Online Safety Amendment (Digital Duty of Care) Bill 2026

Submission

22 September 2026

policy@wesnet.org.au
safety.policy@WwWA.com.au

Acknowledgment of Country

Wesnet and the Working with Women Alliance acknowledge First Nations peoples as the Traditional Custodians of the lands on which we live and work. We pay our respects to Elders past and present, and recognise the enduring connection of Aboriginal and Torres Strait Islander peoples to land, waters, culture and community. We acknowledge that sovereignty was never ceded. This always was and always will be Aboriginal land. We recognise that First Nations women, gender-diverse people and children experience disproportionate rates of gender-based violence as a result of the ongoing impacts of colonisation, dispossession, discrimination and structural inequality. We also recognise the strength and leadership of First Nations women, gender-diverse people, and communities in preventing and responding to violence. We affirm the importance of community-led solutions grounded in culture and self-determination and commit to being informed by the experiences and advocacy of First Nations women and gender-diverse people in our work towards safety and equality.

Acknowledgement of survivors

Wesnet and WwWA also acknowledge all survivors of gender-based violence. We pay respect to those who did not survive and to their family members and friends.

About Wesnet

We are the Peak body for Specialist Women's Domestic and Family Violence (DFV) Services in Australia. Our vision is a future where all women, gender-diverse people and children live free of domestic and family violence and its consequences.

With almost 400 eligible members across Australia, Wesnet represents a range of organisations, the core business of which is supporting survivors of DFV, including women's refuges and supported accommodation services, crisis response and case management services, counselling, recovery and information and referral services. Harnessing its large national network of members and associate members, Wesnet plays an important role in identifying unmet needs, canvassing new and emerging issues, facilitating policy and sector debate and providing advice to government to provide improved responses to the problem of domestic and family violence. We do this within our communities, and in partnership with non-government stakeholders.

Wesnet works within a feminist framework which promotes understanding domestic and family violence as gendered violence, and that women's and children's experiences are also intrinsically shaped by their ethnicity, culture, ability, age, gender identity and class.

About WwWA

The Working with Women Alliance (WwWA) is a national membership-based organisation representing two connected portfolios: gender-based violence and gender equality. Across these portfolios, WwWA has more than 800 members, including specialist services, advocates, researchers, lived-experience representatives, peak bodies and organisations working across women's safety and economic security. WwWA is one of five national women's alliances, funded through the Department of the Prime Minister and Cabinet to ensure that women's voices are central to policy development. Through this role, WwWA works with members, civil society and the Australian Government to provide evidence-based, intersectional gender equality advice on the areas of greatest impact and influence under *Working for Women: A Strategy for Gender Equality*.

Introduction

Wesnet and WwWA welcome the opportunity to provide a submission to the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the department) on the Exposure Draft of the *Online Safety Amendment (Digital Duty of Care) Bill 2026*.

Despite the short consultation period, Wesnet and WwWA have collaborated on this submission to bring together our shared expertise in gender-based violence, technology-facilitated abuse and gender equality. Wesnet and WwWA support the introduction of a Digital Duty of Care. A systems-based duty is the right regulatory response to harms that are produced and amplified by the systems and design choices of online service providers. The shift away from relying on incident-by-incident complaints and content takedowns is necessary and overdue. We agree with the findings of the Statutory Review of the *Online Safety Act 2021* that a systems-based regulatory model is the only way to achieve meaningful improvements in online safety. The concerns and recommendations raised in this submission should be read from this position of support. They do not question the decision to introduce a Digital Duty of Care. Rather, they identify where the exposure draft must be strengthened to ensure the new duty delivers on its intended purpose, including by meaningfully addressing gender-based violence, particularly for women, trans and gender diverse people from communities that are marginalised.

The Bill recognises some manifestations of gender-based violence, but does not recognise gender-based violence as the overarching harm or expressly require providers to assess it as a systemic risk. This is a significant omission given the scale of technology-facilitated gender-based violence (TFGBV) and the Government's public framing of the reform as a response to online misogyny and violence against women and gender-diverse people. The omission is particularly stark given the scale of technology-facilitated violence in the context of domestic and family violence:

- 99.7% of specialist domestic and family violence practitioners surveyed by Wesnet reported supporting clients who had experienced TFGBV.[1]
- More than half of practitioners reported seeing technology-facilitated tactics more frequently than abuse perpetrated without it, while a further 31% encountered both equally as frequently.[2]

This exposes a wider gap between the Australian Government's commitments and its broader reform agenda. The Government is currently developing the Second Action Plan under the *National Plan to End Violence against Women and Children 2022–2032* and has repeatedly declared, including through National Cabinet, that ending gender-based violence is a national priority. But that priority is still not consistently reflected in the major tech policy reforms that shape victim-survivors' lives and safety.

Language Note

In this submission, Wesnet and WwWA use 'gender-based violence' as an inclusive term to acknowledge the targeted perpetration of violence against gender-diverse people. We also recognise that gender-based violence often refers to the disproportionate impact of violence against women and children. At times, this submission uses 'women' or 'women and children' for brevity, or where this reflects the evidence, policy settings or services being discussed. This should not be read as excluding gender-diverse and non-binary people from the analysis or recommendations. Wesnet and WwWA recognise the distinct ways violence can be shaped by homophobia, biphobia, transphobia, intersex discrimination and other forms of stigma and exclusion, and the need for safe, affirming, accessible and community-led responses.

Recommendation Summary

Technology-facilitated gender-based violence

1. Amend the Bill to expressly recognise gender-based violence, including technology-facilitated gender-based violence, as a foreseeable systemic risk that online services must assess and mitigate.
2. Broaden paragraph 25C(1)(c) to recognise gender-based violence, including sexual violence, as a category of serious harm, and introduce definitions of gender-based violence and technology-facilitated gender-based violence.
3. Amend clause 26A to require providers to assess how any functionality of an online service may foreseeably be used by one person to harm another, whether or not that functionality was designed or intended for that purpose.

Public-interest information and proportionate moderation

4. Amend clause 26A to require providers to assess harms arising when moderation, ranking or recommender systems remove, restrict or deprioritise lawful public-interest information.
5. Require providers to distinguish material that perpetrates, promotes or amplifies gender-based violence from material shared for prevention, education, journalism, advocacy or support.
6. Require providers to assess whether moderation systems disproportionately restrict the content or accounts of people with protected characteristics and/or communities experiencing structural discrimination.

Enabling a safer, inclusive, healthy and rights-respecting online environment

7. Amend 3(A) from 'imposing a duty on persons responsible for online services to ensure a safe online environment' to 'imposing a duty on persons responsible for online services to actively enable a safe, inclusive, healthy and rights-respecting digital environment in the long term'.

