Human Rights Law Centre

SUBMISSION ON THE COMMUNICATIONS LEGISLATION AMENDMENT (COMBATTING MISINFORMATION AND DISINFORMATION) BILL 2024 (Cth).

30 September 2024 / David Mejia-Canales

Human Rights Law Centre

Human Rights Law Centre

The Human Rights Law Centre uses strategic legal action, policy solutions and advocacy to support people and communities to eliminate inequality and injustice and build a fairer, more compassionate Australia. We work in coalition with key partners, including community organisations, law firms and barristers, academics and experts, and international and domestic human rights organisations.

We acknowledge the lands on which we work and live, including the lands of the Wurundjeri, Bunurong, Gadigal, Ngunnawal, Darug and Wadawurrung people. We pay our respect to Elders of those lands, both past and present.

We recognise that Aboriginal and Torres Strait Islander people and communities were the first technologists and innovators on this continent, with deep knowledge systems that continue to shape our understanding of innovation, sustainability, land stewardship, and community care.

We recognise that this land always was and always will be Aboriginal and Torres Strait Islander land because sovereignty has never been ceded.

We acknowledge the role of the colonial legal system in establishing, entrenching, and continuing the oppression and injustice experienced by First Nations peoples and that we have a responsibility to work in solidarity with Aboriginal and Torres Strait Islander people to undo this.

We support the self-determination of Aboriginal and Torres Strait Islander peoples.

Follow us at http://twitter.com/humanrightsHRLC

Join us at www.facebook.com/HumanRightsLawCentreHRLC

Contents

1. Introduction

The Human Rights Law Centre thanks the Environment and Communications Legislation Committee (**the Committee**) for the opportunity to make a submission to the inquiry on the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 (**the Bill**).

The rise of internet technologies has greatly benefited our lives, including by amplifying diverse voices, enabling new economic opportunities, democratising access to information and education, and providing new ways us to gather and connect.

The flipside is that these technologies have also enabled the rapid spread of illegal and abhorrent material like child exploitation content, hate speech, misinformation, disinformation and other harmful content. In turn, this has contributed to an erosion of trust in our democracy,[1] and is causing real harm to people and communities.[2] Children, young people, women, Aboriginal and Torres Strait Islander people, communities of colour, and LGBTQIA+ individuals are particularly targeted by harmful content, harassment, and hate speech online.[3]

Digital platforms are the entities responsible for enabling the spread of harmful and illegal content on an unprecedented scale. Large digital platforms in particular wield immense power over public discourse, amplifying and manipulating the information that is shaping our decisions and beliefs. Worst of all, these platforms profit billions of dollars every year from fuelling the spread of harm and hate in our society.

Digital platforms have consistently failed to rectify their use of addictive design features, recommender systems, dark patterns, invasive data harvesting practices, ineffective and vague content moderation policies, and opaque mechanisms for reporting misconduct or abuse online – the list goes on.

It is clear that digital platforms will not voluntarily act to fix their systems which enable the spread of harmful content. Particularly as these platforms lack a commercial incentive to regulate misinformation and disinformation because inflammatory content drives engagement which boosts their profits. In this context, digital platforms, the entities with the greatest ability and capacity to reduce the harmful content they host, must be made to take on more responsibility for mitigating the harms that they enable.

Australia was once a pioneer of digital platform regulation – we were the first country to legislate for online safety and to appoint an Online Safety Commissioner. We led the way in legislating negotiations between digital platforms and news outlets, and insights from the Australian Competition and Consumer Commission's *Digital Platforms Inquiry Final Report* continue to shape policy development nationally and abroad, but despite these efforts continue to fall behind in the fight to protect Australians online.

In recent times, Australia has conducted numerous reviews and inquiries into creating safer online environments. These include reviews of the *Privacy Act 1998* (Cth) and the *Online Safety Act 2021* (Cth), as well as parliamentary inquiries into the influence of large online platforms, the role of social media in Australian society, and the impact of artificial intelligence.

In response, the Bill was introduced into the Australian Parliament on 12 September 2024.

This submission will consider the proposals of the Bill, ultimately providing its comments and recommendations under three headings, being that:

1. the Bill must be **better grounded in human rights law and principles**;
2. the **self-regulation** measures contemplated by the Bill **will be ineffective**; and
3. digital platforms should owe a legislated **duty of care to all users**.

