Gender Equality in the Digital Age: Technology-Facilitated Harm as a National and Economic Security Risk

Away from Keyboard Inc.
Shop 4, 115 Anzac Ave., Seymour VIC 3660
0427203595
www.afk.org.au

Women 4 STEM
G.P.O Box 4572, Melbourne 3001, Australia
0407 457 249
https://women4stem.com.au/

Gender Equality in the Digital Age: Technology-Facilitated Harm as a National and Economic Security Risk

Submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade Inquiry: Gender Equality as a National Security and Economic Security Imperative

TABLE OF CONTENTS

Gender Equality in the Digital Age: Technology-Facilitated Harm as a National and Economic Security Risk

Submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade Inquiry: Gender Equality as a National Security and Economic Security Imperative

Executive Summary

Away From Keyboard Inc. (AFK) and Women 4 STEM welcome the opportunity to contribute to this inquiry. This submission sets out evidence that gender equality in the digital age is no longer only a social or economic objective, but a core national security and economic security condition.

Gender equality in the digital age is no longer only a matter of social policy or individual safety. It is now a material determinant of economic security, national resilience, and institutional trust. Digital systems increasingly shape who can participate safely in education, employment, and public life, and who is exposed to harm, exclusion, and exploitation as a condition of engagement.

Technology-facilitated harm now occurs faster, at greater scale, and across more domains than existing safeguards, justice mechanisms, and regulatory frameworks were designed to manage. Digital platforms and emerging technologies influence social norms, gender relations, and access to opportunity in ways that are structural rather than incidental. Women and girls experience disproportionate harm through sexualised abuse, reputational damage, and exclusion from digital and public spaces. At the same time, boys are increasingly shaped by algorithmically amplified misogyny, grievance-based narratives, and hypersexualised content environments that normalise harm and externalise it into schools, communities, and relationships.

Australia is already confronting entrenched levels of violence against women and girls. Technology-facilitated gender-based violence does not emerge in isolation from this context; it intensifies and accelerates existing patterns of harm. Of particular concern is the widespread, largely unrestricted access that boys now have to increasingly graphic, violent, and degrading sexual content through digital platforms and emerging technologies. These environments shape norms, expectations, and behaviours during formative years, normalising sexual entitlement, coercion, and the objectification of women and girls, with foreseeable implications for future harm.

These risks are no longer theoretical. The deployment of large-scale generative artificial intelligence systems has enabled the rapid creation of non-consensual sexualised imagery, including so-called “nudification” of women and girls, as well as the generation of child sexual abuse material. These capabilities are now accessible at speed, at scale, and with minimal technical expertise, often embedded within mainstream digital environments. Once such material is created and distributed, the harm is enduring and cannot be meaningfully reversed through retrospective moderation or takedown mechanisms.

The consequences are cumulative and structural. Technology-facilitated gender-based violence has reached the level of a national crisis, weakening social cohesion not only through direct harm, but through sustained failures to prevent foreseeable abuse. Where individuals experience repeated harm without effective remedy, confidence in institutions responsible for safety, regulation, and justice declines. This erosion of institutional trust constrains participation across education, work, leadership, and civic life, particularly for women and girls who bear disproportionate risk.

The economic risk is not limited to reduced participation. It is also borne in the downstream cost of repairing harm after innovation has occurred without safety-by-design or human-rights-centred governance. Health systems, education providers, employers, justice institutions, and civil society are left to absorb the consequences of preventable harm, while weak or voluntary guidelines allow risks to compound over time. National resilience is eroded when harm consistently outpaces prevention, regulation, and recovery.

International and regional evidence demonstrates that these dynamics are not unique to Australia. United Nations bodies and Asia-Pacific processes have recognised that technology-facilitated gender-based violence, digital exploitation, and the absence of effective justice pathways undermine equality, stability, and recovery, particularly during periods of crisis, instability, and rapid technological change.

This submission proceeds on the basis that Australia has reached a point where inaction carries greater risk than intervention. The evidence of harm is established, the mechanisms are well understood, and the impacts are already observable domestically and internationally. Without prevention-focused, enforceable approaches that recognise digital rights as human rights and integrate gender equality across technology governance, foreign policy, and national security frameworks, digital systems will continue to entrench inequality by default, with long-term consequences for economic participation, social cohesion, and security.

