Working with Women Alliance

Supporting a gender-responsive Digital Duty of Care

Submission to the Senate inquiry into the Online Safety Amendment (Digital Duty of Care) Bill 2026

October 2026

safety.policy@wwwa.org.au

Working with Women Alliance

Acknowledgment of Country

The Working with Women Alliance acknowledges the Traditional Custodians of the land on which we work and live.

We pay our respects to Aboriginal and Torres Strait Islander Elders past and present, and we value the enduring connection Aboriginal and Torres Strait Islander people have to this land. We value Aboriginal and Torres Strait Islander histories, cultures, and knowledge.

About WwWA

The Working with Women Alliance (WwWA) brings together a diversity of voices, expertise, and lived experience to inform and guide national policy on women's equality, leadership, and safety. We are 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.

WwWA represents more than 800 organisation and individual members across two key portfolios: gender-based violence and gender equality. WwWA connects the critical areas of gender-based violence and the advancement of women's economic equality and leadership, bridging these important policy fields for greater impact.

We work with members and stakeholders, including the Australian Government, to provide expertise and advice on gender equality and women's safety.

Contact
Executive Director: Dr Gemma Killen
Senior Policy Officer: Darcie Newland
safety.policy@wwwa.org.au

Endorsements

Women With Disabilities Australia (WWDA)

Gender Justice Australia

GOGO Foundation

With You We Can

Women's Legal Services Australia

CWES Centre for Women's Economic Safety

YWCA Australia

G+V GENVIC

GENDER EQUITY VICTORIA

Older Women's Network NSW (OWN)

Full Stop Australia

Why a preventative Digital Duty of Care is essential

As stated in our previous submission, WwWA wholeheartedly supports the introduction of an overarching Digital Duty of Care. The Bill gives effect to the central recommendation of the Statutory Review of the *Online Safety Act 2021*, led by Delia Rickard PSM, that online service providers should be required to take reasonable steps to prevent foreseeable harm. This is an essential shift away from a framework that relies primarily on individuals to protect themselves or seek action after harm has occurred.

WwWA's interest in the Bill is grounded in our connected work on gender-based violence and gender equality. This work recognises that safety is shaped by the systems and settings in which people live. Online platforms are increasingly part of this tapestry, and can decide whether they build in safety for their users, or to facilitate harm.

To date, online service providers have failed to take sufficient responsibility for preventing that harm. Wesnet's *Third National Survey of Technology Abuse and Domestic Violence in Australia*, drawing on the experiences of frontline practitioners, found that:

- 94.1% of practitioners saw social media and online platforms used to facilitate abuse often or all the time, up from 48.6 per cent in 2020.
- Provider responses focused on individual incidents do not reflect how technology-facilitated abuse operates. Perpetrators combine conduct across technologies as part of a broader pattern of coercive control.
- Victim-survivors continue to carry the burden of adapting to unsafe digital environments, including by changing accounts because of ongoing concerns about monitoring.[1]

Public reporting repeatedly shows online service providers have failed to take sufficient responsibility for preventing that harm:

- When X (formerly Twitter) integrated its generative AI, Grok, 3 million sexualised images were created within 10 days. Of those, 23,000 pictures depicted children.[2]
- In January 2025, Meta weakened content moderation protections relating to gender and immigration, while acknowledging that more harmful content would remain on its platforms. In a subsequent survey of nearly 7,000 users from protected groups, 72 per cent reported an increase in harmful content targeting those groups.[3]
- Snapchat is currently facing a US lawsuit after its platform enabled a 25-year-old man to groom, locate, and sexually assault a 12-year-old girl. The platform:
    - Failed to prevent an 11-yr-old from creating an account despite a minimum age limit
    - Automatically recommended and promoted the child's profile to the adult man
    - Allowed the adult man to use a cartoon avatar that completely disguised his age and identity
    - Shared the child's real-time location through 'Snap Maps' allowing the man to track down her home address
    - Allowed him to use disappearing message features and "My Eyes Only" features to erase the messages and share sexually explicit material with a child

- Failed to review critical serious user reports before the data vanished from the platform entirely.[4]

Online service providers have repeatedly pushed responsibility for safety back onto users. Users are told to change their settings or limit how they participate online. When harm occurs, they are expected to report each incident through systems that often treat it in isolation. This allows providers to draw narrow lines around where their responsibility starts and ends. Victim-survivors are responsible for making the abuse stop, while the systems enabling it remain intact.

