withyouwecan.org
info@withyouwecan.org

21 September 2026

Submitted to the Department of Infrastructure, Transport,
Regional Development, Communications, Sport and the Arts.

Dear Consultation Team,

Submission on the Exposure Draft Online Safety Amendment (Digital Duty of Care) Bill 2026

About Us

With You We Can works toward better responses to sexual violence through knowledge, connection and advocacy. We maintain a public resource that demystifies police and legal processes for victim-survivors, we run advocacy campaigns, and we publish research to inform reform. We are led by lived expertise and informed by advocates, experts and frontline services, and our work centres the communities least well served by existing responses, including First Nations people, culturally and linguistically diverse communities, people on dependent visas, people with disability and LGBTQIA+ people.

Our reform agenda centres on independent legal representation for complainants, implementation of Australian Law Reform Commission Recommendation 10, and reform of the New South Wales Sexual Assault Communications Privilege framework. We made a submission to the ALRC's inquiry into justice responses to sexual violence.

The question beneath all of that work is whether a system built to respond to sexual violence gives the person harmed any standing inside it. This exposure draft raises it again, in a new setting.

We have had regard to the advocacy positions of the Working With Women Alliance and WESNET, and to The Australia Institute's analysis of enforcement. Our recommendations are intended to be read alongside theirs.

Summary of position

We support the Bill. A duty of care is the right instrument, and the shift from reactive takedown to systemic obligation is one this sector has sought for years. Our 26 recommendations are set out below. We press four of them at length, because they are the points on which we believe we can be most useful, and because each is a gap rather than a disagreement about approach.

One. The Schedule 1 takedown reforms, which we strongly support, bring the cyber-bullying and adult cyber-abuse schemes up to the standard the intimate image scheme already meets. The Bill's new protections then stop short of Part 6. The recognition of reposted and altered material does not extend to intimate images, and Part 6A is narrower than the intimate image scheme it sits beside.

Two. The duty protects adults least. In the definition of a safe online environment, protection from design feature harm, and from misogynistic material, appears only in the provisions that apply to children.

Three. Section 25C does not name non-consensual intimate images, synthetic sexual material or sexual extortion, so nothing in the Bill tells a provider that these are risks it must identify and address. Part 6 is the only complaint scheme in the Act with no counterpart in the duty.

Four. The duty runs to the regulator alone. A person harmed by a breach cannot enforce it, cannot seek compensation, and is not entitled to be told the outcome of any action taken under it. Comparable Australian schemes leave the person harmed a route to a remedy. This one does not, and on the eSafety Commissioner's own evidence, the high threshold in the Adult Cyber Abuse Scheme means roughly two per cent of complaints result in a removal notice.

Recommendations

No.	Recommendation
Schedule 1: carry the new protections into the intimate image scheme	
1	Apply the definition of reposted material in new section 65(2E) to Part 6, so that a complaint under section 32 or an objection notice under section 33 extends to reposted and altered copies of the intimate image, and the Commissioner may give a further removal notice under sections 77, 78 and 79 without a fresh complaint or notice.
2	Define "fake nude material" in section 5 by reference to section 15, so that Part 6A covers synthetic material across the full definition of an intimate image.
3	Extend section 86B to apps and websites designed or predominantly used to share intimate images without consent, not only those that generate fake nude material.
A baseline of protection that applies to everyone	
4	Insert an adult equivalent of section 25B(1)(b)(ii), so all persons in Australia are protected from harms associated with the operation of design features.
5	Align the age thresholds between section 25D (under 18) and section 25B(1)(c) (under 16).
6	Harmonise the protective language of the Act so that the duty and the transparency provisions attach consistently to persons in Australia, rather than being scattered across inconsistent terms such as Australians, users in Australia, end-users in Australia and Australian user accounts.
Name the harms in Section 25C	
7	Add a category covering material depicting a person in a sexual context or in a state of nudity, provided without that person's consent, including material created or altered by any technological means.
8	Add a category covering conduct that threatens to provide such material, or demands money, sexual material or another benefit in exchange for not providing it.
9	Add a category covering material or conduct that encourages, promotes or incites hostility, hatred or violence towards a person or group on the basis of sex or gender.
10	Add a category covering sexually explicit material that promotes or normalises strangulation, or other practices capable of causing serious injury.