AFK's sustained national and international advocacy across digital safety, technology-facilitated gender-based violence (TFGBV), child protection, and emerging technologies demonstrates that current systems are failing to protect women, girls, and boys from harm occurring at speed and scale. These failures undermine social cohesion, workforce participation, institutional trust, and long-term resilience.

Gender Equality in the Digital Age: Technology-Facilitated Harm as a National and Economic Security Risk

Submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade Inquiry: Gender Equality as a National Security and Economic Security Imperative

About Away from Keyboard Inc. | Women 4 STEM

Away From Keyboard Inc. (AFK) is a registered not-for-profit organisation and charity based in regional Victoria, working at the intersection of digital safety, gender equality, child protection, and emerging technology governance. AFK focuses on identifying and responding to technology-facilitated harm that operates at speed and scale, including technology-facilitated gender-based violence, online sexual exploitation, coercive digital abuse, and the impacts of artificial intelligence and platform design on women, children, and communities.

AFK's work is grounded in policy engagement, regulatory consultation, and evidence-informed advocacy. The organisation has made repeated submissions to Australian parliamentary inquiries, engaged with regulators and government agencies, and contributed to United Nations and Asia–Pacific regional processes examining digital safety, access to justice, and the human rights impacts of emerging technologies.

As a community-based organisation operating outside metropolitan centres, AFK brings a perspective informed by regional experience as well as national and international engagement. This includes direct insight into how digital harms affect individuals, families, schools, and services in regional contexts, where access to specialist support and justice pathways is often more limited.

Through this work, AFK connects individual experiences of harm to systemic governance gaps. Its analysis reflects sustained exposure to how digital harms evolve in practice, how existing safeguards and justice mechanisms fail to keep pace, and how these failures undermine social cohesion, workforce participation, institutional trust, and long-term resilience. AFK's contribution to this inquiry draws on both domestic experience and international evidence, positioning technology-facilitated harm as a structural risk to gender equality, economic security, and national security.

Internationally, there is now consolidated guidance at the highest United Nations level recognising that artificial intelligence and digital systems are being developed and deployed without children's rights at their core, and that existing approaches are insufficient to prevent harm or provide effective remedies.[1] Regional discussions across the Asia-Pacific have similarly identified technology-facilitated violence, exploitation, and the breakdown of justice pathways as shared and accelerating challenges.[3]

Women 4 STEM is a registered not-for-profit organisation and charity focused on advancing women's participation, retention, and leadership across the science, technology, engineering, and mathematics pipeline. Its work is relevant to this inquiry because persistent gender gaps in

STEM education and career pathways shape who has influence over the design, development, and governance of digital and emerging technologies.

Gender disparities within the STEM pipeline are not only an equity concern; they have direct implications for how technological risks are identified and addressed. Where women are under-represented in technical and decision-making roles, the lived experiences and perspectives necessary to anticipate gendered harm are more likely to be absent from system design and governance processes. This increases the likelihood that technologies will be developed without adequate consideration of safety, accountability, and human rights impacts for women and girls.

Women 4 STEM's work in identifying participation gaps, structural barriers, and attrition points across STEM pathways provides insight into the upstream conditions that influence technology outcomes. By strengthening women's access to and continuity within STEM fields, organisations such as Women 4 STEM contribute to closing governance blind spots that allow foreseeable risks to be overlooked or deprioritised.

Recognising the importance of gender equity across the STEM pipeline supports a prevention-focused approach to technology governance. Addressing who participates in building and governing technology is a necessary complement to regulatory and policy measures aimed at responding to harm, and reinforces the need to consider gender equality as integral to risk management in the digital age.