The Digital Duty of Care represents a crucial shift towards requiring providers to build safety into their services, rather than expecting individuals to manage the consequences when those services enable harm. This reflects a central tenet of WwWA's advocacy: individualised responses shift responsibility onto victim-survivors to manage risk and navigate systems after harm has occurred, while leaving the settings that enabled that harm largely intact.

The introduced Bill provides a stronger gender-responsive foundation

Against this backdrop, the changes made since the exposure draft are significant. Gender-based violence is now expressly included within the definition of "seriously harmful material or conduct." The Bill also adopts the broad definition from the *National Higher Education Code to Prevent and Respond to Gender-based Violence*, which recognises physical and non-physical violence, harassment and abuse based on gender. This gives the Digital Duty of Care a much stronger foundation for addressing the ways gender-based violence occurs online. The Bill also brings image-based abuse within providers' preventative obligations. Non-consensual fake nude material is expressly recognised as seriously harmful, as is posting or threatening to post an intimate image without consent. These reforms recognise that providers have a responsibility to prevent their services from facilitating this harm, rather than responding only after a victim-survivor reports an individual piece of material.

WwWA is grateful that the concerns raised by gender-based violence organisations and other sector experts have been reflected in the introduced Bill. The result is a substantially stronger and more gender-responsive framework. The recommendations below build on this foundation by addressing the remaining gaps that could limit the Duty's operation in practice.

Related sector submissions

WwWA supports and refers the Committee to the submissions of Wesnet, Gender Justice Australia, With You We Can and Equality Australia. These submissions provide important further analysis of the Bill from across the gender-based violence sector. WwWA encourages the Committee to consider their recommendations alongside those set out in this submission.

Recommendations summary

Recommendation 1: Require risk assessments to assess gender-based violence

Recommendation 1.1: Amend section 27 to expressly require providers to identify and assess actual or reasonably foreseeable risks of gender-based violence, including technology-facilitated gender-based violence, occurring through or facilitated by their services.
Recommendation 1.2: Amend section 25D to expressly recognise gender-based violence, including technology-facilitated gender-based violence, perpetrated through or facilitated by an online service.

Recommendation 2: Establish a direct right of action

Recommendation 2.1: Establish a direct statutory right of action allowing a person who suffers harm because of a provider's breach of the Digital Duty of Care to seek compensation, an injunction or another appropriate remedy.
Recommendation 2.2: If Parliament does not establish a direct right of action, it must provide an independent statutory pathway for individuals to raise alleged breaches of the Digital Duty of Care. This should be through: a) a complaints pathway to eSafety, with procedural rights for the complainant; or b) an industry-funded Digital Ombuds scheme with authority to resolve individual disputes and issue binding directions.

Recommendation 3: Recognise cumulative and volumetric harm

Recommendation 3.1: Expand the definition of harm to recognise cumulative harm arising from repeated exposure or a pattern of material or conduct, including conduct occurring across multiple accounts or services.
Recommendation 3.2: Amend section 27 to require providers to identify and assess reasonably foreseeable risks arising from repeated or coordinated conduct, including conduct occurring across multiple accounts or services.

Recommendation 4: Address identity-based and intersecting harms

Recommendation 4.1: Amend section 25D to recognise material or conduct that encourages, promotes or incites serious hostility towards a person or group on the basis of one or more protected characteristics, where the material or conduct is reasonably likely to cause serious harm.
Recommendation 4.2: Amend section 25E to recognise material or conduct that encourages or promotes hostile attitudes towards persons or communities on the basis of one or more protected characteristics.
Recommendation 4.3: Define "protected characteristic" consistently with Commonwealth anti-discrimination law. Clarify that material or conduct may be based on one or more protected characteristics, including the interaction between those characteristics.

Recommendation 5: Strengthen the fake nude service removal power

Recommendation 5: Amend section 86B so that either predominant design or predominant use is sufficient to enliven the removal power, and extend the provision to services substantially or regularly used to generate non-consensual fake nude material.

Recommendation 1: Require risk assessments to assess gender-based violence

As outlined above, WwWA strongly welcomes the inclusion of gender-based violence in section 25D as a category of seriously harmful material or conduct. We also welcome the Bill's broad definition of gender-based violence, which encompasses physical and non-physical violence, including harassment and abuse based on gender. These are significant reforms that must be preserved. However, the significance of recognising gender-based violence as a statutory harm will ultimately depend on whether providers assess how their services create or increase the risk of that harm.

Section 27 requires providers to identify "reasonably foreseeable risks", along with the material or conduct that gives rise to them. It also requires providers to consider relevant service features and other systems or processes. It does not expressly require providers to assess the risks arising from the statutory harms identified in sections 25D and 25E. In particular, section 27 does not require providers to examine gender-based violence as a systemic risk.