Gender-based violence and technology-facilitated abuse as systemic risks	
11	Define technology-facilitated abuse in section 5.
12	Amend section 26A(2)(a) so a risk assessment must expressly assess the risk of gender-based violence and technology-facilitated abuse occurring through the service.
13	Require section 26A assessments to analyse risk by reference to sex and gender, and to be informed by consultation with specialist services and victim-survivors.
Weaponisation of ordinary features, and cumulative harm	
14	Amend section 26A(2)(a)(iii) so a provider must assess how any functionality of the service can be used by one person to harm another, whether or not the feature was designed for that use.
15	Expand section 25F(1) to include functionality that discloses a user's location, activity, presence or associations, enables account discovery, or enables unsolicited contact.
16	Amend section 26A(2)(b) so assessments address harm arising from repeated or sustained conduct over time, not only the likelihood and severity of discrete risks.
Systems, not individual choice	
17	Amend section 26(3)(a) so 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.
18	Place the feed control obligation announced as "My Feed, My Way" on the face of the Act, as an addition to the systemic obligation rather than a substitute for it.
Transparency that reaches the algorithm	
19	Amend 192D(1) and 192M(2) to expressly cover recommender and ranking systems, amplification and reach metrics, and how the provider identifies, measures and responds to gendered harms.
20	Require publication of section 26A risk assessments, or a substantive summary, by default, with a mechanism to withhold genuinely commercially sensitive or security-sensitive detail.
The private communications carve-out	
21	Recast section 26(7) so it protects against measures requiring general monitoring or inspection of private communications, rather than exempting a class of communication from the duty. In the alternative, provide that it does not apply to material or conduct of a kind described in section 25C.
Complaint processes, remedies and evidence	
22	Make section 26F apply to all online services other than those exempted under section 25A(3), and specify minimum requirements in the Act: an acknowledgement timeframe, a decision with reasons, an internal review pathway, and accessible processes for people experiencing violence.
23	Provide a direct remedy for a person harmed by a breach: a complaints pathway to the Commissioner with a right to be informed of the outcome, and a statutory cause of action for damages and injunctive relief, on the model of Singapore's Online Safety (Relief and Accountability) Act 2025.
24	Provide that a person harmed may apply to the Commissioner for disclosure of information identifying the person responsible, for the purpose of bringing proceedings.

25	Extend section 205B(1) beyond employees of Australian universities to persons engaged by non-government organisations with relevant expertise, subject to equivalent conditions.
Distinguishing harm from discussion of harm	
26	Amend paragraph 26A(2)(a) so providers must also assess harms from their own moderation, ranking and recommender systems removing, restricting or deprioritising lawful public-interest material, and must distinguish material that perpetrates or promotes gender-based violence from material discussing it for prevention, education, journalism, advocacy or support.

One: Schedule 1 should pass, and its new protections should reach Part 6

We support the Schedule 1 reforms without qualification. Halving the time a person must wait for the service to act on their complaint, from 48 hours to 24, matters because material circulates fastest in the first day. The complaint waiver in new sections 65(2A) and 66(2A), and the equivalents in sections 88 to 90, removes a barrier that asks the most of the people least able to bear it. And the breadth of section 65(2E), which treats material as reposted even where it has been cropped, posted as a screenshot, or had its text or commentary changed, describes how image-based abuse actually circulates.

Those reforms are confined to sections 65 and 66, which deal with cyber-bullying material targeted at an Australian child, and sections 88, 89 and 90, which deal with cyber-abuse material targeted at an Australian adult. These are the only removal notice provisions in the Act that require a person to complain to the service first and wait. The intimate image scheme in Division 3 of Part 6 has never worked that way. A complaint under section 32 or an objection notice under section 33 goes directly to the Commissioner, and a removal notice under sections 77 to 79 already carries a 24-hour deadline. Schedule 1 brings the other two schemes up to that standard. The Bill also strengthens Part 6 directly: new section 82 lets the Commissioner require search engines to delete links to an intimate image, and Schedule 2 lifts the civil penalties under sections 75, 80 and 83 from 500 to 6,000 penalty units.