Gender Equality as a National and Economic Security Imperative

Gender equality underpins national security and economic security because it determines who can participate safely, contribute productively, and engage fully in social and civic life. In the digital age, access to safe online environments and equitable participation in technology-related education and work have become practical requirements for education, employment, democratic participation, and access to essential services.[1 7]

Where women and girls are routinely exposed to technology-facilitated abuse, sexualisation, and reputational harm, participation declines. This withdrawal is not the result of individual preference, but of sustained exposure to environments where harm is persistent, foreseeable, and insufficiently addressed. Over time, this constrains workforce participation, leadership pathways, and public engagement, with broader implications for productivity, innovation capacity, and social cohesion.[1 2]

These risks intersect directly with the STEM education and workforce pipeline. Persistent gender gaps in STEM participation emerge early and compound over time, limiting the pool of

women able to shape, govern, and lead in the development of digital and emerging technologies. Evidence from the *STEM Equity Report 2025* demonstrates that women remain significantly underrepresented across Australia's STEM workforce, with particularly acute gaps in information technology, engineering, and senior leadership roles.[7] These gaps are not merely an equity concern; they represent a structural vulnerability in Australia's capacity to anticipate and mitigate gendered risk in technology systems.

At the same time, digital platforms are shaping the socialisation of boys in ways that carry long-term security implications. Algorithmic systems increasingly amplify misogyny, grievance-based narratives, and hypersexualised content, often without meaningful safeguards. These environments normalise harmful gender norms and increase vulnerability to exploitation, coercion, and radicalisation, with impacts that extend beyond the digital sphere into schools, communities, and relationships.[1] [2]

Ensuring that more girls can enter, remain, and progress through STEM pathways is therefore a national imperative. Without deliberate intervention to address pipeline attrition, Australia risks entrenching a technology ecosystem in which systems are designed and governed without sufficient gender diversity, increasing the likelihood that foreseeable harms to women and girls are overlooked or deprioritised. The long-term effect is not only reduced participation, but weakened institutional trust, diminished resilience, and heightened exposure to technology-facilitated harm.[1] [7]

Together, these dynamics undermine trust in institutions responsible for safety, regulation, and justice. A society in which large segments of the population cannot safely engage in the digital environments that underpin economic and civic life, or meaningfully participate in shaping the technologies that govern those environments, is less resilient and more exposed to instability.[1]

Evidence Linking Gender Equality, Economic Growth, and Prosperity

The links between gender equality and economic growth are well established. Less well examined is the role of technology-facilitated harm as a structural driver of economic exclusion, insecurity, and long-term productivity loss in a digital economy.

Digital harm can remove individuals from education, training, and employment pathways rapidly, with effects that persist long after the initial incident. Women and girls who experience sustained online abuse, sexualised harm, or reputational damage frequently disengage from digital platforms that are now integral to recruitment, professional networking, entrepreneurship, education delivery, and access to services. This disengagement represents

lost opportunity not only for individuals, but for the broader economy, particularly as digital participation becomes a prerequisite for labour market access.[1]

The economic costs associated with technology-facilitated harm extend beyond lost income or short-term productivity. Recovery often involves unpaid emotional labour, care responsibilities, health impacts, and financial burden borne by individuals, families, employers, and community organisations. These costs are rarely captured in labour market or productivity data, yet they directly affect workforce participation, retention, and long-term economic security. Where harm is persistent or unresolved, it can permanently alter education and career trajectories, particularly for women and girls.[1]

Technology-facilitated harm also intersects with existing gender disparities in education and workforce participation. Evidence demonstrates that attrition from digital and STEM-related pathways compounds over time, reducing the pool of women available to participate in and lead high-growth, technology-intensive sectors. This loss of capability has long-term implications for innovation capacity, economic diversification, and the ability to identify and mitigate risk in emerging technology systems.[7]

International and regional data relating to online exploitation, sexual extortion, and scam activity further demonstrate that digital coercion increasingly occurs within compressed timeframes, often unfolding faster than reporting, enforcement, or support mechanisms can respond. United Nations reporting and global scam intelligence have recognised that these harms are not limited to isolated incidents or direct interactions with technology, but arise from systemic features of digital ecosystems that enable rapid targeting, anonymity, and scale.[1] [4] The economic impact of such harm is amplified where prevention is weak and recovery mechanisms are slow or inaccessible.