This leaves a clear gap between recognition in the bill, and prevention of gender-based violence in practice. A provider could complete a formally compliant risk assessment without examining whether its service facilitates technology-facilitated gender-based violence. It could also fail to consider whether its systems amplify material promoting hostility towards women or gender equality, despite the Bill expressly recognising that material as harmful to children. Without a clear link between section 27 and the harms recognised elsewhere in the Bill, a provider could define the scope of its assessment narrowly and address only the risks it chooses to identify.

This creates space for selective compliance. Naming gender-based violence will have limited practical effect if providers are not required to examine how their services create or increase that risk. Section 27 must therefore expressly require providers to assess gender-based violence, including technology-facilitated gender-based violence, and identify the measures needed to address it.

Section 25D also recognises material or conduct that encourages, promotes, incites or instructs gender-based violence. However, it does not clearly capture gender-based violence perpetrated through a service where the conduct does not promote violence to others. This distinction matters in the context of technology-facilitated abuse, where ordinary functionality may be used to stalk or control a victim-survivor.

Recommendation 1.1: Amend section 27 to expressly require providers to identify and assess actual or reasonably foreseeable risks of gender-based violence, including technology-facilitated gender-based violence, occurring through or facilitated by their services.

Recommendation 1.2: Amend section 25D to expressly recognise gender-based violence, including technology-facilitated gender-based violence, perpetrated through or facilitated by an online service.

Recommendation 2: Establish a direct right of action

WwWA supports the campaign led by Josh Bornstein and the Australia Institute for a direct right of action. A Digital Duty of Care should be enforceable by the people it is intended to protect. A Duty that only the regulator can enforce does not give the person harmed a right to redress.

The eSafety Commissioner is a world-leading regulator with a broad and expanding remit. eSafety must make decisions about where its intervention will have the greatest public impact. This requires a risk-based approach and the careful prioritisation of finite regulatory resources. In the year to 30 June 2026, eSafety received 108,000 complaints. Just 2% of complaints result in a notice to a tech business to remove unlawful content. Of a handful of cases prosecuted by eSafety, one has resulted in a fine of $650,000 against X.[5] This is not a criticism of eSafety. Prioritising matters according to their seriousness and potential systemic impact is sound regulatory practice. Further resourcing for eSafety would strengthen its capacity, but no level of resourcing could make it an individual remedy for every person harmed by a provider's breach.

This leaves a clear accountability where a person may experience serious harm because a provider failed to meet its Duty, yet have no independent pathway to enforce that Duty or seek redress. For victim-survivors, the result may be that a provider's failure is legally enforceable in theory but not enforceable by the person who bears its consequences. A direct right of action would fill this gap. It would allow a person harmed by a provider's breach to seek compensation or an injunction without depending entirely on regulatory intervention.

A direct right of action would also distribute enforcement beyond government. It would allow individuals to pursue providers through established legal processes while eSafety remains focused on regulatory priorities. This is particularly important in a context where online safety regulators face sustained resistance and public attacks simply for exercising their statutory functions. Australia's eSafety Commissioner has faced litigation from major technology companies and significant personal targeting in connection with regulatory action. Distributed enforcement is already a common feature of Australian regulatory frameworks ASIC and the ACCC operate in tandem. The Fair Work Ombudsman operates alongside workers and unions with independent enforcement rights. Work health and safety regulation also sits alongside compensation claims brought by people harmed by unsafe workplaces. These pathways serve different purposes. Public enforcement protects the broader community, while private action gives the person harmed a direct route to redress. There is no reason for online safety to operate differently.

For victim-survivors, a provider's breach is not an abstract regulatory failure. It can allow abuse to continue while leaving the person harmed to carry the work of trying to make it stop. A Duty intended to protect victim-survivors should not leave them without the power to enforce it.

WwWA's strong preference is for a direct right of action. If Parliament does not establish that right, the Bill must at least provide an independent statutory pathway for individuals to raise alleged breaches of the Digital Duty of Care. This could be achieved through a complaints pathway to eSafety, with procedural rights for the complainant, or through an industry-funded Digital Ombuds scheme empowered to resolve individual disputes.

Recommendation 2.1: Amend the Bill to establish a direct statutory right of action allowing a person who suffers harm because of a provider's breach of the Digital Duty of Care to seek compensation, an injunction or another appropriate remedy.

Recommendation 2.2: If Parliament does not establish a direct right of action, it must provide an independent statutory pathway for individuals to raise alleged breaches of the Digital Duty of Care. This should be through:
a) a complaints pathway to eSafety, with procedural rights for the complainant; or
b) an industry-funded Digital Ombuds scheme with authority to resolve individual disputes and issue binding directions.

