

Formal Submission: Informing Direction for the Second Action Plan

National Plan to End Violence against Women and Children 2022-2032

July 2026

SUBMISSION OVERVIEW AND CONTEXT

This submission is authored by:

[REDACTED] research focuses on the prevalence, nature and impacts of gendered violence, including legal and nonlegal responses to addressing and preventing violence. Her current research is focused on technology-facilitated abuse and image-based sexual abuse.

[REDACTED] research focuses on sexual violence, technology-facilitated harms, and image-based abuse, including emerging issues related to AI and digital technologies. [REDACTED] her PhD which explored victim-survivors' experiences of seeking justice for image-based sexual abuse through reporting and help-seeking pathways.

The submission seeks to inform **Priority Area 1** (victim-survivors) and **Priority Area 2** (prevention and early intervention) with a specific focus on image-based sexual abuse (IBSA), including AI-generated image-based sexual abuse (AI-IBSA).

Our submission draws on data collected from an Australian Research Council (ARC) Future Fellowship project, entitled, *Detecting, Preventing and Responding to Image-Based Abuse* (FT200100604), as well as two Google-funded projects, including a multi-country online survey on IBSA conducted in mid-2023 with 16,000 respondents from ten countries, and a cross-national survey on AI-IBSA conducted in 2024 with 7,231 respondents from Australia, the United Kingdom and the United States.

In this submission, we make the following five recommendations to improve victim-survivor support and drive greater primary prevention and intervention initiatives for IBSA in Australia:

1. Develop and strengthen trauma-informed and accessible reporting and support pathways that respond effectively to the diverse needs of victim-survivors of IBSA.
2. Establish consistent and comprehensive legal and regulatory frameworks to address the full spectrum of IBSA.
3. Invest in evidence-based prevention initiatives that challenge gendered entitlement, promote consent and digital sexual ethics, and address the social norms that enable IBSA.
4. Mandate safety-by-design approaches, standards and accountability requirements for digital platforms.
5. Restrict or prohibit platforms, applications and technologies where the primary purpose is the creation of non-consensual AI-generated intimate images.

PRIORITY AREA 1. VICTIM-SURVIVORS

Recommendation 1: Develop and strengthen trauma-informed and accessible reporting and support pathways that respond effectively to the diverse needs of victim-survivors of IBSA.

Across multiple survey and interview studies, our research shows that many victim-survivors of IBSA chose not to seek support or report their experiences, despite reporting significant harms and negative impacts including anger, humiliation, depression, sadness and fear (Henry et al., 2020; Henry et al., 2026a; Umbach et al., 2024; Umbach, Henry & Beard, 2025). Barriers to reporting and help-seeking include embarrassment, shame, self-blame, uncertainty about available support, fear of retaliation, perceptions that little can be done, and a lack of trust in institutional responses (Henry et al., 2020; Umbach et al., 2024a; Umbach, Henry & Beard, 2025).

When victim-survivors do seek help, they typically prioritise rapid intervention, image removal and practical assistance. For example, victim-survivors in our recent AI-IBSA study were more likely to report incidents directly to digital platforms (58%) or contact websites for image removal (53%) rather than report to police (40%) (Henry et al., 2026a). However, those who engaged with these pathways often described them as slow, ineffective or unhelpful. Our research shows that some victim-survivors were told that content did not breach platform policies, that there was little police could do, or that their experiences did not warrant intervention (Henry et al., 2021; Henry et al., 2026a). Many instead relied on self-directed strategies, such as blocking perpetrators or attempting to manage the situation themselves, as well as informal support from friends and family (Henry et al., 2026a). These experiences can reinforce perceptions of futility and further discourage reporting and help-seeking.

Strengthening reporting and support pathways should be a priority under the Second Action Plan. This includes investing in specialist, trauma-informed and accessible

support services equipped to respond to the full spectrum of IBSA, including emerging forms such as AI-generated abuse and sextortion (e.g., threats made to share intimate images). Dedicated funding should also be provided to build the capacity of frontline services, including police, the eSafety Commissioner, legal services, victim support organisations, domestic and sexual violence services and other first responders, to support victim-survivors of IBSA through specialised training, evidence-based guidance and clear referral pathways. This is particularly important as emerging forms of IBSA continue to develop and many frontline professionals may encounter these harms without adequate knowledge or resources.