Image-based abuse

8. Bring image-based abuse fully within the Digital Duty of Care by expressly including non-consensual intimate material, altered or synthetic intimate images, threats to distribute intimate material and sexual extortion within clause 25C.
9. Define 'fake nude material' in section 5 by reference to the definition of 'intimate image' in section 15.
10. Extend section 86B to services designed for, or predominantly used to facilitate, the non-consensual sharing of intimate images.

A baseline of protection for children and adults

11. Insert an adult equivalent of subparagraph 25B(1)(b)(ii), so that all persons in Australia are protected from harms associated with the operation of design features.
12. Move or replicate the section 25D categories within section 25C, subject to an appropriate seriousness threshold, so that adults are protected from misogynistic material and conduct.
13. Amend clause 25C to include material that promotes or normalises violent practices capable of causing serious injury or death, including strangulation, with alignment to the *Criminal Code Act 1995* where appropriate.

14. Require providers to assess and mitigate harms arising from recommender or ranking systems that amplify misogynistic material or create pathways towards increasingly harmful content.
15. Harmonise the Bill's references to "Australians", "persons in Australia", "users in Australia", "Australian user accounts", "Australian children" and "Australian adults". Protection should apply where harm affects a person in Australia or otherwise has a substantial connection with Australia, regardless of citizenship, visa status or account status.

Systemic discrimination, intersecting and cumulative harm

16. Amend clauses 25C and 25D to expressly recognise material or conduct that attacks, dehumanises or promotes hostility towards people based on one or more protected characteristics. Retain express recognition of misogyny and hostility towards women or gender equality.
17. Amend clause 25D to expressly recognise racial and religious hostility or vilification as harmful to children, including hostility directed towards a child's ethnic, religious or migrant community.
18. Require providers to consider harm directed at a person by reference to a combination of protected characteristics, rather than assessing each characteristic in isolation.
19. Broaden the definition of harm and the risk-assessment requirements to capture persistent conduct, cumulative effects and volumetric attacks, including conduct occurring across multiple accounts or services.

Algorithmic accountability and user choice

20. Require prescribed providers to give the eSafety Commissioner an initial whole-of-service transparency report at the commencement of the Digital Duty of Care and before introducing a prescribed recommender system in Australia.
21. Amend paragraph 26(3)(a) so that appropriate management of design features is defined by reference to not recommending or amplifying seriously harmful material, with user empowerment tools additional to that obligation rather than illustrative of it.
22. Require transparency reports to explain how recommender and ranking systems operate, what they are designed to optimise and how providers identify and mitigate gendered or discriminatory harm.
23. Apply consumer protection frameworks to the male grievance industry as a commercial infrastructure.

Enforcement and redress

24. Provide a direct right of action for a person harmed by a provider's failure to uphold its Digital Duty of Care.
25. Develop a whole-of-government, no-wrong-door approach to online harm, supported by formal coordination and information sharing across relevant regulators.

Guidance

26. Amend clause 26E to require the Commissioner to issue a code of practice on preventing and addressing gender-based violence in online services, developed in consultation with the Domestic, Family and Sexual Violence Commissioner, specialist services and victim-survivor advocates.

1. Gender-based violence must be named in the digital duty of care

The exposure draft recognises some specific manifestations of gender-based violence but does not embed gender-based violence within the operative architecture of the Digital Duty of Care. Paragraph 25C(1)(c) includes material or conduct that encourages, promotes, incites or instructs sexual violence. Paragraph 25C(1)(e) covers explicit threats of physical violence, including threats of rape. Paragraph 25C(1)(f) covers material or conduct intended to cause serious harm by menacing or harassing an individual. These inclusions are welcome, but they capture particular manifestations of gender-based violence rather than recognising the overarching harm.

WwWA and Wesnet are concerned that this will have practical consequences. Sexual violence is a form of gender-based violence, yet the Bill expressly recognises the former without naming the broader category to which it belongs. Gender-based violence is therefore left to be interpreted through general categories such as menacing and harassment. Without statutory definitions of gender-based violence and technology-facilitated abuse, providers may treat conduct as isolated incidents rather than recognising patterns of gendered harm, including violence and control.

- **Broaden paragraph 25C(1)(c) to recognise gender-based violence, including sexual violence, as a category of serious harm, and introduce definitions of gender-based violence and technology-facilitated abuse.**

2. Gender-based violence must be a question of platform governance

Beyond defining gender-based violence and recognising it within clause 25C, the Bill must embed it within the risk-assessment obligations imposed on providers. Naming harmful material and conduct is not the same as requiring providers to examine the systems through which that harm is enabled or amplified. Clause 25C identifies the material and conduct relevant to a safe online environment. Clause 26A determines what providers must examine when assessing reasonably foreseeable risks arising from their services. However, clause 26A does not expressly require providers to assess the risk of gender-based violence or technology-facilitated abuse.

The European Union's *Digital Services Act* (DSA) provides a useful precedent for embedding gender-based violence within a systems-based regulatory framework. The EU DSA prescribes that providers of very large online platforms and of very large online search engines address "*any actual or foreseeable negative effects in relation to gender-based violence*".[3] GBV harms captured under the DSA include harassment, gendered hate, and extreme misogyny content.[4] The DSA Observatory states: *"the DSA's systemic risk framework treats TFGBV as a question of platform governance. Its object of regulation is not harmful content itself but the systems, governance structures and design choices that make such harms foreseeable and scalable"*.[5]

The Digital Duty of Care should take the same approach. Providers should be required to assess how the operation of their services can enable or amplify gender-based violence, including through the foreseeable misuse of ordinary functionality. TFGBV is often perpetrated through ordinary service functionality, rather than only through the design features that clause 25G deems to have innate 'negative behavioural impacts'. Duty holders must be required to look beyond individual instances of

harm; to examine how ordinary service features operate as a collective to facilitate patterns of abuse, and whether safety systems respond to the gendered context in which these harms occur. Expressly recognising TFGBV as a systemic risk would ensure it is treated as a responsibility of platform governance, rather than left to victim-survivors to identify and report individual incidents. It would also give providers and the eSafety Commissioner a clear basis for assessing whether services have taken reasonable steps to prevent and mitigate that risk.

- **Amend the Bill to expressly recognise gender-based violence, including technology-facilitated gender-based violence, as a foreseeable systemic risk that online services must assess and mitigate.**

3. Technology-facilitated abuse is often enabled through ordinary functionality

TFGBV cannot be understood only through obviously abusive content or explicit threats. It is often perpetrated through ordinary service functionality that is not inherently harmful. Location sharing, image sharing, activity indicators, read receipts, account suggestions and communication functions can all be used to monitor or control victim-survivors. Features that allow users to create new accounts after being blocked or contact people who do not follow them can also enable perpetrators to continue abuse after a victim-survivor has attempted to disengage.

Perpetrators do not require features designed to cause harm, or features with innate 'negative behavioural impacts'. Ordinary functionality is sufficient, and it is what perpetrators routinely use. The harm may arise through repeated conduct or the combined use of different features over time. Conduct that appears innocuous when viewed in isolation can form part of a wider pattern of gender-based violence.