---

[1] Gabriel R Sanchez, Keesha Middlemass, 'Misinformation is eroding the public's confidence in democracy', *The Brookings Institute* (Online, 26 July 2022) <https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/>.
[2] Social Media and Online Safety, 'Social Media and Online Safety', Report of the House of Representatives Select Committee on Social Media and Online Safety, (March 2022), 11 - 12.
[3] Ibid 29-44

2. Summary of recommendations

The Human Rights Law Centre recommends that the Committee adopts each of the following recommendations. We provide our rationale for these recommendations in the subsequent sections of this submission:

1. Australia needs a Human Rights Act.

2. The Bill should clarify the concepts of misinformation and disinformation.

3. Clause 70(1) should be amended to bring forward the timing of the first review of the Bill.

4. Clause 70(2) should be amended to broaden the scope of the review to include all applicable human rights.

5. The creation of digital platform rules, codes and standards should be subject to adequate Parliamentary oversight.

6. Clause 11(e) should be amended to reflect a broader commitment to human rights in the Bill's objectives.

7. Media literacy plans must be accessible to be effective.

8. The Australian Human Rights Commission should be consulted on the development of codes.

9. Reports submitted to ACMA under digital platform rules should be released to the public to enhance public trust and understanding of the Bill's functionality.

10. Platforms should be required to grant free access to operational application programming interfaces (APIs) to enhance transparency.

11. The Bill should be amended to include specific immunities for Australian researchers acquiring platform data for good faith research.

12. The Bill should establish a legislated duty of care for digital platforms.

3. The Bill must be better grounded in human rights law and principles

Everyone should be able to enjoy their human rights, including when we go online to connect with others or to access information. Indeed, human rights law requires that the rights that we enjoy offline must be equally guaranteed online.[4]

Human rights law provides a ready-made and universal framework to protect fundamental rights and freedoms through internationally recognised laws, principles, and standards. Grounding the Bill in this framework would ensure that any restrictions on human rights are lawful, strictly necessary to achieving a legitimate objective, and proportionate.

Furthermore, by aligning regulations with human rights law and principles, harmful online content can be effectively addressed —such as misinformation, disinformation, and hate speech—while also balancing the fundamental rights of all users.

As with any proposed law, there will always be some tension between certain fundamental rights. Right now, we note there is community concern that the Bill may limit the freedom of expression. Laws that seek to regulate platforms for the exchange of information must be subject to close scrutiny to ensure that they do not unduly and disproportionately limit the freedom of expression.

A human rights-based approach to regulating misinformation and disinformation online is therefore crucial, particularly as harmful online content can significantly undermine the enjoyment of a number of human rights, including:

3.1 The right to life

The right to life is contained in Article 6 of *the International Covenant on Civil and Political Rights* (***ICCPR***), to which Australia is a signatory.

The right to life is the most fundamental right from which no derogation is permitted, even in times of national emergency or armed conflict.[5] Logically, the protection of the right to life is a prerequisite for the enjoyment of all other human rights.[6]

The right to life must be broadly interpreted to ensure all people are entitled to live a life with dignity, free from acts or omissions that could lead to premature or unnatural death.[7]

As a signatory to the ICCPR, Australia has a duty to prevent foreseeable threats to life from private individuals or entities, including non-state actors. This duty also obliges Australia to address broader societal conditions that can and do pose threats to life.[8]

Recently, online misinformation and disinformation led to an innocent person being falsely accused of being the perpetrator of a mass stabbing in Sydney. A major news media outlet further amplified this false information at scale, inflaming tensions. Social media users then acted on this misinformation, inciting

4 UN Human Rights Council Resolutions (2012-2018), The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/38/7 (5 July 2018), A/HRC/RES/32/13 (1 July 2016), A/HRC/RES/26/13 (26 June 2014), A/HRC/RES/20/8 (5 July 2012).
5 United Nations Human Rights Committee, *General Comment No. 36 Article 6: Right to Life*, UN Doc CCPR/C/GC/36 (3 September 2019) 2.
6 Ibid.
7 Ibid 3.
8 Ibid 21-26.

retribution and spreading baseless claims, which increased the risk of real violence against the innocent person and their loved ones.[9]

Another recent example is the case of a Queensland GP who faced death threats and abuse due to anti-vaccination misinformation circulating online about his practice. After false claims about the deaths of two children at his clinic circulated on social media, he was forced to withdraw from the COVID-19 vaccine rollout due to genuine and legitimate fears the doctor had for his and his colleagues' safety.[10]

3.2 The right to health

The right to health is contained in Article 12 of the *International Covenant on Economic, Social and Cultural Rights* (***ICESCR***) to which Australia is a signatory. The right to health is a fundamental human right that is indispensable for the exercise of other human rights.[11]

The right to health extends beyond the right to health care and health services but also includes underlying determinants of health such as access to safe water, sanitation, food, nutrition, healthy working conditions, and a healthy environment.[12]