The Bill's new protections then stop short of Part 6 in three ways.

First, reposting. New section 65(2E) accepts that material is the same material when it has been cropped, screenshotted or had its commentary changed, and sections 65(2C) and (2D) let the Commissioner give a further removal notice for a repost within six months without the person going back to the service. That definition is used only in sections 65, 66, 88, 89 and 90. Part 6 has no equivalent. An objection notice under section 33 objects to the provision of the intimate image on a particular service, so when the image reappears in altered form, or on another site, it is at best unclear whether the original complaint or notice still covers it. The provision written to describe how image-based abuse circulates does not apply to image-based abuse.

Second, the reach of Part 6A. The power in new section 86B turns on "fake nude material", which is not defined anywhere in the Bill or the Act. On its ordinary meaning it is narrower than the definition of intimate image in section 15. That definition covers a person's private parts whether bare or covered by underwear, a

person engaged in a sexual act, and a person shown without attire of religious or cultural significance, and it extends to material that appears to depict the person. Synthetic material of each kind is an intimate image under Part 6 but may not be fake nude material under Part 6A.

Third, section 86B reaches only apps and websites that generate fake nude material, and only through app stores and search engines. There is no equivalent power for an app or website designed or predominantly used to share intimate images without consent.

We do not believe these gaps are deliberate. Recommendations 1 to 3 would close them. Recommendations 1 and 2 require no new policy: the drafting already exists in new section 65 and in section 15 of the Act. We regard them as the most valuable amendments available in Schedule 1.

Two: the duty protects adults least

The duty of care must apply to all, not only to young people. As drafted, much of it does not. Section 25B defines a safe online environment in three limbs. The first protects persons in Australia from seriously harmful material and conduct. The second protects children from material and conduct harmful to children, and from harms associated with the operation of design features. The third stops design features with negative behavioural impacts operating for children under 16 on social media.

Protection from design feature harm therefore appears in the children's limb alone. There is no equivalent anywhere in section 25B for anyone else. Given that sections 25F and 25G are devoted to defining design features and deeming all five of them to have negative behavioural impacts, we do not think the Bill can be intended to leave adults outside that protection. The only design feature obligation that reaches adults is the requirement in section 26(3)(a) to manage design features appropriately, and the Bill gives that requirement no content beyond user empowerment tools. The consequences are not hypothetical: recommender systems that surface misogynistic content to adult men, and feedback features that reward escalating abuse, are both listed design features, and both cause harm to adults.

The same pattern appears in the harm definitions. Material or conduct that encourages or promotes hostile attitudes towards women or gender equality appears in section 25D, which applies to children, and nowhere else. The Bill treats misogyny as a developmental risk to children rather than as a harm to the women at whom it is directed. Harms do not end at 18.

We support the Bill's stronger protections for children and do not seek to dilute them. We ask that they sit above a baseline rather than in place of one. Recommendation 4 would insert an adult equivalent of section 25B(1)(b)(ii). It does not require the under-16 restriction to be extended to adults, and we do not propose that.

Three: section 25C omits the sexual violence harms the Act addresses elsewhere

Section 25C lists the material and conduct that is seriously harmful for the purposes of the duty. It is a serious list and we dispute nothing on it. Absent from it are the non-consensual sharing of intimate images of adults, sexually explicit synthetic material depicting adults, and sexual extortion.

The Act already recognises these harms as serious enough to warrant a dedicated removal notice scheme in Part 6, which this Bill extends through the new section 82 link deletion power. The duty meant to prevent them recurring does not name them. Part 6 is the only complaint scheme in the Act left without a counterpart in the duty. Adult cyber-abuse under Part 7 is reflected in section 25C(1)(f), child cyber-bullying under Part 5 in section 25D(1)(e), and the material covered by the online content scheme in Part 9 across sections 25C and 25D.