Economic growth therefore depends not only on access to opportunity, but on the conditions that allow people to participate without disproportionate risk. Where digital environments function as sites of predictable harm rather than safe participation, exclusion deepens, confidence declines, and economic security is weakened. Addressing technology-facilitated harm is consequently not ancillary to economic policy, but integral to sustaining inclusive growth and long-term prosperity in a digital economy.[1]

National and International Security Implications, Including Crises and Climate

Technology-facilitated harm now presents a material risk to national and international security because it operates across borders, scales rapidly, and undermines social cohesion, institutional trust, and access to justice. These risks are magnified during periods of crisis, instability, and environmental disruption, when safeguards weaken and reliance on digital systems increases.[1]

International and regional evidence demonstrates that technology-facilitated gender-based violence, online exploitation, and digital coercion intensify during humanitarian emergencies, climate-related disasters, and conflict-adjacent contexts. Digital platforms enable rapid targeting of individuals who are displaced, isolated, or economically stressed, often beyond effective jurisdiction or timely intervention.[1] [2]

Recent discussions across the Asia-Pacific region in United Nations-led forums have identified the absence of effective justice pathways for technology-facilitated harm as a shared and accelerating concern. Participants consistently noted that digital transformation is proceeding faster than legal, regulatory, and institutional systems can adapt, with no established best-practice model globally for preventing harm or delivering remedies at scale.[3] This gap has direct implications for stability, recovery, and trust in institutions during and after crises.

Domestic governance analysis further illustrates how system design failures contribute to foreseeable harm. Independent assessment of Australia's proposed Scam Prevention Framework identifies significant delays in implementation, limited coverage, weak obligations on digital businesses, and fragmented dispute-resolution mechanisms for victims. Major digital environments, including social media platforms, dating applications, gaming platforms, app stores, and online marketplaces, remain excluded from coverage, despite being recognised as high-risk channels for harm.[4]

These exclusions do not operate in a neutral manner. The absence of safeguards in high-risk digital environments disproportionately exposes women and girls to sexualised abuse, exploitation, and reputational harm, while also leaving boys vulnerable to grooming, coercion, and scam-linked sexual extortion. Where perpetrators are anonymous, offshore, or automated, and remedies are delayed or inaccessible, harm compounds and confidence in institutions responsible for protection and justice erodes.[1] [4]

The delayed implementation of protective frameworks further amplifies risk. In digital environments where harm occurs repeatedly and within compressed timeframes, prolonged policy delay functions as a risk multiplier. Each year of inaction entrenches exposure,

normalises harm, and transfers the burden of prevention and recovery onto individuals, families, and civil society.[4]

From a national security perspective, these dynamics undermine resilience by weakening social cohesion, reducing trust in institutions responsible for protection and justice, and constraining participation in education, work, and civic life. Internationally, they contribute to instability by exacerbating inequality, enabling exploitation across borders, and complicating humanitarian response and recovery efforts.[1] [2]

Technology-facilitated harm should therefore be understood not only as a safety or consumer protection issue, but as a cross-cutting security risk that intersects with crisis response, climate resilience, and international stability. Without timely, enforceable, and prevention-focused intervention, digital systems will continue to generate and amplify harm in ways that undermine equality, security, and recovery at both national and international levels.[1] [2] [3] [4]

Locally-Led Leadership and Decision Making

Locally led organisations, community groups, and civil society actors play a critical role in identifying emerging harms, supporting victim-survivors, and responding to technology-facilitated violence in real time. These organisations are often the first to detect new patterns of abuse, exploitation, and system failure, particularly where harms affect women, children, and marginalised communities.

However, in the context of digital harm and emerging technologies, locally led leadership is increasingly required to compensate for ethical and governance failures upstream, rather than complement effective regulation. Civil society organisations are left to absorb the consequences of platform and system design decisions made without human-rights-centred safeguards, while lacking access to the data, authority, or resources required to prevent harm at scale.

The absence of binding international standards, interoperable regulatory frameworks, and enforceable safety-by-design obligations means that the risks associated with emerging technologies are not hypothetical; they are real, foreseeable, and unevenly managed. In this vacuum, the onus is placed on individual businesses to determine what constitutes “ethical” deployment, often without clear benchmarks, shared accountability, or consistent oversight.

While many organisations express a genuine intent to deploy artificial intelligence responsibly, evidence indicates that ethical commitments are frequently aspirational rather than operational. Without clear human-rights-centred standards and regulatory alignment, ethical decision-making is shaped by commercial pressure, speed to market, and competitive

advantage, rather than by the protection of women, children, and vulnerable communities. This results in inconsistent safeguards, fragmented accountability, and preventable harm.