As a signatory to the *ICESCR*, Australia has an obligation to ensure, among other things: adequate health facilities and goods, the equitable distribution of health resources, adequate immunisation programs, the prevention, treatment, and control of epidemic and endemic diseases, and adequate health education and information regarding prevalent health issues.[13]

Coordinated disinformation campaigns online pose a serious threat to our right to health, as highlighted during the COVID-19 pandemic.[14] During the pandemic, vaccines were one of the biggest topics of misleading health claims.[15] It is estimated that misinformation and disinformation about COVID-19 vaccines alone cost the United States' economy up to USD $300 million per day due to hospitalisations, long-term illness, lives lost and economic losses from missed work.[16]

3.3 The freedom of thought and conscience

The freedom of thought and conscience is contained in Article 18 of *the International Covenant on Civil and Political Rights* (***ICCPR***) and gives all people the right to think freely and hold beliefs or opinions based on their conscience, religion, or other convictions. Not only are these rights the foundation for every free and democratic society,[17] they also form a basis for the full enjoyment of other human rights.[18]

The freedoms of thought and conscience are absolute, meaning that the *ICCPR* does not permit them to be restricted, even in times of national emergency.[19]

---

[9] Joseph Palmer, 'Social media users incorrectly name killer in Sydney mall attack', *AFP Fact Check* (Online, 18 April 2024) < https://factcheck.afp.com/doc.afp.com.34PH9YM>.
[10] Anastasia Tsirtsakis, 'RACGP calls for anti-vaxxer crackdown after GP receives death threats', *Royal Australian College of General Practitioners*, (Online, 1 February 2022) <https://www1.racgp.org.au/newsgp/professional/racgp-calls-for-crackdown-on-anti-vaxxers-after-gp>.
[11] United Nations Economic and Social Council, *Substantive issues arising in the implementation of the international Covenant on Economic, Social and Cultural Rights General Comment No. 14 (2000)*, Committee on Economic, Social and Cultural Rights 22nd session, UN Doc E/C.12/2000/4 (11 August 2000) 1-3.
[12] Ibid 4.
[13] Ibid 43-44.
[14] Kirsten Pickles, 'Covid-19 misinformation trends in Australia: prospective longitudinal national survey' (2021) 23(1) *Journal of Medical Internet Research* <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7800906/>.
[15] Monica Wang, Olivia Britton, Jennifer Beard, 'The call for science communication and public scholarship' (2023) 13(3) *Translational Behavioural Medicine,* 156-159 <https://doi.org/10.1093/tbm/ibac096>.
[16] Ibid 156-159.
[17] UN Human Rights Committee, *General Comment No. 34: Article 19 (Freedoms of Opinion and Expression),* Human Rights Committee 102nd session, UN Doc CCPR/C/GC/34 (12 September 2011) 2.
[18] Ibid 4.
[19] Ibid 5.

The UN Human Rights Committee has noted that to protect the freedom of thought and conscience, countries must protect all people from undue interference from other individuals or organisations which could hinder their ability to enjoy these freedoms.[20]

Despite this obligation, digital platforms rely on powerful algorithms that prioritise viral, emotionally charged content which boosts user engagement and in turn increases their profits.[21] Because these algorithms are often opaque, users might think they are being served objective information, but in reality, the content they are seeing is shaped by many hidden factors, including the commercial imperatives of the platforms.

This can, in turn, impact or influence how users form and develop their opinions in a way that may be incompatible with Australia's obligations to protect the freedom of thought and conscience. For example, a 2015 study found that merely the way internet search results were ranked on a page could influence the voting preferences of undecided voters by 20 percent or more.[22]

3.4 The freedom of expression

Article 19 of the *ICCPR* guarantees the right to freedom of expression.

The right allows people to seek, receive, and share information and ideas through any medium.[23] The freedom of expression allows people to share all types of information, not just information that is true, albeit subject to some limited restrictions.[24]

Under Article 19, any restriction on the freedom of expression must meet the following criteria: it must be necessary and proportionate, clearly defined by law, and aimed at protecting the rights or reputation of others, or safeguarding national security, or public order, or public health, or public morals.[25]

Human rights law offers a universal framework for balancing the freedom of expression with other rights when conflicts arise. Effective regulation of digital platforms must be grounded in this legal framework to maintain this balance. Particularly as the freedom of expression must be interpreted in relation to other human rights, which ensures that one right does not unduly undermine or conflict with the protection of other rights. For example, human rights law requires that Article 19 be read alongside Article 20 of the *ICCPR*, which mandates that states must prohibit propaganda for war and speech that advocates national, racial, or religious hatred that incites discrimination, hostility, or violence.[26]

It is regrettable that a narrow interpretation of the freedom of expression advocated by some has been weaponised to avoid or hide any accountability for the harms caused by abuses <u>of</u> the freedom of expression.

