Working with Women Alliance

Privacy Reforms and Gender-Based Violence

Privacy Amendment (Personal Data Protection) Bill 2026

September 2026

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.

The Working with Women Alliance (WwWA) represents more than 800 organisation and individual members across two key portfolios: gender-based violence and gender equality. The 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
Policy Officer: Darcie Newland
safety.policy@wwwa.org.au

Executive Summary

The Working with Women Alliance (WwWA) welcomes the opportunity to provide feedback on the *Privacy Amendment (Personal Data Protection) Bill 2026* and the associated consultation paper.

WwWA is a national membership-based organisation representing two connected portfolios: gender-based violence and gender equality. Across these portfolios, WwWA has more than 900 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 the five National Women's Alliances funded through the Department of Prime Minister and Cabinet to ensure women's voices are central to national policy development.

WwWA's interest in the Bill is grounded in women's safety. Personal information and digital technologies are being weaponised to monitor, locate and control victim-survivors. WwWA supports the proposed amendments, particularly the stronger recognition of precise geolocation data, AI-generated inferences and synthetic material as personal information. The recommendations below focus on strengthening the reforms through safeguards prevent foreseeable technology-facilitated abuse and ensure victim-survivors can exercise and enforce their privacy rights.

WwWA endorses the submission made by *With You We Can*, a national lived experience-led advocacy organisation, and supports its recommendations to strengthen privacy protections for victim-survivors.

We thank the Department for the opportunity to provide input and look forward to continued engagement on these important reforms.

Recommendations

1. Entities should be required to assess and address foreseeable privacy and safety risks before introducing products or features that enable people to be recorded, monitored or located without their knowledge.
2. Ensure the legislation or supporting guidance expressly recognises domestic, family or sexual violence as a circumstance that can create heightened privacy and safety risks. Require entities applying the fair and reasonable test to consider foreseeable misuse against victim-survivors and adopt safeguards proportionate to the likelihood and severity of harm.
3. The definition of precise geolocation tracking data should include both ongoing tracking and one-off disclosures of an individual's precise location.

4. The right to erasure should apply to all APP entities holding personal information, rather than being limited to large digital platforms.
5. The consent framework should expressly protect people who have no meaningful opportunity to know about or refuse the collection of their personal information, including people captured by wearable surveillance technologies.
6. The final complaints framework should allow individuals to approach the Information Commissioner directly where first complaining to the APP entity would be inappropriate or impracticable, including where there is an urgent risk to safety.
7. The Australian Government should introduce an accessible direct right of action for serious interferences with privacy.

Camera glasses are new, but patterns of abuse are not

The Australian Government has released these reforms against the backdrop of serious concern about Kmart's $89 camera glasses, which made discreet recording technology available at a price and scale not seen before. Unlike a phone held up to record, camera glasses can capture people without their knowledge and make it difficult for women to know when their privacy is being violated. The Government has described the Bill as strengthening privacy and safety, yet it is unclear how the proposed reforms would require Kmart or other retailers to assess and address these foreseeable risks before placing such a product on the market.

These glasses are not an isolated or uniquely sinister technology. Social media has become a vehicle for harassment and image-based abuse. Location-sharing tools and tracking devices can be used to stalk victim-survivors, while spyware can turn a phone into a surveillance device. Generative AI has created new ways to produce and distribute synthetic intimate images and child sexual abuse material. Governments will continue to struggle to legislate for each new product or platform as it emerges. But victim-survivors are not describing a series of unrelated technologies. They are describing the same patterns of control and violence that are being enabled through changing tools and technology.

Privacy law cannot prevent these harms by responding to one technology at a time. It must require entities to identify how products, features and data practices could foreseeably be misused to facilitate gender-based violence, and to address those risks before harm occurs. The Privacy Act Review recommended mandatory Privacy Impact Assessments before high-risk activities commence. This should expressly include assessment of whether a product or feature could foreseeably be misused to locate, monitor or expose a person experiencing violence.

Recommendation 1: Entities should be required to assess and address foreseeable privacy and safety risks before introducing products or features that enable people to be recorded, monitored or located without their knowledge.

Fair and reasonable test

WwWA supports the introduction of a fair and reasonable test. This is an important shift away from relying too heavily on consent and towards requiring entities to take responsibility for the consequences of their information-handling practices.

We particularly welcome the requirement for entities to consider the potential impacts on individuals and give particular regard to circumstances involving people experiencing vulnerability. What is fair, reasonable and proportionate must depend on the consequences for the person affected, including the likelihood and severity of foreseeable harm. The Bill and supporting guidance should expressly recognise that domestic, family or sexual violence can create heightened privacy and safety risks. Information handling that may present limited risk in ordinary circumstances can have serious consequences where personal information could be misused by a perpetrator to monitor, locate or expose a victim-survivor.

Entities should therefore be required to consider these risks when applying the fair and reasonable test and adopt stronger safeguards where technology-facilitated abuse is known or reasonably foreseeable. This assessment should focus on the safety consequences for the person affected, not only the entity's ordinary operations or commercial interests.

Recommendation 2: Ensure the legislation or supporting guidance expressly recognises domestic, family or sexual violence as a circumstance that can create heightened privacy and safety risks. Require entities applying the fair and reasonable test to consider foreseeable misuse against victim-survivors and adopt safeguards proportionate to the likelihood and severity of harm.

Personal and sensitive information, including geolocation tracking data

WwWA supports changing the definitions of personal information and sensitive information to replace 'about' with 'relates to'. WwWA also supports recognising precise geolocation tracking data as sensitive information. However, limiting the definition to information collected and held over time overlooks the safety risk created by a single disclosure. For a victim-survivor, one disclosure of their precise location can be enough to enable stalking and abuse.

