analyse the compatibility of the legislative instrument will require the ACMA to have regard to relevant matters in any decision by the ACMA to approve or make the relevant instrument. International human rights norms are multi-factorial, broad ranging and open ended. While important matters to consider when developing legislation or legislative instruments, their inherently indeterminate character makes them inappropriate for incorporation into Australian law as legal standards that limit the power of decision-makers. This principle is reflected in the legislation which seeks to ensure that questions of compliance with the obligations to prepare the human rights compatibility statement do not provide grounds for any legal challenge to the validity, operation or enforcement of the instrument (see *Human Rights (Parliamentary Scrutiny) Act 2011* s.9(4); *Legislation Act 2003* s15K(2)).