We anticipate the response that paragraph 25C(1)(f), covering material or conduct intended to cause serious harm by menacing or harassing an individual, already captures this. It does not. It requires an intention to cause serious harm, and much of this material circulates among people indifferent to the person depicted, on services that host it at scale. It requires an individual target, which a service hosting a library of such material does not have. And it characterises a sexual violation as harassment, which shapes how providers classify it, resource their response to it and report on it.

The practical consequence lies in section 26A. Section 26A(2)(a)(i) requires a provider to identify all reasonably foreseeable risks, but leaves the provider to decide what they are. The duty itself is defined by the harms named in sections 25C and 25D, and nothing in either tells a provider that non-consensual intimate imagery is a risk it must identify and address. Part 6 gives the individual a takedown. Schedule 2 does not require the service to prevent the next one.

One observation captures the problem. Consent appears once in the entire Bill, in the phrase “consenting adults” in section 26(7), where it forms part of an exemption from the duty. In a Bill addressing online safety, consent is a term that should be doing substantive work. Recommendations 7 to 10 would name these harms, and Recommendations 11 to 13 would require providers to assess gender-based violence and technology-facilitated abuse as risks their services create.

Four: enforcement cannot rest with the regulator alone

This is the recommendation we press most strongly, and the one closest to the rest of our work. The duty created by section 26 runs to the Commissioner. There is no private right of action, no compensation, and no complaints pathway to the Commissioner in respect of a breach. Schedule 3 goes further. It repeals section 40 of the Act, the existing right to complain to the Commissioner that an industry participant has breached an industry code or standard, and puts nothing in its place.

A person cannot compel a risk assessment or seek a remedial direction under section 26D, and has no role in any investigation. Formal warnings may be published at the Commissioner’s discretion under new section 183AA, but the person affected is not entitled to be told the outcome of any action taken under the duty. Under the existing takedown schemes a complainant must at least be told if the Commissioner refuses to give a removal notice, and can seek review of that refusal.

The Bill’s own objects clause promises more than this. New paragraph 3(c) states an object of providing complaints schemes or mechanisms to quickly investigate, remove and remediate illegal or seriously harmful

material. Nothing in the Bill remediates anything. There is no provision under which a person receives a remedy of any kind.

Comparable Australian schemes do not leave the person harmed without a remedy. Many of the obligations enforced by ASIC, the ACCC and the Fair Work Ombudsman can also be enforced by the people they protect. Work health and safety law is the closest model for this Bill. Section 25H of this Bill reproduces paragraphs (a) to (e) of the work health and safety test of reasonable practicability, adding a privacy limb. The work health and safety duty is enforced by the regulator, and section 267 of the Work Health and Safety Act 2011 confers no civil right of action for a breach. But that duty sits on top of a common law duty of care and statutory workers' compensation, so the injured worker is compensated. A person harmed by a breach of the digital duty of care has neither. The Bill borrows the test and leaves out the system around it that compensates the person injured.

The consequences of a monopoly are already visible. In evidence to the Royal Commission on Antisemitism and Social Cohesion, eSafety reported receiving approximately 108,000 complaints in the year to 30 June 2026. The Commissioner told the Royal Commission that the high threshold in the Adult Cyber Abuse Scheme meant roughly two per cent of complaints resulted in a removal notice. Of the handful of civil penalty proceedings eSafety has brought, one produced a penalty of $650,000 against X Corp in 2026, by consent, and another a penalty of $343,500 against an individual in 2025 for posting deepfake intimate images. Nothing from either went to the people harmed. We adopt The Australia Institute's analysis of these figures. A regulator with finite resources must triage, and will rightly prioritise the most dangerous material, which means most harm goes unaddressed. The Bill reinforces the point: breach of the duty carries a maximum penalty of 60,000 penalty units, described by the Government as $109.2 million, but new section 163A sets the amount payable under an infringement notice for the same provision at 600 penalty units for a body corporate per contravention, or $218,400. That is ten times the standard amount under the Regulatory Powers Act, and still about 0.2 per cent of the headline figure. None of it reaches the person harmed.