Recommendation 3: Recognise cumulative and volumetric harm

Technology-facilitated gender-based violence rarely occurs as a single, self-contained incident. Perpetrators may use repeated messages or multiple accounts as part of a broader pattern of coercive control. Each incident may appear minor when viewed alone, while the pattern as a whole causes serious harm.

The Bill recognises that harm may arise from material or conduct, including a combination of both. However, it does not expressly recognise the cumulative effect of conduct over time. Nor does section 27 clearly require providers to assess volumetric abuse, where many accounts direct harmful conduct towards the same person. This creates a risk that providers will assess individual incidents separately and overlook the harm produced by the pattern. A provider may conclude that no single message or post reaches the relevant threshold, even where the combined conduct has made a victim-survivor feel constantly monitored or unable to participate safely online. Incident-by-incident assessment also fails to reflect how abuse operates across services. A perpetrator may continue the same pattern through a new account or move between accounts and platforms after being blocked. The harm does not restart each time the technology changes.

The Bill must therefore recognise that individually sub-threshold conduct may collectively cause serious harm. Providers should be required to identify patterns of repeated or coordinated conduct and assess the risk created by those patterns.

Recommendation 3.1: Expand the definition of harm to recognise cumulative harm arising from repeated exposure or a pattern of material or conduct, including conduct occurring across multiple accounts or services.

Recommendation 3.2: Amend section 27 to require providers to identify and assess reasonably foreseeable risks arising from repeated or coordinated conduct, including conduct occurring across multiple accounts or services as part of the risk assessment.

Recommendation 4: Build on the recognition of gender-based violence by addressing identity-based and intersecting harms

The Bill's recognition of gender-based violence provides a strong foundation for addressing online harms shaped by gender inequality. However, it does not provide equivalent recognition of harms based on other protected characteristics.

For adults, section 25D may capture some identity-based abuse through the provisions concerning serious menacing or harassment. However, these provisions focus on conduct directed at an individual and may not capture material that promotes serious hostility towards a broader group. This leaves uncertainty around sustained racialised abuse or religious vilification. It may also leave gaps for ageist, homophobic, transphobic or ableist hostility where the conduct does not clearly fall within another statutory category.

There is a related gap in section 25E. The Bill recognises material or conduct that encourages or promotes hostile attitudes towards women or gender equality as harmful to children. However, it does not provide equivalent recognition of hostility based on race, religion or disability. Nor does it clearly recognise hostility based on sexual orientation or gender identity. Children may be harmed by material targeting a community to which they belong, even where the material is not directed at them personally.

The Bill should also recognise that identity-based harms may be shaped by more than one protected characteristic. Gendered abuse may also be racialised. Abuse targeting a person with disability may take a different form because of gender. Treating each characteristic separately can obscure the nature of the conduct and its impact.

These amendments would sit alongside the gender-based violence provision. They would not displace its specific recognition of violence and abuse based on gender. Rather, they would provide clearer coverage where identity-based hostility does not fall within that definition or another existing harm category. The adult and child provisions should be amended separately to preserve the different thresholds already established by the Bill.

Recommendation 4.1: Amend section 25D to recognise material or conduct that encourages, promotes or incites serious hostility towards a person or group on the basis of one or more protected characteristics, where the material or conduct is reasonably likely to cause serious harm.

Recommendation 4.2: Amend section 25E to recognise material or conduct that encourages or promotes hostile attitudes towards persons or communities on the basis of one or more protected characteristics.

Recommendation 4.3: Define "protected characteristic" consistently with Commonwealth anti-discrimination law. Clarify that material or conduct may be based on one or more protected characteristics, including the interaction between those characteristics.

Recommendation 5: Strengthen the fake nude service removal power

WwWA welcomes the targeted power in section 86B to restrict access to services used to generate non-consensual fake nude material. However, the introduced Bill requires the eSafety Commissioner to establish that a service was designed predominantly for this purpose and is predominantly used for it. The exposure draft used "or", while the Explanatory Memorandum continues to describe the power as applying to services predominantly "designed or used" for generating this material.

The two tests should operate as alternative grounds for action. Requiring both may exclude a service that was designed for this purpose but is not yet predominantly used for it. It may also exclude a general-purpose service that becomes predominantly used for this harm.

Additionally, a large general-purpose service could be regularly used to generate non-consensual fake nude material at scale without that activity representing most of the service's overall use. Section 86B should therefore also cover services substantially or regularly used for this purpose.