The exposure draft's general references to harmful material and conduct may capture some of this abuse. However, the Bill does not expressly require providers to consider the gendered context in which their services are used or the foreseeable ways their functionality can be used to perpetrate harm. Clause 25F defines "design features" inclusively, meaning the concept is not legally confined to the features expressly listed. However, the listed features are primarily associated with engagement and content consumption, including recommender systems, endless feeds and feedback mechanisms. Clause 25G then deems these same categories to have innate "negative behavioural impacts", rather than misuse of ordinary functionality. This framing directs attention towards how design features affect a user's behaviour, such as by encouraging compulsive use or amplifying harmful material. This leaves TFGBV implicit within a general duty, despite the Government's own emphasis on gendered online harm. This gap is reinforced by clause 25F. The five design features identified in that clause are directed primarily towards engagement and addictive design. They do not reflect the ordinary functionality through which technology-facilitated abuse and gender-based violence is commonly perpetrated.

Subparagraph 26A(2)(a)(iii) requires providers to identify design features that give rise to reasonably foreseeable risks. While that obligation may extend beyond the examples in clause 25F, the Bill does not expressly require providers to assess how ordinary functionality may be misused in perpetrating

gender-based violence. Without that direction, providers may focus on the listed engagement features while overlooking account settings, location functions and contact mechanisms that perpetrators routinely use. The assessment must also extend beyond individual uses of a feature. Technology-facilitated abuse and gender-based violence may involve repeated conduct across different accounts or services. A risk assessment that treats each action separately may fail to identify the course of conduct through which control is exercised.

- **Amend clause 26A to require providers to assess how any functionality of an online service may foreseeably be used by one person to harm another, whether or not that functionality was designed or intended for that purpose.**

4. Providers must prevent harm without suppressing public-interest information

While it is important to address the harms emerging from the circulation of certain content, it is equally important to address the harms emerging from the removal, suppression and non-circulation of public-interest material.[6] The exposure draft requires providers to identify and assess reasonably foreseeable risks associated with their services, including risks arising from content, design features and other systems or processes. This is an important shift towards proactive regulation. However, the Bill's risk framework focuses primarily on harms arising from the circulation of material and conduct. It does not expressly require providers to consider harms arising from their own moderation and recommender systems.

The Digital Duty of Care must account for both. Providers should be required to prevent the circulation and amplification of harmful material, while ensuring their systems do not unreasonably remove, restrict or deprioritise lawful public-interest information. This distinction is particularly important in relation to gender-based violence. Material discussing violence may contain language, images or descriptions that automated moderation systems identify as harmful. But the same material may be essential to community education or help seeking. For example, non-fatal strangulation poses a risk to women and girls. It is a risk factor in intimate partner violence and 'one of the most lethal forms'.[7] Women whose partners tried to strangle them were over seven times more likely than other women survivors to be killed.[8] Non-lethal strangulation can leave little physical evidence, and lead to serious injury, acquired brain injury or death. Public-awareness campaigns such as It Left No Marks communicate these risks and support earlier recognition and help-seeking. A moderation system focused only on references to violence or strangulation may fail to distinguish between material that promotes harm and material intended to prevent it.

The risk is not confined to automated moderation. Content removal, account restrictions and reduced visibility can also result from human moderation or the interaction of automated and human decision-making. These practices can be applied unevenly, with women, sex workers, activists and communities experiencing structural discrimination disproportionately affected. The suppression of their accounts can restrict access to public-interest information and limit the reach of advocacy and education.

A holistic risk-based duty

The EU DSA model strikes a balance in addressing the circulation of harmful content, need for public interest material and freedom of expression based in human rights frameworks.[9] The DSA prescribes that providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess four systemic risks:

a) the circulation of illegal content,
b) any actual or foreseeable negative effects for the exercise of fundamental rights, including human dignity, protection of personal data, freedom of expression and information, including the freedom and pluralism of the media, non-discrimination, and consumer protection;
c) actual or foreseeable negative effects on civic discourse and electoral processes, and public security;
d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.[10]

The Digital Duty of Care should adopt this broader approach by requiring providers to assess whether their systems can distinguish material that perpetrates or amplifies gender-based violence from public-interest material intended to prevent violence, support victim-survivors, inform the community or hold perpetrators and institutions to account.

- **Amend clause 26A to require providers to assess harms arising when moderation, ranking or recommender systems remove, restrict or deprioritise lawful public-interest information.**
- **Require providers to distinguish material that perpetrates, promotes or amplifies gender-based violence from material shared for prevention, education, journalism, advocacy or support.**
- **Require providers to assess whether moderation systems disproportionately restrict the content or accounts of people with protected characteristics and/or communities experiencing structural discrimination.**

5. Enabling a safer, inclusive, healthy and rights-respecting online environment

While a risk-based model would contribute to improving online safety, the Digital Duty of Care can be strengthened with a more inclusive outcomes-based model. At present, the Bill proposes the responsibility of online services to 'ensure a safe online environment'. Borrowing from researchers at the ARC Centre of Excellence for Automated Decision-Making and Society and the Centre for Artificial Intelligence and Digital Ethics,[11] we suggest that this outcome can be strengthened to require services to 'actively enable a safe, inclusive, healthy and rights-respecting digital environment in the long term'.[12] There are precedents for this, such as anti-discrimination legislation that protects individuals from discrimination based on race, sex, disability and age. For instance, the introduction of positive duty into the Sex Discrimination Act 1984 requires that organisations and businesses have a positive duty to eliminate, as far as possible, in a work context or in connection to work.

- **Amend 3(A) from 'imposing a duty on persons responsible for online services to ensure a safe online environment' to 'imposing a duty on persons responsible for online services to actively enable a safe, inclusive, healthy and rights-respecting digital environment in the long term'.**

6. Bring image-based abuse fully within the reforms

The Bill strengthens responses to image-based abuse, including through new powers targeting services that generate synthetic intimate images. However, gaps remain across the Digital Duty of Care and the intimate image scheme. Clause 25C does not expressly recognise non-consensual intimate images, including synthetic or technologically altered images, or threats to distribute them, as seriously harmful material or conduct. While clause 26A requires providers to assess reasonably foreseeable risks of harm, express inclusion in clause 25C would make clear that providers must prevent and mitigate the systemic risks that enable image-based abuse. This would complement the removal pathway in Part 6, which operates after an intimate image has been shared. The Bill also introduces a pathway for responding to reposted or altered material but does not extend it to intimate images. Victim-survivors should not be required to make a fresh complaint or objection notice each time an image is copied, altered or redistributed. Further, proposed Part 6A uses the undefined term "fake nude material" and applies only to services that generate such material. It should clearly cover the full definition of an intimate image in section 15 and services designed for, or predominantly used to facilitate, the non-consensual sharing of intimate images.