There is a model available. Singapore's Online Safety (Relief and Accountability) Act 2025 creates a statutory tort across 13 categories of online harm, imposing duties on the person who posts, the administrator of the group or page, and the platform, and giving the person harmed a claim for damages and an injunction. Its first phase commenced on 29 June 2026, and two of the five priority harms in that phase are intimate image abuse and image-based child abuse. From the same date a person may apply to the regulator for information identifying the person responsible in order to bring a claim, a power that matters particularly in image-based abuse, where the perpetrator is very often anonymous to the person harmed.

We recognise that the Government may be reluctant to create a new cause of action, and we ask that the question be considered on its merits rather than by analogy to the existing scheme. The people affected by these harms want the material gone, an account of what the service did and failed to do, and acknowledgement of the harm. The Bill delivers the first through Schedule 1 and offers nothing toward the second or the third. Recommendations 23 and 24 set out what we consider the minimum, and we note that they are common ground across organisations approaching this Bill from very different starting points.

Further matters

We support the following recommendations on the same reasoning, and note that they are shared ground with the Working With Women Alliance.

Weaponisation and cumulative harm (Recommendations 14 to 16). Section 25F(1) is expressed inclusively, but the five features it lists are all engagement features. The functionality actually used to commit technology-facilitated abuse is ordinary and not harmful in itself: location and activity disclosure, read and view receipts, account suggestion, unlimited account creation, and contact from accounts a person does not follow. Section 26A(2)(b) also tests likelihood and severity, which captures the single serious act and misses the pattern that constitutes coercive control.

Systems, not individual choice (Recommendations 17 and 18). Section 26(3)(a) requires providers to manage design features appropriately, "including by providing user empowerment tools as required". That is the only content the Act gives to appropriate management, which makes configurability the measure of compliance. It also assumes that the people causing harm will choose to limit their own exposure. An early assessment published in The BMJ found that circumvention of the under-16 social media restrictions was common, with little evidence of reduced use, and there is no reason to expect the men most immersed in misogynistic content to be the ones who switch the algorithm off. We also note that the feed control announced on 8 September does not appear in the exposure draft: section 26(4) is a power for the Minister to require user empowerment tools by instrument, and nothing requires that instrument to be made.

Transparency (Recommendations 19 and 20). Neither section 192D(1) nor section 192M(2) refers to recommender or ranking systems, to amplification, or to how a provider identifies gendered harms. Risk assessments are also not published by default, so the only evidence of compliance is unavailable to the organisations that see the harm.

The private communications carve-out (Recommendation 21). Section 26(7) exempts lawful private communications solely between consenting adults. Image-based abuse, sexual extortion and technology-facilitated coercive control occur overwhelmingly in private channels, and consent is the contested fact. The privacy objective is already served proportionately by section 25H(e)(ii), which weighs the privacy impact of any measure.

Complaints and evidence (Recommendations 22 to 25). Whether a service must have a complaints process at all depends on a future determination under section 26F(3), which is inconsistent with the Schedule 1 waiver now turning on whether a service has a functional complaints mechanism. Separately, section 205B confines data access to employees of Australian universities, excluding the organisations that hold much of the evidence about how these harms occur.

Distinguishing harm from discussion of harm (Recommendation 26). A risk assessment aimed at gender-based violence creates its own incentive toward over-removal, particularly of survivor advocacy, journalism and

prevention content that necessarily engages with the subject matter. Section 26A(2)(a) should require providers to assess this risk directly, and to distinguish material that perpetrates or promotes gender-based violence from material that discusses it for prevention, education, journalism, advocacy or support.

Conclusion

We support this Bill and want it to pass. Carry the Bill's recognition of reposted material into Part 6, and give Part 6A the reach of the Act's own definition of an intimate image, so image-based abuse is not the harm the new protections pass over. Give adults a baseline of protection beneath the children's provisions. Name the sexual violence harms the duty omits, and require providers to assess gender-based violence and technology-facilitated abuse as risks their services create. And give the person harmed a place in the scheme, which at present they do not have. We would welcome the opportunity to discuss this submission with the Department.

Yours sincerely,

Sarah Rosenberg
Executive Director and Co-Founder
With You We Can