Reliance on voluntary ethics frameworks or self-assessment models is insufficient where technologies have the capacity to automate and scale harm. In the absence of enforceable standards, businesses that seek to act responsibly are disadvantaged, while those that externalise risk face limited consequences. This regulatory gap contributes directly to the burden placed on civil society and locally led organisations, who are left to respond to harm after it has occurred rather than preventing it at source.

A growing concern is the gap between how organisations perceive their use of artificial intelligence as "ethical" and the reality of how these systems operate in practice. Australian research on responsible AI maturity demonstrates that while many organisations believe they are deploying AI responsibly, the majority remain at low to moderate levels of ethical maturity, with limited implementation of safeguards related to safety, accountability, contestability, and human oversight. This disconnect means that risks to women, children, and vulnerable communities are often not identified or mitigated until harm has already occurred.[6]

Ethical intent cannot substitute for enforceable standards where the consequences of failure involve sexual violence, exploitation, and violations of fundamental human rights.

Where human rights are treated as secondary considerations, applied after deployment rather than embedded at the point of design, AI systems can automate and scale harm, including technology-facilitated gender-based violence, non-consensual sexualised imagery, sexual extortion, and the creation of child sexual abuse material. Evidence from Australia's online safety regulator demonstrates that even where detection tools exist, they are unevenly deployed, inconsistently applied, and frequently reliant on user reporting rather than proactive prevention, placing the burden of safety on those most at risk. [5]

The result is a systemic transfer of responsibility. Victim-survivors, families, educators, health services, and community organisations are expected to manage the consequences of harms generated by technologies deployed without adequate ethical foresight or enforceable standards. This model deepens inequity, strains local capacity, and erodes trust in institutions responsible for safeguarding the public.

Recognising and supporting locally led leadership therefore requires addressing the upstream ethical conditions that generate harm. Consultation and community response alone are insufficient. Sustainable leadership depends on enforceable safety-by-design obligations, transparency requirements, and governance frameworks that treat digital rights as human

rights. Without systemic reform, community-based responses risk becoming permanent substitutes for effective regulation, rather than partners in a resilient, rights-centred digital governance framework.

Decision-making is further constrained when governments continue to rely on digital platforms that have demonstrably failed to prevent harm to women and children at scale. Official use of such platforms is not a neutral communications choice; it confers institutional legitimacy and signals tolerance of governance models that prioritise reach and engagement over safety, accountability, and human rights.

Where governments maintain an active presence on platforms associated with systemic technology-facilitated gender-based violence, non-consensual sexualised imagery, or risks of child sexual exploitation, this creates a tension between stated policy commitments and operational practice. It undermines public confidence in regulatory intent, weakens ethical leadership, and complicates efforts to demand higher standards from industry.

Away From Keyboard Inc. has raised these concerns formally with the Australian Government, noting that continued government use of platforms lacking robust, enforceable safeguards constrains the ability to take principled positions on prevention, safety-by-design, and human-rights-centred technology governance. Leadership in this context requires governments to align their own practices with the standards they seek to impose, recognising that government communications choices set norms and expectations across the digital ecosystem.

Australian Government Efforts to Advance Gender Equality

The Australian Government has articulated strong commitments to advancing gender equality and protecting the human rights of women and girls across foreign policy, defence, national security, and digital governance. These commitments are reflected in strategies addressing violence against women, online safety, artificial intelligence, and Australia's engagement with international human rights frameworks.

However, there remains a significant gap between policy intent and operational outcomes in the digital environment. Technology-facilitated gender-based violence, non-consensual sexualised imagery, sexual extortion, and AI-enabled exploitation continue to occur at scale, indicating that existing approaches have not yet translated into effective prevention or meaningful reduction of harm.

Current government responses remain heavily weighted towards post-harm intervention, user reporting, and voluntary or principles-based industry compliance. While these measures have a role, they are structurally ill-suited to address harms that occur rapidly, anonymously, and

across borders, particularly where perpetrators are unknown, automated, or offshore. In such contexts, reliance on reporting and takedown mechanisms places the burden of safety and recovery on those experiencing harm, rather than on the systems that enable it.[16]

There is also a growing inconsistency between Australia's policy commitments and aspects of its operational practice. Continued government reliance on digital platforms associated with persistent harm to women and children undermines the credibility of safety-by-design and human-rights-centred governance objectives. Where governments engage with or depend on platforms that lack robust, enforceable safeguards, it weakens the capacity to demand higher standards from industry and erodes public trust in regulatory intent.