7. Online harm and misogyny do not end at 18

The exposure draft creates two different standards of online safety. For adults, providers are required to prevent and address only material and conduct that meets the Bill's threshold of being "seriously harmful". Children receive broader protection from material and conduct that the Bill recognises as harmful, even where it does not meet that higher threshold. For example, clause 25D recognises content promoting disordered eating, bullying and harmful practices as harmful to children. It also expressly recognises material or conduct that encourages or promotes hostile attitudes towards women or gender equality. These protections are not extended to adults through clause 25C.

This is an arbitrary distinction. Misogyny does not become harmless when a person turns 18. Nor are its impacts confined to the people consuming misogynistic material.

The omission is particularly significant given the Government's public emphasis on the manosphere in making the case for the Digital Duty of Care. The manosphere consists of online spaces and communities that centre on male grievances and empowerment, and what it means to be a man. Key beliefs include misogyny and male supremacy that emphasise traditional rigid gender roles: violence against girls and women can be normalised as part of being a "real man".[13] This translates into in-person impacts and behaviours, such as girls, young women and gender-diverse people feeling unsafe at schools and women teachers experiencing gender-based violence ranging from verbal comments and harassment like 'make me a sandwich', implying women's place is in the kitchen, or making sexually suggestive comments.[14] There are also links between key beliefs promoted in the manosphere and hate crimes, particularly against LGBTIQA+ communities and migrant and refugee communities.[15] A current Victorian Inquiry is examining how the manosphere is contributing to homophobic and

biphobic attacks on gay and bisexual men.[16] While sexism is not new, the manosphere amplifies disrespect towards girls, women, and gender-diverse people by boys and men. An Australian study shows that almost two-thirds of the young men surveyed were regularly engaging with men and masculinity influencers. The same study finds that regular engagement with such content was linked with more negative and limiting attitudes towards women and their roles in relationships.[17]

The Bill already accepts the underlying principle that material promoting hostility towards women or gender equality can cause harm. There is no clear basis for limiting that recognition to children. Doing so overlooks the harm experienced by women, trans and gender-diverse people and leaves providers without an express obligation to address the circulation and amplification of misogynistic material affecting adults. This concern is consistent with the Statutory Review of the *Online Safety Act 2021* which found the regulatory framework's historical focus on children had not adequately accounted for adults' experiences of online harm, particularly women's and gender-diverse people's experiences of TFGBV[18]. It also identified the higher threshold for regulatory intervention in relation to adult cyber-abuse as a barrier for women experiencing serious harm below that threshold.[19]

Sexually explicit material normalising non-fatal strangulation

The adult protection gap also extends to material that normalises serious violence. Clause 25D recognises pornography as harmful to children, but the Bill does not expressly address sexually explicit material that presents strangulation as normal or without risk, whether encountered by children or adults. Non-fatal strangulation is a recognised indicator of escalating risk in intimate partner violence. It can leave little visible evidence while causing acquired brain injury, serious injury or death. Women whose partners have attempted to strangle them are also more than seven times more likely to be killed.[20] Material that normalises strangulation in a sexual context should be understood as a gender-based violence harm. Its omission is difficult to reconcile with clause 25C(1)(c), which expressly recognises material or conduct that encourages, promotes, incites or instructs sexual violence.

Children require strong and age-appropriate safeguards. However, these protections should build on a meaningful baseline for everyone in Australia, rather than creating an artificial boundary that leaves adults exposed to harms the Bill already recognises.

Harms arising from platform features that sustain the male grievance industry

Misogynist content forms part of a much broader commercial industry. In an era where it takes an average of 23 minutes for male-identified accounts to receive misogynist content[21], we draw attention to research that highlights the commercial infrastructure that capitalises on male vulnerability. Rather than using the term 'manosphere', research by *Reset Tech* and *Equimundo* problematise the male grievance industry which is the "*commercial ecosystem of creators, platforms, membership schemes, educational products, supplement funnels, and funding networks that monetise male vulnerability at scale*".[22] The research finds that the male grievance industry targets and exploits boys' and men's need to belong and need for economic security, and how online platforms fuel this industry.[23]

> *Their recommendation algorithms surface this material to young men who were not necessarily looking for it. Their monetization infrastructure provides the revenue that*

funds it. Their inconsistent and retroactive enforcement removes individual posts while leaving the broader commercial ecosystem untouched.[24]

Importantly, the research characterises the male grievance industry as a consumer protection problem: a commercial ecosystem that profits from deceptive and exploitative practices. These include paid advertising, affiliate schemes presented as community and crypto promotions without appropriate financial disclosure. While the Digital Duty of Care can address the role of platform design and business practices in amplifying this industry, Wesnet and WwWA urge the Australian Government to consider complementary regulatory measures targeting its commercial infrastructure. *The Grift Economy* proposes a number of options, including liability where platforms profit from algorithmically amplifying content that causes documented harm, public and machine-readable cross-platform advertising repositories, and disclosure requirements for political funding of influencer content

- **Insert an adult equivalent of subparagraph 25B(1)(b)(ii), so that all persons in Australia are protected from harms associated with the operation of design features.**
- **Move or replicate the section 25D categories within section 25C, subject to an appropriate seriousness threshold, so that adults are protected from misogynistic material and conduct.**
- **Amend clause 25C to include material that promotes or normalises violent practices capable of causing serious injury or death, including strangulation, with alignment to the *Criminal Code Act 1995* where appropriate.**
- **Require providers to assess and mitigate harms arising from recommender or ranking systems that amplify misogynistic material or create pathways towards increasingly harmful content.**
- **Apply consumer protection frameworks to the male grievance industry as a commercial infrastructure.**

8. The definition of harm must be broadened

Currently, the Bill protects Australians from individual incidents of online harm, overlooking harm arising from cumulative incidents, and the effect of online harm on the offline world. Section 25E provides that harm can be caused by material or conduct (or any combination of both), including in instances where a victim of online harm is not the user of the online service. This is a useful provision that should be expanded further and carried throughout the Bill, especially relating to risk assessments.

The Statutory Review of the *Online Safety Act 2021* highlighted concerns that the Bill failed to capture experiences of online abuse involving 'pile-on' or 'volumetric attacks' where numerous people target an individual.[25] As it stands, the Bill also fails to recognise where individual instances that are seemingly harmless, culminate in a severe harm due to repetitive patterns. Paragraph 26A(2)(b) requires a provider to assess the likelihood and potential severity of risks. That is an incident-based test. It captures the single incident and misses the pattern, which is how TFGBV actually operates. A hundred messages, none of which in isolation meet the threshold for harm, will not be considered a risk under the duty.