Support services and reporting pathways also need to be designed to respond to the diverse experiences and needs of victim-survivors of IBSA. This includes ensuring culturally safe, accessible and inclusive responses for groups who may face additional barriers to disclosure and support, including Aboriginal and Torres Strait Islander peoples, LGBTQI+ communities, young people, older people, people with disability, migrants and culturally and linguistically diverse communities, and sex workers. Responses should recognise that barriers to help-seeking are shaped by multiple factors, including stigma, discrimination, concerns about confidentiality, fear of institutional responses, and existing vulnerabilities and power imbalances.

Governments should also invest in innovative digital support options that complement, rather than replace, appropriately resourced human services. Anonymous, private and self-directed digital interventions, including trauma-informed chatbots and online decision-support tools, have the potential to address barriers to disclosure by providing timely information, safety planning, referral pathways and emotional support for victim-survivors who may feel too embarrassed, ashamed or fearful to seek assistance through traditional channels. These tools may be particularly valuable at early stages of victimisation, when individuals are seeking information about whether what has occurred constitutes abuse, what options are available, and what steps they can take to empower themselves and enhance their safety (Henry, Witt & Vasil, 2025).

Improving the responsiveness of reporting pathways is equally important. Police, online safety agencies, digital platforms and other reporting bodies should ensure that reports of IBSA are taken seriously, responded to promptly, and that victim-survivors are kept informed throughout the reporting process. Given that rapid content removal is consistently identified by victim-survivors as a key priority, greater collaboration between governments, law enforcement, support services and technology companies is needed to streamline reporting processes and improve access to timely image removal and other practical supports.

PRIORITY AREA 2. PREVENTION AND INTERVENTION

Recommendation 2: Establish consistent and comprehensive legal and regulatory frameworks to address the full spectrum of IBSA.

In our cross-national survey of over 16,000 adults across 10 countries, more than one in five respondents (22.6%) reported experiencing at least one form of IBSA. Victimization rates were higher among LGBTQ+ and younger respondents, and although women and men reported similar rates of victimization, women reported greater harms and negative impacts. Nearly one-third (30.9%) of victim-survivors did not disclose their experience to anyone (Umbach et al., 2025).

AI-IBSA represents an emerging and significant form of abuse. In our cross-national survey of Australia, the United Kingdom and the United States, 14.9% (n = 7,230) of respondents reported experiences involving non-consensual digitally altered or manipulated images, including 6.6% who reported experiences specifically involving AI-generated intimate images (Henry et al., 2026a).

In Australia, all state, territory and federal jurisdictions (with the exception of Tasmania) have introduced specific criminal offences prohibiting the non-consensual distribution of intimate images, as well as threats to distribute intimate images. Within these laws, an “intimate image” is generally defined as nude or sexual material, and includes images created, altered or manipulated by digital technologies. However, legal protections remain inconsistent, particularly in relation to the creation of non-consensual synthetic intimate images, including AI-generated sexual images.

A nationally consistent approach should include criminal laws that address the full range of IBSA behaviours, including the non-consensual creation, distribution and threats to distribute intimate images, and including non-consensual intimate images generated by digital means like AI. Such reforms may contribute to prevention by establishing clearer social and legal norms around unacceptable conduct. This aligns with community attitudes on the issue, with nearly 90% of respondents from our multi-national survey rating AI-IBSA as either “totally unacceptable” or “somewhat unacceptable” (Henry et al., 2026b).

However, criminalisation alone is unlikely to be sufficient, and, in some circumstances, may not be appropriate, particularly in cases involving young people where prevention, education and restorative approaches may provide a more effective response. A comprehensive legal response should also include civil and regulatory mechanisms that provide alternative remedies for victim-survivors, including timely removal processes, compensation and other forms of redress.

Strengthening online safety regulation is also critical. This should include clear obligations for digital platforms and AI services to prevent, detect and respond to the

creation and dissemination of non-consensual intimate images, as well as threats involving intimate images (e.g., sextortion). These obligations should be supported by transparent reporting and complaints mechanisms, timely responses, and effective pathways for victim-survivors to seek assistance and have harmful content removed. The effectiveness of legal frameworks will depend on adequate implementation, including police training, resourcing and guidance for frontline responses. Research indicates that police responses to IBSA remain inconsistent, contributing to victim-survivors feeling unsupported or let down by criminal justice responses (Henry et al., 2018; Rackley et al., 2021).