The bill must reflect the real-world safety risks created by personal information, including where information that appears innocuous can be used to locate and monitor a victim-survivor.

Recommendation 3: the definition of precise geolocation tracking data should include both ongoing tracking and one-off disclosures of an individual's precise location.

Right to erasure on large digital platforms

WwWA strongly supports the introduction of a right to erasure, also known as the "right to be forgotten", which has been a longstanding call of privacy and human rights advocates. This right can give victim-survivors greater control over personal information that may otherwise remain available long after its original collection or publication. It is an important protection where intimate images, covert recordings, location information or other identifying material can be repeatedly accessed or used to continue abuse.

However, the proposed right only applies to large digital platforms that satisfy the revenue or user threshold of platforms with $500 million in group revenue or 2.5 million monthly users. These thresholds reflect an entity's size and assumed capacity to comply, not the seriousness of the harm its handling of personal information may cause. Harmful material does not become less dangerous because it is held by a smaller platform. Harmful material including intimate images, covert footage, and doxxing practices may be more prevalent among smaller 'niche' providers whose platforms and services are specifically designed to facilitate technological abuse.[1] This includes 'nudify' applications, some people-searching sites, and pornography sites hosting child sexual abuse and other illegal material. These platforms and services are often origin points or 'incubators' of harmful material, which is then spread to other online spaces.[2] They are also often disguised, marketed as photo editing or entertainment tools.[3]

The power to prescribe additional platforms provides some flexibility, but it still leaves protection dependent on government identifying individual services after risks have emerged. Victim-survivors should not need to determine the size, revenue or regulatory status of a platform before they can exercise control over their own personal information.

Recommendation 4: The right to erasure should apply to all APP entities holding personal information, rather than being limited to large digital platforms.

Consent

WwWA supports the proposed requirement that consent be voluntary, informed, current, specific and unambiguous. These changes provide important safeguards against bundled consent and pre-selected settings designed to steer people towards agreement.

WwWA recommends that the definition be expanded to be expressly withdrawable and must not be obtained through coercion. The exception allowing sensitive

information to be collected where it is "strictly necessary" to deliver a requested service must remain a high bar and apply only where the service could not be provided through a less privacy-intrusive alternative. Stronger consent requirements also cannot protect people who do not know they are being recorded or have no opportunity to refuse. The fair and reasonable test must provide substantive protection for people captured by wearable surveillance technologies, regardless of whether the technology's user has consented to its terms.

Recommendation 5: The consent framework should expressly protect people who have no meaningful opportunity to know about or refuse the collection of their personal information, including people captured by wearable surveillance technologies.

OAIC powers and efficiency

As outlined in the Privacy Act Review, effective enforcement of the Privacy Act is essential to protecting the privacy of individuals and the public interest in privacy WwWA supports strengthening the Information Commissioner's powers. These powers are increasingly important as privacy investigations involve complex digital systems and entities that may be unwilling to cooperate.

Stronger powers must also be matched by clear coordination between the OAIC, eSafety Commissioner and other relevant regulators. Privacy and online-safety harms frequently overlap, and victim-survivors should not be left to identify the correct regulator or navigate separate systems before action is taken. The OAIC and eSafety Commissioner should establish clear pathways for referrals, information-sharing and coordinated regulatory action, particularly where technology-facilitated abuse creates an immediate safety risk or harmful practices affect people across multiple platforms.

WwWA supports measures to improve the early resolution of privacy complaints. The exposure draft must retain the exception contemplated by the *Privacy Act Review* for circumstances where it would be inappropriate or impracticable to require an individual to complain to the APP entity first, including where there is an urgent risk to safety. For victim-survivors, delays in responding can allow harm to continue. The final framework must provide a clear pathway for urgent complaints to be made directly to the Information Commissioner.

Expanded powers must be matched by adequate resourcing. The OAIC needs sufficient resourcing to investigate complex digital systems, respond to urgent safety risks and address systemic non-compliance, including through litigation. As per the Privacy Act Review should consider cost recovery through a levy or fees to fund enforcement activities.

Recommendation 6: The final complaints framework should allow individuals to approach the Information Commissioner directly where first complaining to the APP entity would be inappropriate or impracticable, including where there is an urgent risk to safety.

A direct right of action

In addition to strengthening the powers of the OAIC, the Australian Government should seriously consider introducing the direct right of action recommended by the *Privacy Act Review*. This would give individuals another pathway to enforce their rights and ensure compliance does not rest on the capacity of a single regulator. This was a clear recommendation of the *Privacy Act Review*, which recognised that individuals should have a pathway to enforce their privacy rights directly rather than relying solely on the capacity of the Information Commissioner.

Recommendation 7: The Australian Government should introduce an accessible direct right of action for individuals who suffer loss or damage because of an interference with their privacy, with appropriate safety protections for victim-survivors.

---

[1] Institute for Strategic Dialogue, (2026). *Mapping the 'Nudify' Tools Ecosystem*, https://www.isdglobal.org/wp-content/uploads/2026/08/Mapping-the-Nudify-Tools-Ecosystem.pdf

[2] Institute for Strategic Dialogue, (2026). *High risk, small platforms: Understanding synthetic non-consensual intimate imagery and community norms on 4chan*, https://www.isdglobal.org/digital-dispatch/high-risk-small-platforms-understanding-synthetic-non-consensual-intimate-imagery-and-community-norms-on-4chan/

[3] National Center on Sexual Exploitation, (2026). *New Research Finds Apple App Store and Google Play Target Users with Ads for "Nudify" Apps*, https://endsexualexploitation.org/articles/new-research-finds-apple-app-store-and-google-play-target-users-with-ads-for-nudify-apps/