- **Broaden the definition of harm and the risk-assessment requirements to capture persistent conduct, cumulative effects and volumetric attacks, including conduct occurring across multiple accounts or services.**

9. Protected characteristics must be expressly recognised

Clause 25D(1)(c) expressly recognises material or conduct that encourages or promotes hostile attitudes towards women or gender equality as harmful to children. This inclusion is welcome. However, the Bill does not provide equivalent recognition of other forms of identity-based harm. Clause 25D does not expressly recognise material promoting hostility towards people based on race, ethnicity, religion, age, disability, sexual orientation or gender identity. Clause 25C provides no equivalent protection for adults from hostility based on gender or other protected characteristics. This gap was clearly identified by the Statutory Review of the *Online Safety Act 2021*. The Review found that First Nations people, women, LGBTIQA+ people, culturally and linguistically diverse communities, people with disability, people of particular faiths and older Australians face a heightened risk of online abuse. It identified the failure to address abuse targeting protected characteristics, including intersecting characteristics such as gender and race, as a significant gap in the existing framework.[26] The Review recommended that duty holders consider harms associated with protected characteristics, including sex, gender, sexual orientation, race, ethnicity, disability, age and religion. The exposure draft does not implement that recommendation.

For adults, the Bill's current structure risks overlooking serious abuse directed at people with protected characteristics where the conduct does not meet a criminal threshold, but nevertheless causes significant harm. The Government has indicated that clause 25C is intended to focus on illegal material and conduct, while clause 25D recognises a broader range of harms affecting children. However, identity-based abuse does not always involve an explicit threat or constitute a criminal offence. Sustained racialised abuse, religious vilification, homophobic or transphobic harassment, ableist abuse and age-based abuse targeting older women can all cause serious harm, particularly where the conduct is repeated or coordinated. The Bill must also expressly recognise intersecting harm. Women, trans and gender-diverse people may be targeted because of the interaction between gender and race, religion, age, disability, sexuality or migration background. These harms do not simply add together. Their interaction can change the nature of the abuse and magnify its effects. A framework that assesses each characteristic separately risks missing the full pattern and severity of the harm.

- **Amend clauses 25C and 25D to expressly recognise material or conduct that attacks, dehumanises or promotes hostility towards people based on one or more protected characteristics. Retain express recognition of misogyny and hostility towards women or gender equality.**
- **Amend clause 25D to expressly recognise racial and religious hostility or vilification as harmful to children, including hostility directed towards a child's ethnic, religious or migrant community.**
- **Require providers to consider harm directed at a person by reference to a combination of protected characteristics, rather than assessing each characteristic in isolation.**
- **Broaden the definition of harm and the risk-assessment requirements to capture persistent conduct, cumulative effects and volumetric attacks, including conduct occurring across multiple accounts or services.**

10. Algorithmic harm cannot be solved through user choice alone

The Australian Government has promoted "My Feed, My Way" as a central feature of the Digital Duty of Care, giving people greater control over the content recommended to them. Greater user choice is welcome. Notably, more information about this measure was provided in the Government's press conference than in the exposure draft itself. User empowerment tools occupy only three short subsections of a 76-page Bill, with their application and operation to be determined through a future legislative instrument. WwWA and Wesnet do not object to the detail of user empowerment tools being prescribed through delegated legislation. This approach provides flexibility to respond to emerging harms and changes in technology without requiring primary legislation to be amended each time. Our concern is the weight being placed on user empowerment as the answer to systemic algorithmic harm.

WwWA and Wesnet support giving users greater choice over the content recommended to them. However, an opt-out is unlikely to mitigate the harms the measure is intended to address. It assumes users will recognise harmful recommendation pathways and choose to leave them, even where personalised recommendations are central to the service and opting out may significantly reduce its functionality. Some users may not recognise the pathway, while others may continue engaging with misogynistic material because it validates their grievances or offers a sense of belonging. More fundamentally, an opt-out does not address the systems producing the harm. It does not change what recommender systems are designed to optimise or prevent providers from profiting from harmful engagement.

Women, trans and gender-diverse people bear the consequences of those systems even when they are not the users consuming the material. Women, girls, trans and gender-diverse people cannot opt out of these consequences by changing their own feed settings. Their safety cannot depend on whether someone else recognises a harmful recommendation pathway and chooses to leave it. This exposes the fundamental limitation of "My Feed, My Way". It centres the choices available to the person receiving content, while doing little for the people affected by the attitudes and conduct that content promotes. The harm is gendered, intersecting with various forms of inequality, and is not distributed equally. The Digital Duty of Care must therefore look beyond individual user choice. Providers must be required to assess who bears the consequences of the content their systems recommend and profit from, and to change those systems where they reinforce reasonably foreseeable gender-based harm.

11. Require mandatory baseline algorithmic transparency

Wesnet and WwWA welcome the introduction of transparency reporting to support the eSafety Commissioner to identify systemic risks and obtain the information needed to investigate them. We recommend that the Bill strengthen these provisions by establishing a mandatory baseline reporting obligation for prescribed providers. Providers should be required to submit an initial whole-of-service transparency report when the Digital Duty of Care commences.

The report should provide the eSafety Commissioner with sufficient information to understand how the provider's algorithms operate, what they are designed to optimise, and how commercial incentives influence the content shown to users. It should also explain how the provider identifies and mitigates foreseeable harms, including misogyny, gender-based and discriminatory harms. The report should

require providers to demonstrate how their recommender, ranking and amplification systems interact with the categories of harm recognised in the Bill. This should include seriously harmful material and conduct under clause 25C, material and conduct harmful to children under clause 25D, and harms associated with the operation of design features. This information could be provided confidentially to protect genuinely sensitive technical and commercial information. However, providers should not be able to withhold information necessary for regulatory scrutiny solely because their systems are proprietary.

This baseline obligation would ensure that transparency does not depend on the eSafety Commissioner already knowing where risks exist or which questions to ask. Providers hold the information needed to understand how their systems create and amplify harm. They should be required to disclose that information as a condition of operating prescribed recommender systems in Australia. The Bill cannot meaningfully require providers to prevent specified harms without requiring them to show the regulator how their systems may amplify those very harms.

- **Require prescribed providers to give the eSafety Commissioner an initial whole-of-service transparency report at the commencement of the Digital Duty of Care and before introducing a prescribed recommender system in Australia.**
- **Amend paragraph 26(3)(a) so that appropriate management of design features is defined by reference to not recommending or amplifying seriously harmful material, with user empowerment tools additional to that obligation rather than illustrative of it.**
- **Require transparency reports to explain how recommender and ranking systems operate, what they are designed to optimise and how providers identify and mitigate gendered or discriminatory harm.**

12. Enforcement should not solely rely on the capacity of eSafety

The duty of care created under section 26 is enforced exclusively by the eSafety Commissioner. This is unlike other regulators who operate alongside complementary enforcement bodies. At establishment, the eSafety Commissioner operated alongside ACMA when the role was limited to protecting children under the Online Content Scheme. While the Digital Platform Regulators Forum, including the eSafety Commissioner, the ACCC, the ACMA, and the OAIC coordinate on cross-cutting issues involving the regulation of online services, they ultimately operate under different legislative frameworks with different policy objectives, and different Ministers.