Efforts to promote responsible and ethical use of artificial intelligence further illustrate these challenges. Evidence indicates that while many organisations, including those engaging with government, believe they are deploying AI responsibly, ethical maturity remains uneven, with limited integration of human rights impact assessment, accountability, contestability, and safety-by-design. Without clear, enforceable standards and regulatory alignment, ethical commitments remain aspirational, and foreseeable risks to women, girls, and children are insufficiently mitigated.[6]

From a governance perspective, the absence of binding international standards and interoperable regulatory frameworks places disproportionate responsibility on individual businesses to self-regulate. This approach creates uneven protections, rewards risk externalisation, and disadvantages organisations that seek to act responsibly. It also shifts the downstream costs of harm onto individuals, families, public services, and civil society, rather than addressing risk at source.

Advancing gender equality and the human rights of women and girls in the digital age therefore requires a shift from reactive and voluntary approaches towards prevention-focused, enforceable governance. This includes embedding human rights as a foundational requirement in technology design, deployment, procurement, and regulation; aligning government practice with stated policy commitments; and ensuring that accountability mechanisms operate effectively even where harm is automated, anonymous, or transnational.

Without this shift, government efforts, however well intentioned, risk reinforcing a system in which harm is managed after the fact rather than prevented, and where gender inequality is reproduced by default through digital systems that operate beyond effective oversight.

Women, Peace and Security Agenda and Australia's Role

The Women, Peace and Security (WPS) agenda remains a critical framework for advancing gender equality, protecting women and girls, and strengthening peace and security outcomes globally. However, the nature of threats affecting women, girls, and communities has evolved significantly since the adoption of the WPS agenda, requiring its practical implementation to adapt to contemporary realities.

Technology-facilitated gender-based violence, digital exploitation, online coercion, and AI-enabled abuse now operate across borders, at speed, and with limited accountability. These harms undermine the core objectives of WPS by restricting participation, eroding trust, and exacerbating insecurity, particularly in fragile, crisis-affected, and digitally dependent contexts. Where digital systems amplify misogyny, sexual violence, and exploitation, they weaken peacebuilding efforts and compromise recovery, stability, and resilience.

Recent discussions convened by the United Nations Economic and Social Commission for Asia and the Pacific (UN ESCAP), including regional briefings held in preparation for the 70th Commission on the Status of Women, have highlighted shared concerns across the region regarding technology-facilitated harm, the absence of effective justice pathways, and the disproportionate impact of digital transformation on women and girls. Participants consistently identified that digital harms are escalating faster than legal, regulatory, and institutional systems can respond, creating gaps in protection that undermine equality, trust, and security across diverse national contexts.[3]

These regional findings reinforce international human rights assessments that emerging technologies, when deployed without safeguards, can entrench inequality and enable new forms of violence. In this context, failure to integrate digital harm and emerging technology governance into WPS implementation risks leaving the agenda operationally incomplete, despite its continued conceptual relevance.

Australia has consistently positioned itself as a supporter of the WPS agenda and as a proponent of gender equality in foreign policy and international engagement. This creates both an opportunity and a responsibility to demonstrate leadership in addressing technology-facilitated harms as part of contemporary security challenges. Aligning WPS implementation with regional evidence emerging through UN ESCAP processes would strengthen Australia's credibility and enhance the effectiveness of its international engagement.

Meaningful leadership in this area requires recognising that digital environments are now central to conflict dynamics, humanitarian response, civic participation, and access to

services. Where women and girls are excluded from these environments due to risk, or where digital systems are used to target, exploit, or silence them, peace and security outcomes are directly compromised. Similarly, the exposure of boys and young men to unregulated digital ecosystems that normalise misogyny and violence carries long-term implications for social stability and gender relations in post-conflict and crisis settings.

Australia's international engagement through development assistance, diplomatic channels, and multilateral forums, therefore, presents an opportunity to advocate for human-rights-centred technology governance as a core component of WPS. This includes prevention-by-design, access to justice for technology-facilitated harm, and safeguards addressing AI-enabled exploitation and digital coercion.