However, it is also important to recognise that strict over-regulation, especially when it is not grounded in human rights law, can itself pose a legitimate threat to freedom of expression. Excessive or poorly designed regulations may suppress free speech, stifle public debate, or lead to censorship that is neither necessary nor proportionate.

A regulatory regime grounded in human rights law would protect users from both extremes—ensuring accountability for harmful content while safeguarding individuals from undue restrictions on their rights.

---

[20] Ibid 7.
[21] Ibid.
[22] Kate Jones, '*Online Disinformation and Political Discourse Applying a Human Rights Framework*', (Report, November 2019) <https://www.chathamhouse.org/sites/default/files/2019-11-05-Online-Disinformation-Human-Rights.pdf> 35.
[23] *International Covenant on Civil and Political* Rights, art 19(2).
[24] *International Covenant on Civil and Political* Rights, art 19(2).
[25] ICCPR Article 19. See also: UN Human Rights Committee, *General Comment No. 34* (2011) 22.
[26] ICCPR Article 20.

3.5 The right to privacy

Article 17 of the *ICCPR* guarantees the right to privacy. The right protects individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence, and from unlawful attacks on their reputation. This right ensures that personal information, communications, and private activities remain protected from undue intrusion.

The right to privacy is essential for preserving human dignity and autonomy, allowing people to freely express themselves, form consensual relationships, and engage in private matters without fear of unjust surveillance or exposure.[27]

Currently, digital platforms are falling well short of meeting these minimum standards – contrary both to their own obligations under business and human rights frameworks, and Australia's legal duty to protect people from human rights violations. Personal data online is collected, sold, and used extensively by platforms in opaque algorithmic processes, often without a user's awareness or full consent.

This widespread use of personal data by the platforms threatens our right to privacy while also generating significant profits for the platforms while leaving individuals with limited control over what happens to their information.[28]

3.6 The right to participate in public affairs and the right to vote

Article 25 of the *ICCPR* guarantees the right of citizens to participate in public affairs, either directly or through freely chosen representatives, and the right to vote in genuine and free elections. This right is fundamental to a functioning democracy, ensuring that citizens have a say in the governance of their country and that elections are conducted fairly and transparently.

The United Nations Human Rights Committee has emphasised that to protect this right, countries must ensure voters can form opinions independently, free from violence, coercion, or manipulation.[29] The Committee also highlights that the free exchange of information and ideas between citizens, candidates, and elected officials is essential for a functioning democracy.[30]

However, digital platforms and their opaque algorithms are distorting public debate around elections and referendums, including by spreading disinformation, about voting and electoral processes which can undermine democratic participation, discourage voting or campaigning, or prevent users from accessing accurate information on which to form their views and beliefs.[31]

Likewise, the collecting and trading of personal data to manipulate voting behaviour through highly targeted advertisements can also influence public debate or how they form their opinions.[32] For example, a political consulting firm could purchase or collect data on users that is held by a digital platform, which identifies individuals who are likely to be undecided voters to target them with misleading advertisements about an opponent candidate's political position.

[27] Kate Jones, '*Online Disinformation and Political Discourse Applying a Human Rights Framework*', (Report, November 2019) <https://www.chathamhouse.org/sites/default/files/2019-11-05-Online-Disinformation-Human-Rights.pdf> 37-38.
[28] Ibid 38.
[29] UN Human Rights Committee, *General Comment No. 25* (1996) 19.
[30] Ibid 25.
[31] Kate Jones, '*Online Disinformation and Political Discourse Applying a Human Rights Framework*', (Report, November 2019) <https://www.chathamhouse.org/sites/default/files/2019-11-05-Online-Disinformation-Human-Rights.pdf> 49.
[32] Ibid.

3.7 The Bill currently is not sufficiently grounded in human rights law and principles

We note, with disappointment, that the Bill is not sufficiently grounded in human rights law and principles.

Given the growing recognition of human rights as a vital component in regulating digital platforms, it is a missed opportunity that the Bill has overlooked this foundational framework.

The Bill's Statement of Compatibility with Human Rights (**Statement**) fails to adequately reflect the full spectrum of rights potentially impacted by its provisions. Notably absent from the Statement are fundamental rights such as the right to life and freedom of conscience.