Online safety is a highly complex regulatory environment where enforcement is shared but is not formally coordinated. For example, while eSafety is responsible for image-based abuse, criminal law is responsible for cyberstalking, doxing and threats, and civil law for reputational damage.[27] Victims of online harms may engage with multiple agencies and be required to reshare traumatic details of incidents each time they lodge, or attempt to lodge, a complaint.[28] The 2021 Review recounts *"understanding these legislative frameworks and where the policy responsibility of one Minister ends, and another begins, has been challenging, particularly as the digital landscape continues to evolve…This limits the ability of Government to respond dynamically and nimbly to emerging harms and risks."*

As has been highlighted in the Statutory Review of the *Online Safety Act 2021*, the functions and powers of the eSafety Commissioner have increased alongside a rapidly evolving operational environment since the establishment of the role in 2015[29]. Concerns that governance arrangements are now inadequate given the present scale of the eSafety Commissioner's remit were raised in the 2018 Statutory Review, where a standalone online safety entity was first suggested. Similarly, the Joint Select Committee on Social Media and Australian Society has called for a Digital Affairs Ministry with overarching responsibility for the coordination of regulation.[30]

The consequences of a single enforcement body are already visible: Of the 108,000 complaints eSafety received in the year to 30 June 2026, approximately two percent resulted in a removal notice, and only one prosecution brought by eSafety resulted in a fine of $650,000 against X.[31] eSafety is a risk-based regulator and triages accordingly. Not all harms can be meaningfully addressed through eSafety alone, leaving victims of online harm without access to remedy.

The Bill promises more than this: Paragraph 3(c) outlines the object of providing a complaints scheme is to remove and remediate illegal or seriously harmful material. There is no provision in the Bill which provides remediation for victims of online harm. People who bear these harms - predominantly women and gender-diverse people – can have harmful material removed under Schedule 1 of the Bill, but have no access to further remediation, including through a private right of action, compensation, or even involvement in the investigation process and notification of outcome.

A right to civil remedy

Enforcement schemes must be designed with remediation options for victims of online harm. The Bill focuses on online service providers' duty of care without actually creating a remedial pathway for victims of online harms resulting from breaches of the duty. Under the Bill, victims of online harms resulting from breaches of the Digital Duty of Care, cannot take legal action to enforce the duty.

This is unlike other enforcement environments, where, for example – if a business breaches its duty of care to maintain a safe workplace, it can be prosecuted by a regulator, and fined or sued for compensation by employees who are harmed. This is an especially significant oversight given eSafety's limited operational capacity relative to the growing influx of complaints received. Regulators have limited resources and can only investigate and prosecute a small percentage of complaints. eSafety cannot effectively police all online safety.

The scale and severity of online harms due to breaches of the proposed duty is well recorded by specialist domestic, family and sexual violence services. As stated, Wesnet's survey of frontline services found that 99.3% of practitioners are observing TFGBV in cases they support.[32] The Australian National Research Organisation for Women's Safety highlights that technology-facilitated abuse is a gendered issue and that women face barriers to help-seeking including TFGBV not being taken seriously by police and courts, and inadequate responses from online service providers.[33] Wesnet's survey found that only 4.7% of practitioners reported that police always take technology-facilitated abuse seriously.[34]

WwWA and Wesnet echo the Australia Institute's open letter to the Prime Minister, which calls for victims of online harm to have a legislated right to pursue a civil claim, including injunctions and compensation.

- **Provide a direct right of action for a person harmed by a provider's failure to uphold its Digital Duty of Care.**
- **Develop a whole-of-government, no-wrong-door approach to online harm, supported by formal coordination and information sharing across relevant regulators.**

13. Code of Practice to address GBV

Clause 26E states that the Commissioner may publish Digital Duty of Care guidelines. Wesnet submits this can be strengthened by the development of a Code of Practice to improve online safety for women, gender-diverse people, and children. The United Kingdom *Online Safety Act 2023* mandates the publication of guidance for service providers to improve online safety for girls and women, and that the regulator should consult with the Domestic Abuse Commissioner.[35i]We note that the specialist family violence sector in the United Kingdom advocated for a violence against women and girls-specific Code of Practice,[36] as guidance has less legal standing.

While there is existing Industry guidance on safety by design in Australia[37], developing a specific Code of Practice to address gender-based violence should be prioritised.

- **Amend Clause 26E to state that 'The Commissioner must prepare and issue a code of practice for online services to address gender-based violence. The code must contain advice and examples of minimum steps and good practice for assessing risks of harm to women, gender-diverse people, and children from seriously harmful material and conduct. Before producing the guidance (including revised or replacement guidance), the Commissioner must consult the Domestic, Family and Sexual Violence Commissioner, specialist domestic, family and sexual violence services and survivor advocates'.**

Appendix: Proposed amendments to the exposure draft

#	Issue identified	Suggested Amendment
Coverage		
All	The Bill inconsistently refers to "Australians", "persons in Australia", "users in Australia", "Australian user accounts", "Australian children" and "Australian adults".	Harmonise and define the terminology. Ensure the duty applies where harm occurs in Australia, affects a person in Australia or otherwise has a substantial connection with Australia, regardless of whether the person is an Australian citizen, holds an account or directly uses the service. Protections should apply to every person in Australia, including migrants, refugees, temporary visa holders and permanent residents, and where transnational conduct causes harm to a person in Australia.
All	The Bill variously refers to the "safety of the online service for Australians", "online safety of its users in Australia", risks to "users of the services in Australia", "Australian user accounts" and active "end-users".	Harmonise terminology throughout the transparency provisions and align it with the people protected by the substantive duty.
Seriously harmful material and conduct (25C)		
25C(1)	Clause 25C does not expressly capture serious identity-based material or conduct affecting adults, despite its broader focus on illegal material and conduct closely connected to criminal offending. This leaves an inconsistency between the Bill's recognition of other serious or unlawful harms and its treatment of serious hostility or violence directed at people because of a protected characteristic.	Insert an additional category in subsection 25C(1) covering: *material or conduct that constitutes, encourages, promotes or incites an offence under Division 80 of the Criminal Code Act 1995 involving force, violence or harm directed at a person or group because of a protected characteristic.*
25C (c)	The express inclusion of material or conduct that encourages, promotes, incites or instructs sexual violence is welcome. However, sexual violence is one form of gender-based violence. The Bill does not explain why this form is expressly recognised while other forms of gender-based violence are left implicit. This creates a distinction between forms of gender-based violence and risks excluding harmful material or conduct that does not relate specifically to sexual violence.	Retain the express reference to sexual violence and broaden clause 25C(1)(c) to recognise gender-based violence as the overarching category of harm. ***(c)** material or conduct that encourages, promotes, incites or instructs gender-based violence, including sexual violence;*
		Insert a definition based on the *National Higher Education Code to Prevent and Respond to Gender-based Violence*: ***gender-based violence** means any form of physical or non-physical violence, harassment, abuse or threats, based on gender, that results in, or is likely to result in, harm, coercion, control, fear or deprivation of liberty or autonomy.*
Harmful to children (25D)		