Without such integration, WPS risks being implemented in a manner that does not fully account for the mechanisms through which contemporary harm is produced and sustained. Updating WPS practice to reflect digital realities would strengthen its relevance, protect hard-won gains in gender equality, and reinforce the agenda's contribution to peace, security, and resilience in an increasingly technologised world.

Related Matters: Emerging Technologies and Human Rights–Centred Risk

Emerging technologies, including artificial intelligence, algorithmic recommender systems, and generative tools, should not be understood as secondary or incidental contributors to gender inequality and harm. Where these technologies are developed and deployed without human rights at their core, they function as primary drivers of harm, shaping social norms, amplifying inequality, and constraining access to justice at scale.[1]

International human rights mechanisms have made clear that most AI systems in use today are not designed with the rights, safety, or wellbeing of children and women as foundational requirements. Instead, they are optimised for engagement, growth, and automation, with foreseeable consequences for exposure to sexualised content, technology-facilitated gender-based violence, exploitation, and the erosion of effective remedies.[1]

Evidence now demonstrates that these risks are not theoretical. International monitoring has identified a rapid escalation in AI-generated child sexual abuse material, with thousands of AI-generated abuse videos identified in a single year and a significant proportion classified at the most severe legal level. This demonstrates how emerging technologies, when deployed without human rights safeguards, can accelerate harm at a scale that overwhelms existing detection, prevention, and justice mechanisms.[5]

Critically, harm arising from emerging technologies often occurs without a clearly identifiable perpetrator. Automation, anonymity, cross-border deployment, and opaque system design undermine traditional justice pathways that rely on attribution and individual culpability. Where human rights safeguards are not embedded upstream in technology design, governance, and deployment, accountability is deferred until after harm has occurred, if it occurs at all.

For these reasons, emerging technologies must be understood as a foundational governance issue for gender equality, child protection, economic participation, and national resilience. Treating technology risk as secondary or downstream fails to address the structural conditions that allow harm to be produced, replicated, and normalised at speed and scale.

Across all Terms of Reference, AFK and Women 4 STEM identifies three compounding risks:

1. Velocity: harm now occurs faster than justice and safeguarding systems can respond.
2. Scale: technology enables mass replication and persistence of abuse.
3. Weaponisation: platforms shape gendered norms that amplify harm to girls while exposing boys to coercive and misogynistic ecosystems.

These risks are already evidenced internationally and domestically. Failure to intervene will, by design, entrench inequality and insecurity.

Conclusion

This inquiry comes at a critical moment. Gender equality in the digital age is no longer separable from questions of national security, economic security, and Australia's standing as a credible international actor. Technology-facilitated gender-based violence, AI-enabled exploitation, and digital coercion now operate across borders, at speed, and with limited accountability, undermining social cohesion, institutional trust, and participation in economic and civic life.[1] [2]

The evidence presented in this submission demonstrates that these harms are foreseeable outcomes of governance choices, not unintended side effects of innovation. Where emerging technologies are developed and deployed without human-rights-centred design, safety-by-design obligations, and enforceable accountability, harm is produced and scaled by default. The cumulative effect is borne not only by women and girls, but by communities, public institutions, and systems responsible for education, health, justice, and recovery.

Australia is not confronting these challenges in isolation. International human rights mechanisms, regional UN processes, and comparable jurisdictions are grappling with the same risks and reaching similar conclusions: voluntary standards and post-harm responses are insufficient in the face of automated, anonymous, and transnational digital harm. In this context, Australia's foreign policy, defence posture, and international engagement have an important role to play in shaping norms, expectations, and governance responses.

The National AI Plan and Australia's commitments under the Women, Peace and Security agenda provide an opportunity to demonstrate leadership. Their effectiveness, however, will depend on whether human rights, particularly the rights of women and children, are treated as foundational constraints on technology development and deployment, rather than as secondary considerations addressed after harm has occurred.

This submission does not call for the abandonment of innovation. It calls for coherence, foresight, and leadership. By aligning domestic practice with international advocacy, embedding human rights at the centre of technology governance, and recognising technology-facilitated gender-based violence as a strategic risk, Australia can strengthen its security, resilience, and credibility in an increasingly technologised world.