Where appropriate, voluntary and survivor-centred restorative justice approaches should also be considered as part of a broader response. Such approaches may provide opportunities for acknowledgement, accountability and behavioural change, while recognising that they cannot replace access to legal redress and support services.

Recommendation 3: Invest in evidence-based prevention initiatives that challenge gendered entitlement, promote consent and digital sexual ethics, and address the social norms that enable IBSA.

Prevention initiatives are critical to addressing the social and cultural drivers of IBSA. Our multinational survey of over 16,000 respondents across 10 countries examined the prevalence, motivations and relational dynamics of IBSA perpetration. More than one in nine respondents reported engaging in at least one IBSA perpetration behaviour, including creating, stealing, sharing or threatening to share intimate images without consent (Umbach & Henry, 2025). Importantly, IBSA is not limited to those who directly perpetrate abuse: one quarter of respondents reported knowingly seeking out or requesting non-consensual intimate images, and almost half reported being bystanders who had received such content. These findings demonstrate that IBSA operates within a broader digital ecosystem in which the creation, circulation and consumption of non-consensual intimate images can become normalised.

Our findings also highlight the need for prevention approaches that move beyond narrow understandings of IBSA as primarily a form of revenge or individual malicious intent. Motivations varied across different forms of IBSA, demonstrating the importance of recognising the diverse contexts in which abuse occurs, including image creation, sharing, threats to share and non-consensual consumption (Umbach & Henry, 2025). Prevention initiatives should therefore address the range of attitudes and behaviours that contribute to IBSA, including gendered entitlement, misconceptions about consent, peer norms, victim-blaming, and the trivialisation of sexual harm.

Emerging forms of IBSA involving artificial intelligence further demonstrate the importance of prevention approaches that address changing technological practices and social norms. In our study, 3.2% of respondents reported creating, sharing or

threatening to share non-consensual AI-generated sexual content. These behaviours were more common among younger respondents, men, respondents from racially marginalised backgrounds and people living with disability (Umbach et al., 2026). Participants often described motivations that were not framed as malicious, including that they “thought it was funny”, wanted to “experiment with technology” or sought to “show off” to others. These findings suggest that AI-IBSA may occur within peer cultures where sexualised synthetic content is used for humour, bullying, social bonding or mockery, highlighting the importance of prevention approaches that challenge the normalisation and trivialisation of these behaviours (Umbach et al., 2026; Henry, Vowles & Beard, 2025).

Educational interventions should promote a broader understanding of consent that extends to the creation, sharing, requesting and use of intimate images and synthetic sexual content. Prevention initiatives should also include bystander-focused approaches that challenge the normalisation of viewing, requesting or circulating non-consensual intimate images and empower individuals to respond safely when they encounter abusive content.

Prevention efforts should also be tailored to different communities and contexts. Our research found higher rates of reported victimisation and perpetration among men, LGBTQ+ respondents and younger respondents, with variation across countries (Henry et al., 2026a; Umbach & Henry, 2025). This highlights the importance of developing targeted, inclusive and developmentally appropriate interventions, including education that addresses peer-to-peer IBSA and sextortion among “at-risk” groups.

There is also growing support for a whole-of-community approach to sexual consent education and prevention. Such approaches recognise that preventing IBSA requires addressing the broader attitudes and social norms that shape digital sexual behaviours, including gendered entitlement, shame and stigma surrounding sexuality, and the denigration of women and gender-diverse people. They should also promote positive understandings of sexuality, consent and respectful relationships, while empowering people of all genders to participate in digital environments (Umbach et al., 2025). As technologies continue to evolve, prevention initiatives must support young people and adults to recognise and respond to emerging forms of harm, including AI-generated abuse (Henry et al., 2026a).

Recommendation 4: Mandate safety-by-design approaches, standards and accountability requirements for digital platforms.

Digital platforms and AI service providers should have clear policies prohibiting the creation, sharing, dissemination and threatened dissemination of non-consensual nude or sexual imagery, including synthetic or AI-generated content. These policies should be supported by effective mechanisms to prevent, detect and respond to such

harms, including accessible reporting pathways, timely removal processes and appropriate support for victim-survivors.