25D	Clause 25D identifies categories of material and conduct that are harmful to children but does not require the provision to be interpreted or applied in accordance with the best interests of the child. The best interests of the child is a fundamental principle of international and Australian law and should be expressly reflected in the Bill. Without this principle, providers may approach their obligations through a narrow content or compliance lens rather than considering the broader effects of their services on children's safety.	Insert the best interests principle into a new subsection: *In interpreting and applying this section, including when identifying, assessing and mitigating risks of harm to children, the best interests of the child must be a primary consideration.*
	The provision appropriately recognises hostility towards women or gender equality as harmful to children but does not address harmful material targeting children or communities on the basis of other protected characteristics. Misogyny intersects with racism, ableism, homophobia, transphobia and other forms of identity-based hostility.	Retain express recognition of misogyny and hostility towards women or gender equality. Introduce an additional clause 25D(1)(c) to include material or conduct that promotes hostility, discrimination, dehumanisation or unequal treatment based on a protected characteristic.
	Clause 25D does not expressly recognise racial or religious hostility as harmful to children. Its general reference to abuse, harassment and bullying may not adequately capture content that normalises hostility towards a child's ethnic, religious or migrant community, including repeated mockery of accents, religious dress or cultural practices. Conduct that may appear minor when viewed as a single incident can cause significant harm when it is persistent, targeted or experienced alongside other forms of discrimination.	Amend clause 25D to expressly recognise material or conduct that encourages or promotes racial or religious hostility, vilification or dehumanisation as harmful to children, including where harm arises through persistent conduct, repeated exposure or the interaction of multiple protected characteristics.
25D(1)(f)	The reference to a "combination" does not clearly capture recommendation pathways, repeated exposure or cumulative harm. The phrase "could inflict serious harm" also differs from the "may cause harm" threshold in subsection (2).	Expressly include combinations or patterns of material and conduct, repeated exposure, and cumulative or compounding effects. Adopt a consistent "causes or is reasonably likely to cause harm" threshold. *(i) that causes, or is reasonably likely to cause, harm, including through repeated exposure or cumulative or compounding effects over time;*
Harm (25E)		
25E	Clause 25E does not substantively define harm. It identifies only that harm may be caused by material, conduct or a combination of both. It does not identify the forms harm may take or expressly recognise direct, indirect, cumulative, compounding or cross-platform harm.	Insert a substantive definition of harm. Clarify that harm may be direct or indirect, immediate or cumulative, and may arise from a single incident or through repeated exposure, patterns of conduct, volumetric attacks or conduct across multiple accounts or services.

25E	The clause does not recognise that service design, features, systems or processes may cause, facilitate, amplify or compound harm. This is inconsistent with clause 26A, which requires providers to assess risks arising from these matters.	Clarify that harm may be caused, facilitated, amplified or compounded by material, conduct, design features, systems or processes, including through their reasonably foreseeable use or misuse.
	The "reasonably practicable" test does not expressly require consideration of cumulative harm or harmful patterns.	Require duty holders to consider repeated exposure, recurring patterns, volumetric attacks and cumulative or compounding effects, together with the service's contribution to the risk through its design and systems.
Guidelines		
26E	Clause 26E provides that the Commissioner may publish guidelines to assist online services to meet the Digital Duty of Care. It does not require guidance on how the duty applies to gender-based violence, despite the need for services to recognise and address these harms as foreseeable systemic risks.	Amend Clause 26E to state: *'The Commissioner must prepare and issue a code of practice for online services to address gender-based violence. The code must contain advice and examples of minimum steps and good practice for assessing risks of harm to women, gender-diverse people, and children from seriously harmful material and conduct. Before producing the guidance (including revised or replacement guidance), the Commissioner must consult the Domestic, Family and Sexual Violence Commissioner, specialist domestic, family and sexual violence services and survivor advocates.*
Risk assessment and Transparency reports		
26A	Clause 26A requires providers to identify reasonably foreseeable risks arising through their services but does not expressly require them to assess gender-based violence or technology-facilitated abuse. A provider could complete a risk assessment without considering gendered harm as a systemic risk.	Amend paragraph 26A(2)(a) to require a risk assessment to identify and assess actual or reasonably foreseeable risks of gender-based violence, including technology-facilitated gender-based violence, occurring through the service.
		Amend subparagraph 26A(2)(a)(iii) to require providers to assess: *how any functionality of the service may foreseeably be used by one person to harm another.*
26A(2)(a)	The Bill does not expressly require providers to assess harms caused when their moderation or recommender systems suppress lawful public-interest information.	Amend paragraph 26A(2)(a) to require providers to assess harms arising from systems that remove, restrict or deprioritise lawful public-interest material. Require providers to distinguish material that perpetrates or promotes gender-based violence from material shared for prevention, education, journalism, advocacy or support.
	The transparency provisions do not require reporting about the operation of recommender and ranking systems or how those systems amplify harm.	Amend subsections 192D(1) and 192M(2) to expressly require information about: • recommender and ranking systems • amplification and reach

		• the objectives those systems optimise for • the effectiveness of mitigation measures
	Providers should hold baseline information about how their systems operate and provide that to the eSafety Commissioner.	Require prescribed providers to submit an initial whole-of-service transparency report at commencement and before introducing a prescribed recommender system in Australia. The report should explain how recommender systems operate and how they interact with the harms recognised in clauses 25C and 25D. Require updated reporting following material changes.
Image-based abuse		
77 - 79	The Bill introduces a pathway for responding to reposted or altered cyberbullying and adult cyber-abuse material, but does not extend it to intimate images. Victim-survivors may therefore need to make a fresh complaint or objection notice each time an image is copied, altered or redistributed.	Apply the reposted-material pathway in new subsections 65(2C) to (2E) to Part 6, allowing the Commissioner to issue a further removal notice under sections 77, 78 or 79 without a fresh complaint under section 32 or objection notice under section 33.
25C	Clause 25C does not expressly recognise non-consensual intimate images, including synthetic or technologically altered images, or threats to distribute them, as seriously harmful material or conduct.	Insert an additional category in subsection 25C(1) covering: *an intimate image of a person provided, or threatened to be provided, without the person's consent, including an image created or altered by artificial intelligence or other technological means.*
86B	Proposed section 86B applies to services designed for, or predominantly used for, generating fake nude material, but not services dedicated to facilitating the non-consensual sharing of intimate images.	Extend section 86B to apps and websites designed for, or predominantly used to facilitate, the non-consensual sharing of intimate images.