Recommendations

Away From Keyboard Inc. and Women 4 STEM respectfully recommend that the Committee consider the following within its foreign affairs, defence, trade, and national security remit:

1. **Recognise technology-facilitated gender-based violence as a national security and economic security risk**, including its impacts on social cohesion, institutional trust, workforce participation, and long-term resilience, particularly in the context of emerging technologies and artificial intelligence.
2. **Ensure Australia's foreign policy, defence, and national security settings integrate human-rights-centred technology governance**, including explicit consideration of the gendered and child-specific risks associated with artificial intelligence and digital platforms.
3. **Assess the National AI Plan through a national security and international engagement lens**, ensuring its implementation supports Australia's obligations under international human rights law, advances gender equality, and addresses foreseeable risks arising from AI-enabled exploitation, technology-facilitated violence, and digital coercion.
4. **Support Australia's leadership in international and regional forums**, including through DFAT engagement with United Nations processes such as the Women, Peace and Security agenda and UN ESCAP, to promote prevention-focused, human-rights-centred approaches to emerging technologies.
5. **Encourage coherence between Australia's domestic commitments and international advocacy**, recognising that government operational practice, procurement, and digital engagement choices shape Australia's credibility and influence in promoting safe, ethical, and rights-respecting technology governance globally.
6. **Promote the integration of digital and emerging technology risks into the Women, Peace and Security agenda**, recognising that technology-facilitated harm undermines peacebuilding, humanitarian response, and recovery, and disproportionately affects women, girls, and vulnerable communities.
7. **Acknowledge the limits of voluntary and principles-based approaches in international technology governance**, and consider how Australia can contribute to

the development of interoperable standards, norms, and accountability mechanisms that reduce reliance on civil society to absorb the consequences of preventable harm.

Sarah Barnbrook
Founder & CEO, Away from Keyboard Inc.

Mary-Beth Hosking
CEO, Women 4 STEM

REFERENCES

1. **Human rights, children's rights, sexual exploitation, and digital systems**
   Human Rights Council, Protecting children from sale, sexual exploitation and sexual abuse: progress, new frontiers and the path forward (Report of the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children).
   Human Rights Council, Visit to Australia (Report of the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children).
   Joint Statement, Artificial Intelligence and the Rights of the Child (United Nations system-level statement).
   Global Anti-Scam Alliance, The Global State of Scams.
   United Nations Human Rights Council, thematic materials on children, digital environments, and protection from sexual exploitation and abuse.

2. **Gender equality, misogyny, sexualisation, and technology-facilitated gender-based violence**
   UN Women, materials on technology-facilitated gender-based violence.
   United Nations Development Programme, materials on gender equality and digital transformation.
   Collective Shout, Turning Women and Girls into Porn.
   Away From Keyboard Inc., Why Safety by Design Matters for Women and Children in a Digital World.

3. **Asia–Pacific regional evidence and UN ESCAP processes**
   United Nations Economic and Social Commission for Asia and the Pacific, CSW70 Asia–Pacific Regional Briefings.
   Asia-Pacific Development, Diplomacy & Defence Dialogue, materials on gender, technology, and regional security.

   Soroptimist International South East Asia Pacific briefings and materials.

4. **Scam, sextortion, system design failure, and economic harm**
   Australian Government, Scam Prevention Framework.
   Resolver, Weaponised Loneliness: Critical Harm Intelligence Briefing.
   Australian Government, Australian Responsible AI Index 2025.

5. **AI-enabled sexual exploitation, image-based abuse, and child sexual abuse material**
   Internet Watch Foundation, materials on AI-generated child sexual abuse material.

BOSE, Child Sexual Exploitation and Sexual Extortion Periodic Notices.
Australian online safety regulator, materials on image-based abuse and online exploitation.
Harm, Progress and Addiction.

6. **Artificial intelligence governance, ethics, and institutional maturity**

Australian Government, National AI Plan.
International Association on Ethical Artificial Intelligence, governance and ethics materials.
Women in AI Governance and Human Rights Committee, briefing materials.

7. **Civil society advocacy and policy engagement**

Away From Keyboard Inc., submissions and correspondence to the Australian Government.
Away From Keyboard Inc., Submission to the Senate.
Away From Keyboard Inc., letters to the Prime Minister.
Soroptimist International, briefing materials.
Commonwealth Women's Network, briefing materials.

Women 4 STEM, STEM Equity Report