Recommendation 5: Amend section 86B so that either predominant design or predominant use is sufficient to enliven the removal power, and extend the provision to services substantially or regularly used to generate non-consensual fake nude material.

Amendments table

Provision	Issue identified	Suggested amendment
Section 27: Risk assessment of gender-based violence	The Bill expressly recognises gender-based violence as seriously harmful material or conduct, but section 27 does not require providers to assess the risks of gender-based violence arising through their services. A provider could complete a formally compliant risk assessment without examining technology-facilitated gender-based violence.	Amend section 27 to expressly require providers to identify and assess actual or reasonably foreseeable risks of gender-based violence, including technology-facilitated gender-based violence, occurring through or facilitated by the service.
New provision following section 26C: Direct right of action	A person harmed by a provider's breach has no express statutory pathway to enforce the Duty or obtain an individual remedy.	Establish a direct statutory right of action allowing a person who suffers harm because of a provider's breach to seek compensation, an injunction or another appropriate remedy.
Schedule 3 and section 40: Individual complaints pathway	Schedule 3 repeals the existing pathway for complaints about breaches of industry codes or standards without establishing an equivalent pathway for alleged breaches of the Digital Duty of Care.	If Parliament does not establish a direct right of action, it must provide an independent statutory pathway for individuals to raise alleged breaches of the Digital Duty of Care. This should be through: a) a complaints pathway to eSafety, with procedural rights for the complainant; or b) an industry-funded Digital Ombuds scheme with authority to resolve individual disputes and issue binding directions.
Section 5: Definition of harm	The definition does not expressly recognise cumulative harm arising from repeated exposure or a pattern of conduct.	Clarify that harm includes cumulative harm arising from repeated exposure or a pattern of material or conduct, including conduct occurring across multiple accounts or services.
Section 27: Cumulative and volumetric risks	Providers are not expressly required to assess patterns of repeated or coordinated conduct. An incident-based assessment may overlook	Require providers to identify and assess reasonably foreseeable risks arising from repeated or coordinated conduct, including conduct occurring across multiple accounts or services.

	the harm created by the pattern as a whole.	
Section 25D: Adult identity-based harms	The Bill may not capture serious hostility towards a broader group where the material does not amount to menacing or harassment directed at an individual.	Recognise material or conduct that encourages, promotes or incites serious hostility towards a person or group on the basis of one or more protected characteristics, where it is reasonably likely to cause serious harm.
Section 25E: Child identity-based harms	Section 25E recognises hostility towards women or gender equality but does not provide equivalent recognition of hostility based on other protected characteristics.	Recognise material or conduct that encourages or promotes hostile attitudes towards persons or communities on the basis of one or more protected characteristics.
Section 5 and sections 25D–25E: Protected characteristics	"Protected characteristic" is not defined, and the Bill does not expressly recognise harms shaped by intersecting characteristics.	Define "protected characteristic" consistently with Commonwealth anti-discrimination law. Clarify that conduct may be based on one or more protected characteristics, including the interaction between those characteristics.
Section 86B: Fake-nude service removal power	The Bill requires both predominant design and predominant use. This differs from the exposure draft and the Explanatory Memorandum's description of services "designed or used" for the relevant purpose. The predominant-use threshold may also exclude services facilitating harm at scale.	Replace "and" with "or" between the predominant-design and predominant-use tests. Extend the provision to services substantially or regularly used to generate non-consensual fake nude material.

[1] Wesnet, Third National Survey of Technology Abuse and Domestic Violence in Australia, report, August 2026,https://wesnet.org.au/wp content/uploads/2026/09/Wesnet_ThirdNationalSurvey_Digital-art.pdf.
[2] Center for Countering Digital Hate, 'Grok floods X with sexualized images of women and children', 22 January 2026, https://counterhate.com/research/grok floods-x-with-sexualized-images/
[3] UltraViolet, All Out and GLAAD, *More Hate, Fewer Protections: Harmful Content on Meta's Platforms in the Wake of Rollbacks, According to Users* (2025), pp 4–5, 12.
[4] Social Media Victims Law Center, 'Snapchat Lawsuit: Teen Mental Health & Sextortion Lawsuits' (updated 27 August 2026) <https://socialmediavictims.org/snapchat-lawsuit/> accessed 28 October 2026.
[5] Royal Commission on Antisemitism and Social Cohesion (2026) *Transcript of Proceedings - Hearing Block 3, Day 4*, https://asc.royalcommission.gov.au/system/files/2026-07/transcript-day-4-sydney-2-july-2026.pdf