The omission of these key rights represents a significant oversight, particularly given the far-reaching consequences that misinformation and disinformation can have on those rights as well as on the wellbeing of individuals and communities.

In contrast, the European Union's *Digital Services Act* (***DSA***) serves as a robust example of how human rights can be embedded into regulatory frameworks for misinformation and disinformation.

The *DSA* places clear obligations on digital platforms to assess the impact of their activities on fundamental rights. For example:

- Article 34 requires platforms to conduct risk assessments which must consider potential effects or risks on fundamental human rights.
- Article 35 mandates platforms to implement risk mitigation measures with a view to safeguarding those rights.
- Article 36 highlights that when assessing whether a platform is contributing to a serious threat or crisis in the Union, the protection of fundamental rights must be considered as part of this assessment.

Additionally, Article 1 of the *DSA* clarifies that one of its primary aims is to ensure the protection of fundamental rights within its regulatory scope. The Bill falls short of such clarity and ambition, leaving significant gaps in human rights protections for Australian users.

The Bill does acknowledge human rights to a certain extent. Notably, under the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth), legislative instruments, such as the codes, platform rules, and standards referenced made under the Bill, are required to be accompanied by a Statement.[33] While this is a positive inclusion, there are important limitations to note.

While these Statements can find that a legislative instrument is incompatible with or derogate from human rights, such a finding does not trigger an automatic review or inquiry mechanism. The lack of any such mechanism means that incompatible legislative instruments could remain in force without any further scrutiny.

Additionally, while future reviews of the Bill will consider its impact on freedom of expression, the scope of these reviews remains too narrow and does not adequately address the full range of human rights affected by misinformation and disinformation.

[33] Clause 47, Clauses 50-51, Clauses 55-63.

3.8 The practical distinction between misinformation and disinformation in the Bill is unclear

The Bill introduces two separate concepts: misinformation and disinformation. While the Bill provides detailed definitions for each, the practical distinction between them appears narrow.

Both misinformation and disinformation involve the spread of false or misleading information that causes or is likely to cause harm, yet the key difference lies in the intent. Disinformation is defined as the deliberate dissemination of falsehoods, whereas misinformation does not require intent.

This distinction, however, is blurred in the broader application of the Bill's regulatory framework. Both concepts trigger the same obligations and oversight mechanisms, with the only substantive difference being the scope of enforcement powers under section 67. Under this section, the Australian Communication and Media Authority (**ACMA**) may exercise take-down and banning powers for disinformation, but not for misinformation.

Given that both types of harmful content can lead to serious consequences, the Bill could benefit from further clarity on why such differing enforcement measures are necessary.

In light of the above, we make the following recommendations to the Committee:

1. **Australia needs a Human Rights Act.**
   A Human Rights Act would ensure that all people are protected under a consistent legal framework and would hold governments and public bodies accountable for upholding human rights. A Human Rights Act would provide a clear framework for balancing competing rights, reducing the need for ad-hoc approaches or piecemeal amendments to individual Bills. It could streamline legislative processes by embedding human rights considerations into lawmaking from the outset, ensuring that new laws are consistent with core rights principles. Additionally, having a Human Rights Act would strengthen public trust, as it would demonstrate the government's commitment to protecting individual freedoms and dignity for all, in a transparent and systematic way.

2. **The Bill should clarify the concepts of misinformation and disinformation.**
   Currently, the Bill introduces separate definitions for misinformation and disinformation, with the only substantive difference being the scope of take-down and banning powers under clause 67. This separation is unclear and may create confusion. The Bill should clearly signpost that the primary difference lies in the enforcement mechanisms provided under clause 67. This amendment would improve clarity and regulatory coherence.

3. **Clause 70(1) should be amended to bring forward the timing of the first review of the Bill.**
   Clause 70(1) currently requires that the first review of the Bill take place after the third anniversary of its commencement, followed by subsequent reviews at intervals of no longer than three years. Given the potential impact this Bill may have on fundamental rights, it is recommended that the clause be amended to require the first review after two years of operation. Such a review could also consider the efficacy and appropriateness of ACMA's regulatory powers. Subsequent reviews should continue at intervals of no more than three years, ensuring that the Bill's effects are monitored in a timely and thorough manner.

4. **Clause 70(2) should be amended to broaden the scope of the review to include all applicable human rights.**
   At present, clause 70(2) limits the review to assessing the impact of the Bill on the freedom of expression. This is too narrow. It is recommended that the clause be amended to require an assessment of the Bill's impact on a wider range of human rights, including but not limited to the right to life, the right to health, freedom of conscience and religion, freedom of expression, the right to privacy, and the right to participate in public affairs and vote. This broader scope will ensure that the review addresses the full spectrum of human rights affected by misinformation and disinformation.