More broadly, platforms and AI providers should be required to adopt safety-by-design approaches that embed prevention, risk assessment and accountability throughout the design, development and deployment of their products and services. This includes ensuring that platform features, AI systems, reporting mechanisms, moderation processes and user-facing tools are designed to reduce foreseeable risks of harm.

To ensure meaningful adoption of safety-by-design approaches, governments should establish clear legal obligations, minimum standards and accountability mechanisms for digital platforms and AI service providers. This could include enforceable duties of care, mandatory risk assessments for services that enable image generation or sharing, transparency obligations regarding the prevention and handling of IBSA, and independent oversight to monitor compliance. Platforms should be required to demonstrate how they identify and mitigate foreseeable risks, respond to reports of abuse, and provide effective remedies for victim-survivors.

Our research demonstrates that IBSA perpetration and engagement with non-consensual intimate images occur across a range of motivations and contexts, including malicious motivations such as retaliation, control and sexual gratification, as well as contexts involving curiosity, experimentation, entertainment and peer interaction (Henry, Vowles & Beard, 2025; Umbach et al., 2026; Umbach & Henry, 2025). This diversity highlights the need for interventions that address both deliberate abuse and the social norms, peer cultures and technological affordances that can enable the creation, circulation and consumption/viewing of non-consensual sexual imagery.

Search engines and hosting platforms should take proactive steps to reduce the visibility, discoverability and amplification of AI-IBSA content, as well as AI image-generation tools that can be used to create non-consensual sexual imagery. The accessibility and ease of use of such technologies may contribute to their misuse, making preventative interventions at the design and infrastructure level essential.

General-purpose AI model developers and providers (e.g., Google, Meta and OpenAI) should also be required to implement robust safeguards to prevent the misuse of AI systems to create non-consensual sexual content. This should include meaningful restrictions on image generation capabilities, assessment of potential misuse, and transparent processes for responding to reports of abuse. Requiring AI developers and digital platforms to exercise a duty of care may reduce the creation of non-consensual sexual imagery while also establishing stronger social norms that such uses of technology are unacceptable. This is particularly important given that 18% of respondents in our survey reported knowingly seeking out non-consensually generated AI intimate images (Umbach et al., 2026).

AI-generated abusive content is distributed through diverse channels, including highly visible public dissemination (e.g., social media posts and dedicated deepfake pornography websites) and less visible forms of distribution (e.g., individual or group messaging, screensharing and cloud sharing) (Umbach et al., 2026). While publicly available content may be identifiable and actionable under platform policies, private methods of sharing present greater challenges for automated detection approaches, including image-hashing technologies. Platforms should therefore implement accessible reporting mechanisms, provide guidance for users who encounter abusive content involving themselves or others, and establish clear pathways to specialist support services.

These obligations should also address sextortion and other forms of technology-facilitated sexual coercion, where the threat to distribute intimate images may itself cause significant harm even when content has not been shared. Platforms should ensure that reporting systems detect and respond to threats, coercion and extortion involving intimate images, including providing timely responses and safety information for users.

Overall, these findings underscore the need for a shift from reactive responses that rely primarily on victim-survivor reporting towards proactive responsibility by platforms and AI developers. Safety-by-design approaches should ensure that digital systems are developed, deployed and governed in ways that reduce opportunities for IBSA and other forms of technology-facilitated sexual harm.

Recommendation 5: Restrict or prohibit platforms, applications or technologies where the primary purpose is the creation of non-consensual AI-generated intimate images.

In addition to imposing criminal and civil penalties on individuals, continued attention should be directed towards the technologies and services that facilitate the creation and sharing of non-consensual intimate images. While the *Online Safety Act 2021* (Cth) provides the Australian eSafety Commissioner with powers to respond to intimate images shared online without consent, including through removal and other regulatory mechanisms, it does not specifically address purpose-built applications and services designed to generate non-consensual, AI-generated sexual imagery.

Our research demonstrates that AI-IBSA can arise in contexts involving a range of motivations, including experimentation with technology, humour and peer interaction, as well as more explicitly harmful motivations (Umbach et al., 2026). The availability and ease of access to purpose-built “nudify” applications and deepfake generation tools creates environments in which the production of non-consensual sexual imagery can be undertaken cheaply, quickly and at scale. Where technologies are specifically designed to facilitate the creation of sexualised images of real people without their

consent, restricting or prohibiting access represents an important primary prevention opportunity.