[1] Wesnet et al., (2026) Third National Survey of Technology Abuse and Domestic Violence in Australia (Wesnet), https://wesnet.org.au/3rdnatsurvey
[2] Ibid.
[3] European Union, (2022), *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) (Text with EEA relevance)*, https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.
[4] European Board for Digital Services and the European Commission, (2026), *Second report on systemic risks on very large online platforms and search engines under the Digital Services Act,* https://digital-strategy.ec.europa.eu/en/policies/dsa-board.
[5] Jóźwiak, M., & Ohnesorge, J, (2026), *Platform Governance and Technology-Facilitated Gender-Based Violence: Positioning the DSA in the EU's Legal Framework*, https://dsa-observatory.eu/2026/07/13/platform-governance-and-technology-facilitated-gender-based-violence-positioning-the-dsa-in-the-eus-legal-framework/.
[6] Collins, C., Parker, C., Paterson, J.M., Weatherall, K., Carah, N., Burgess, J & Angus, D. (2026) *Digital Duty of Care Policy Brief. (ARC Centre of Excellence for Automated Decision-Making and Society),* https://apo.org.au/node/334632, p. 9.
[7] Toivonen, & Backhouse (2018). National Risk Assessment Principles for domestic and family violence, p.13.
[8] Ibid.
[9] Collins, C., Parker, C., Paterson, J.M., Weatherall, K., Carah, N., Burgess, J & Angus, D. (2026) Digital Duty of Care Policy Brief, p.9.
[10] The final text of the Digital Services Act (DSA) https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html

[11] Collins, C., Parker, C., Paterson, J.M., Weatherall, K., Carah, N., Burgess, J & Angus, D. (2026) Digital Duty of Care Policy Brief, pp.11-12.
[12] Ibid.
[13] Pfitzner, N., McCook, S., Phelan, A., Wescott, S., Roberts, S. & Scott, B, (2026), *An Introductory Guide to the Manosphere and the Impacts for Young People, Teachers and Schools* (ANROWS Insights 01/2026). ANROWS, p.10. https://doi.org/10.71940/1h2k-x058.
[14] Pfitzner, N., et al, (2026), *An Introductory Guide to the Manosphere and the Impacts for Young People, Teachers and Schools,* https://research.monash.edu/en/publications/an-introductory-guide-to-the-manosphere-and-the-impacts-for-young/ ; Wescott, S. & Roberts, S. (2025), *From violence to sexism, the manosphere is doing real-world harm*, The Conversation, https://theconversation.com/from-violence-to-sexism-the-manosphere-is-doing-real-world-harm-262205.
[15] P Pfitzner, N., et al, (2026), *An Introductory Guide to the Manosphere and the Impacts for Young People, Teachers and Schools,* https://research.monash.edu/en/publications/an-introductory-guide-to-the-manosphere-and-the-impacts-for-young/
[16] Parliament of Victoria, (2026), *Inquiry into anti-LGBTIQA+ hate crimes in Victoria,* https://www.parliament.vic.gov.au/antilgbtqiahatecrimes; Kolovos, B., (2026), *Role of far-right manosphere in homophobic attacks on men to be investigated in Victoria*, The Guardian, https://www.theguardian.com/australia-news/2026/feb/18/far-right-influencers-homophobic-attacks-dating-apps-investigation-ntwnfb;
Kolovos, B., (2026), *Gay students extorted with threat of being 'outed' in home countries, Victorian hate crime inquiry hears*, The Guardian, https://www.theguardian.com/australia-news/2026/jun/24/gay-international-students-extorted-threat-of-being-outed-victoria-hate-inquiry-ntwnfb.
[17] Fisher, K., Rice, S., & Seidler, Z., (2025), *Young men's health in a digital world,* Melbourne: Movember Institute of Men's Health, https://au.movember.com/movember-institute/masculinities-report.
[18] Delia Rickard, (2024), *Report of the Statutory Review of the Online Safety Act 2021,* https://www.infrastructure.gov.au/department/media/publications/report-statutory-review-online-safety-act-2021
[19] Ibid.
[20] Glass, N., et al, (2009), *Non-fatal strangulation is an important risk factor for homicide of women*, Journal of Emergency Medicine, https://pmc.ncbi.nlm.nih.gov/articles/PMC2573025/
[21] Baker, C., Ging, D., & Andreasen, M.B. (2024) *The role of algorithmic recommender functions on YouTube Shorts and TikTok in promoting male supremacist influencers* (Dublin: Dublin City University Anti-Bullying Centre), https://www.dcu.ie/antibullyingcentre/recommending-toxicity.
[22] Reset Tech and Equimundo, (2026), *The Grift Economy: How Young Men Are Being Sold Fake Belonging and Fake Wealth Online,* (p. 10), https://www.equimundo.org/resources/the-grift-economy/
[23] Ibid, (p. 6)
[24] Ibid, (p. 6)
[25] Delia Rickard, (2024),*Report of the Statutory Review of the Online Safety Act 2021,* https://www.infrastructure.gov.au/department/media/publications/report-statutory-review-online-safety-act-2021
[26] Ibid.
[27] Delia Rickard, (2024), *Report of the Statutory Review of the Online Safety Act 2021,* https://www.infrastructure.gov.au/department/media/publications/report-statutory-review-online-safety-act-2021
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] eSafety Commissioner, (2026), *Legal proceedings involving eSafety*, https://www.esafety.gov.au/industry/legal-proceedings-involving-esafety
[32] Wesnet, (2026), *Submission to the Second Action Plan under the National Plan to End Violence against Women and Children 2022–2032* (2026), https://wesnet.org.au/wp-content/uploads/2026/08/Wesnet-2AP-Submission-final.pdf
[33] Flynn, A., Powell, A., & Hindes, S., (2021),*Technology-facilitated abuse: A survey of support services stakeholders,* Australian National Research Organisation for Women's Safety (ANROWS), https://www.anrows.org.au/publication/technology-facilitated-abuse-a-survey-of-support-services-stakeholders/
[34] Wesnet et al., (2026) Third National Survey of Technology Abuse and Domestic Violence in Australia (Wesnet), https://wesnet.org.au/3rdnatsurvey.
[35] Ofcom. (2025) *Statement and Guidance: A safer life online for women and girls* (London: Ofcom), https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/a-safer-life-online-for-women-and-girls.
[36]Domestic Abuse Commissioner, We must build on the Online Safety Act to ensure all victims are protected from online abuse published on December 19, 2023.
[37] eSafety Commissioner (2024) *Technology, gendered violence and Safety by Design* (eSafety Commissioner), https://www.esafety.gov.au/sites/default/files/2024-09/SafetyByDesign-technology-facilitated-gender-based-violence-industry-guide.pdf?v=1786603903734.