We propose the following amendments to the current drafting of clause 70(2)(a) to give effect to the above:

The review must:

(a) include an assessment of the impact of this Part on human rights. An assessment conducted for the purposes of this clause 70(2)(a) must include, but is not limited to, an assessment of the impact of this Part on freedom of expression, freedom of conscience and religion, the right to privacy, the right to health, the right to life, and the right to participate in public affairs and vote; and

[...]

5. The creation of digital platform rules, codes and standards should be subject to adequate Parliamentary oversight.

Digital platform rules, misinformation codes, and misinformation standards should be referred to a Parliamentary Committee for review, specifically to assess their impact on human rights, as soon as they are registered in the Federal Register of Legislation as legislative instruments. This Committee's mandate should focus solely on evaluating the effects of these regulations on the human rights that Australia is obligated to protect, as outlined in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth). The Committee should have the authority to hold public hearings, consult relevant stakeholders, and ideally report its findings to Parliament before the end of the legislative instrument's disallowance period.

6. Clause 11(e) should be amended to reflect a broader commitment to human rights in the Bill's objectives.

Clause 11(e) presently refers to the Bill's objective of empowering ACMA to regulate in a way that respects the freedom of expression. This clause should be amended to reflect a broader commitment to human rights more broadly, ensuring that ACMA's powers are exercised in a manner that respects and upholds the full range of human rights Australia is obliged to protect, not just the freedom of expression. This change would align the Bill's objectives with a human rights-based approach to regulation.

We propose the following amendments to the current drafting of clause 11(e) to give effect to the above:

The objects of this Part are:

[...]

(e) to provide the ACMA with powers, which respect and uphold all human rights that Australia has an obligation to protect under international human rights law including but not limited to the freedom of expression, to take action for the purposes of this Part; and

7. Media literacy plans must be accessible to be effective.

The Bill's provisions for media literacy plans are unlikely to be effective unless they are made accessible and understandable to the groups they aim to serve. We recommend that the following requirements be mandated for all media literacy plans:

- Media literacy plans must be available in at least the top 10 languages spoken in Australia per the most recent Census.
- If the platform is accessible to minors, the media literacy plans must be understandable to this group.
- Media literacy plans must be provided in plain English and also in accessible formats to ensure inclusivity.

Failure to meet these standards will render media literacy plans ineffective and will exclude large sections of the population, including people whose main language is a language other than English, children and young people, and people with disability, making this aspect of the Bill incompatible with human rights by undermining the right to education, freedom of expression, and the right to access information – all of which are integral to ensuring that all people can navigate online spaces in a safe and informed manner.

8. The Australian Human Rights Commission should be consulted on the development of codes.

A new clause 47(1)(h) should be introduced, requiring that the ACMA be satisfied that the Australian Human Rights Commission has been consulted in the development of any code under the Bill. This consultation process is crucial to ensuring that human rights expertise is embedded into the code's development, and that the impact on human rights is carefully considered. This measure would enhance the Bill's alignment with Australia's human rights obligations and promote greater accountability in the regulation of digital platforms.

4. Self-regulation will be ineffective

We strongly oppose the Bill's reliance on digital platform self-regulation at first instance.

If the ACMA does not take a more assertive approach from the outset, the Bill must ensure greater access to the data and processes used by digital platforms, as this information is currently shared only voluntarily and in an inconsistent manner

Such information will enable independent review and assessment of the platforms' conduct, with the risk of ongoing reputational damage incentivising process improvement on a separate front to the threat of the ACMA's discretionary infringement notices or civil penalties.

Experience has shown that relying on self-regulation by large corporations is ineffective and insufficient to address serious issues. A notable example is the voluntary Food and Grocery Code of Conduct, which was introduced to regulate the conduct of supermarket retailers and wholesalers toward their suppliers.[34] A Treasury review found that the Code failed to achieve its purpose due to the significant power imbalance between major supermarket chains and their smaller suppliers.[35]

Repeated allegations of misuse of power by large corporations eventually led the Australian Government to introduce a mandatory code of conduct, which imposes multimillion-dollar penalties for serious breaches. As a result, corporations like Coles, Woolworths, and Metcash will be subject to multi-million-dollar penalties for serious breaches of the new code.[36]

At present, platforms are not voluntarily providing key data to researchers in Australia that would allow independent review.[37]

Recently, Reset Tech Australia requested access to Meta's data. The request included data on how Meta detects fact-checked falsehoods and data describing the accuracy of Meta's content moderation processes. This request was rejected, with Meta stating that the information that was being requested by Reset Tech Australia was irrelevant to its transparency reporting.[38]

In addition, Meta's recent shutdown of CrowdTangle – a tool used by researchers, watchdog organisations and journalists to monitor social media posts to track how misinformation spreads on the company's platforms – evidences a clear intention to provide less assistance, rather than more, when it comes to combatting misinformation and disinformation on its own volition.