The Second Action Plan should therefore consider regulatory approaches that place obligations on developers, app stores, hosting services and other intermediaries to identify and restrict technologies whose primary function is the creation of non-consensual intimate imagery. Such approaches should be complemented by broader safety-by-design obligations for legitimate AI services (see response above), recognising that preventing IBSA requires intervention not only after harmful content has been created or shared, but also at the point where enabling technologies are developed and deployed.

CONCLUSION

Overall, the recommendations outlined in our Submission align closely with the key priorities for the Second Action Plan identified in the consultation paper, including:

- Developing fast, effective responses to emerging forms of technology-facilitated abuse and harm.
- Improving experiences of policing and justice responses to reduce re-traumatisation, strengthen trust, and ensure equitable access to protection and accountability for all victim-survivors.
- Improving understanding of safe and healthy relationships, behaviours, attitudes and consent.
- Challenging and correcting common myths and misconceptions about violence, and creating opportunities to prevent their spread.
- Ensuring respectful relationships education remains current and responsive to emerging harms experienced by young people, including those enabled by digital technologies.
- Addressing major evidence gaps in public attitudes and the institutional systems that enable, excuse or fail to prevent and respond to violence.

Together, our five recommendations provide a comprehensive framework for addressing IBSA. They recognise that effective responses require more than individual accountability after harm has occurred; they also require investment in prevention, survivor-centred support, effective legal and regulatory frameworks, and greater responsibility from digital platforms and technology providers.

We believe that implementing these recommendations would make a meaningful contribution to improving the safety and wellbeing of at risk-users and victim-survivors, and in doing so strengthen Australia's broader response to technology-facilitated abuse.

References

Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A. & Scott, A.J. (2020). *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*. Routledge.

Henry, N., Witt, A. & Vasil, S. (2025). A “design justice” approach to developing digital tools for addressing gender-based violence: Exploring the possibilities and limits of feminist chatbots. *Information, Communication & Society*, 28(11), 1884-1907.
<https://doi.org/10.1080/1369118X.2024.2363900>

Henry, N., Umbach, R., Shelby, R. & Gonzalez-Pons, K. (2026a). “That experience still haunts me to this day”: A multi-region study of AI-generated image-based sexual abuse victimization. Under Review.

Henry, N., Umbach, R., Shelby, R., Beard, G. & Given, L. M. (2026b). “It’s still abuse”: Community attitudes and perceptions on AI-generated image-based sexual abuse. *Information, Communication & Society*, 1–21. <https://doi.org/10.1080/1369118X.2026.2613437>

Henry, N., Vowles, C. & Beard, G. (2026). “Doing gender”: A digital ethnography of image-based abuse perpetration. *New Media & Society*, 28(4), 1571–1591.
<https://doi.org/10.1177/14614448251356604>

Our Watch, 2025. Respectful relationships education: A blueprint for preventing gender-based violence through education systems.
<https://assets.ourwatch.org.au/assets/RREresources/Respectful-relationships-education-blueprint.pdf>

Rackley, E., McGlynn, C., Johnson, K., Henry, N., Gavey, N., Flynn, A. & Powell, A. (2021). Seeking justice and redress for victim-survivors of image-based sexual abuse. *Feminist Legal Studies*, 29(3), 293–322. <https://doi.org/10.1007/s10691-021-09460-8>

Umbach, R. & Henry, N. (2025). Perpetration of image-based sexual abuse in the digital age: Prevalence, motivations, and community attitudes in 10 countries. *Journal of Cybersecurity*, 11(1). <https://doi.org/10.1093/cybsec/tyaf033>

Umbach, R., Henry, N. & Beard, G. (2025). Prevalence and impacts of image-based sexual abuse victimization: A multinational study. In N. Yamashita, V. Evers, K. Yatani, X. Ding, B. Lee, M. Chetty & P. Touns-Dugas (Eds.), *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (pp. 1–20). ACM. <https://doi.org/10.1145/3706598.3713545>

Umbach, R., Henry, N., Shelby, R., Stevens, G. & Gonzalez-Pons, K. (2026). AI-generated image-based sexual abuse: Perpetration and consumption across three regions. *Computers in Human Behavior*, 179. <https://doi.org/10.1016/j.chb.2026.108935>