Recently, Elon Musk's X Corp took legal action against the Center for Countering Digital Hate, based in the United State of America.[39] X accused the non-profit of violating the platform's terms of service by compiling public data and publishing reports that documented the rise in hate speech on the platform after Musk's acquisition.[40] Although the lawsuit was dismissed by the U.S. District Court Judge the Honourable Judge Breyer, who ruled that the lawsuit was about punishing the non-profit for its speech rather than addressing any legitimate technological harm,[41] the case underscores the precarious position researchers find

---

[34] The Treasury, '*Independent Review of the Food and Grocery Code of Conduct',* (Final Report, June 2024) 10.
[35] Ibid 19.
[36] Australian Government, *Government Response to the Independent Review of the Food and Grocery Code of Conduct'*, (Online, June 2024) <https://treasury.gov.au/sites/default/files/2024-06/p2024-534717-gr.pdf> 5-6.
[37] Reset Tech Australia, '*Submission to Inquiry into the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 [Provisions]* (Online, September 2024) <https://au.reset.tech/news/> 8-10.
[38] Reset Tech Australia, '*Submission to Inquiry into the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024 [Provisions]* (Online, September 2024) <https://au.reset.tech/news/> 8-10.
[39] Barbara Orturay, David Klepper, 'Judge dismisses lawsuit by Musk's X against non-profit researchers tracking hate speech on platform', *The Associated Press* (Online, 10 March 2024) <https://apnews.com/article/x-twitter-musk-hate-speech-lawsuit-fafa1904f5525f9ab64250e81a72d210>.
[40] Ibid.
[41] Ibid.

themselves in when their work challenges powerful platforms. Without sufficient legal protections, researchers can be subject to costly and lengthy legal battles intended to silence them.

These examples illustrate the necessity of regulatory incentives to ensure platforms provide essential data for decision-making and research. The *DSA* requires large platforms to provide timely access to data for researchers, similar provisions should be considered for Australia.[42]

In this vein, existing Application Programming Interfaces (**API**) and data libraries should be made accessible to independent researchers, which would support a sustainable research ecosystem crucial for combating misinformation and disinformation effectively.

In this context, we make the following recommendations to the Committee:

9. **Reports submitted to ACMA under digital platform rules should be released to the public to enhance public trust and understanding of the Bill's functionality.**
Clause 17 of the Bill allows digital platforms to publish their risk assessment reports, misinformation and disinformation policies, and media literacy plans. While we commend this initiative, we recommend the creation of a single, coordinated repository for public users to access this information, administered by the ACMA. Furthermore, all materials submitted to the ACMA by platforms should be made publicly accessible via this repository after a reasonable period.

10. **Platforms should be required to grant free access to operational application programming interfaces (APIs) to enhance transparency.**
Operational researcher API, content library, or other access tools already in use by platforms should be made freely accessible to Australian researchers that are affiliated with accredited organisations, including academic institutions and not-for-profit entities, provided that these have non-commercial purposes.

11. **The Bill should be amended to include specific immunities for Australian researchers acquiring platform data for good faith research.**
The Bill should be amended to include specific immunities for Australian researchers acquiring platform data for good faith research. The research environment surrounding misinformation and disinformation is fraught with challenges, including significant financial barriers and evolving legal risks to researchers acting in good faith. These obstacles have limited the capacity of many organisations to engage in this critical area. Recent cases, such as the lawsuit by Elon Musk's X Corp. against the Center for Countering Digital Hate, which was dismissed for attempting to punish researchers for compiling public data, highlight the growing risk for researchers studying platform behaviour. Without clear legal protections, Australian researchers could face similar punitive actions, stifling vital research.

[42] Article 40.12.

5. Platforms should owe a duty of care

A legislated duty of care owed by digital platforms – being a legal obligation to ensure the safety and well-being of others by taking reasonable steps to prevent harm or injury –is essential to protect users from harm.

The Bill must require platforms to proactively design their systems to prevent harm in the first place, rather than providing that the only protective mechanism is a retrospective review of content posted to those platforms. To be effective, a duty of care should require digital platforms to:

a. uphold and protect the fundamental human rights of users;

b. undertake comprehensive risk assessments to identify and analyse risks stemming from their products and systems;

c. address identified risks though effective risk mitigation measures; and

d. open up their assessment and mitigation measures for public scrutiny, including by third parties, to enable independent testing and verification of platform's claims.

Similarly, there must also be effective mechanisms for redress for harms caused by a digital platform's breach of their duty of care.

5.1 Approach under the *DSA*

The *DSA* takes a risk-mitigation based approach to regulating digital platforms, underpinned by extensive transparency and accountability requirements that are imposed on the platforms. These include:

a. **comprehensive risk assessments**: large digital platforms are required to undertake annual risk assessments to identify significant systemic risks arising from the functioning and use of their services. This encompasses algorithms, recommender systems, content moderation systems, user terms and conditions, advertising systems and data-related practices;[43]

b. **risk mitigation**: where risk assessments undertaken by large platforms identify systemic risks, these platforms are required to implement "reasonable, proportionate and effective mitigation measures";[44]

c. **transparency measures**: large digital platforms must follow the following procedures:

   i. platforms' risk assessments and mitigation measures are subject to independent audits;[45]

   ii. platforms must provide annual public transparency reports which are heavily prescriptive;[46]

   iii. large platforms must provide advertising repositories, which are openly searchable, and include details regarding the advertisements on their platforms, including information about who paid for the advertisement;[47] and

[43] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (*Digital Services Act*), art 34.
[44] Ibid art 35.
[45] Ibid art 37.
[46] Ibid art 17.
[47] Ibid art 39.

iv. on request from the regulator, platforms are required to provide independent researchers with access to platform data to detect, identify and understand the systemic risks that have been reported by the platforms and to assess the adequacy, efficiency and impacts of the platforms' risk mitigation measures;[48] and

d. **regulator oversight:** the *DSA* provides the regulator, the European Commission, with strong enforcement powers, including the ability to impose significant penalties for violations. These can amount to fines of up to 6% of a platform's worldwide annual turnover for breaches of *DSA* obligations or applying periodic penalties of up to 5% of the average daily worldwide turnover for each day that a platform delays in complying with remedies.[49]

5.2 Approach under the UK's *Online Safety Act*

The United Kingdom's *Online Safety Act 2023* (**UK's *Online Safety Act***) also takes a similar risk-mitigation approach to regulation while imposing duties on social media companies and search engines to protect users, particularly children, from online harm.[50] Key provisions of the UK's *Online Safety Act* include:[51]

a. **risk reduction**: platforms must implement systems to minimise the risk of illegal activity on their services and actively remove illegal content when it appears. The strongest protections are for children, requiring platforms to block harmful and age-inappropriate content;

b. **transparency and control**: platforms must be transparent about the harmful content on their services and provide tools for users to control what they see online;

c. **regulator oversight**: The Office of Communications, the independent regulator, is empowered to enforce the UK's *Online Safety Act*, set safety standards, and ensure platforms comply with new duties. Significant penalties can be imposed for violations, including fines up to £18 million (approximately AUD$35,372,000) or 10% of a platform's global revenue – whichever is the highest; and

d. **global reach**: the UK's *Online Safety Act* applies to any service accessible in the UK, even if the company is based outside the country.

5.3 Lessons for Australia

Mitigating risk is a practical way to reduce potential harms while still allowing room for innovation and growth. This approach applies the strongest protections where the risks are highest, helping to build accountability and trust across digital industries without slowing progress.

Australia has an opportunity to draw upon successful frameworks established by *DSA* and the UK's *Online Safety Act* to inform our regulatory framework. The Bill should be amended to establish a legislated duty of care for digital platforms, mandating a legal obligation to ensure they prioritise the safety and well-being of users.

By establishing a clear and enforceable duty of care, we can foster accountability among digital platforms, protect users from harm, and encourage an environment of safety and trust in the digital landscape. This proactive approach will help mitigate risks while allowing room for innovation and growth, ultimately enhancing user safety and well-being.

---

[48] Ibid art 40.
[49] European Commission, *'The Enforcement Framework Under the Digital Services Act'* (Website, 30 April 2024) <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>.
[50] Department for Science, Innovation & Technology (UK), *'Guidance- Online Safety Act: Explainer'* (Website, 8 May 2024) <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>.
[51] Ibid.

In light of the above, we make the following recommendation to the Committee:

12. The Bill should establish a legislated duty of care for digital platforms. Drawing on the examples provided by the *DSA* and the UK's *Online Safety Act*, this duty should require platforms to proactively design their systems to prevent harm from occurring in the first place. To be effective, the duty of care should similarly require platforms to uphold and protect the fundamental human rights of their users and consider the impacts on human rights as part of their risk assessment.