

Research & Policy

WomanACT Submission to
Innovation, Science and Economic
Development Canada:
**Enhancing Trust in Artificial
Intelligence Through Increased
Transparency**

September 23, 2026



WomanACT



Submission to Innovation, Science and Economic Development Canada

Enhancing Trust in Artificial Intelligence Through Increased Transparency

Submitted by WomanACT
September 23rd, 2026

About WomanACT

WomanACT is a Toronto-based charitable organization working to end gender-based violence (GBV) and advance gender equity through systems change, education, research, policy advocacy, and community mobilization. Our work is grounded in survivor-centred, trauma-informed, anti-racist, and anti-oppressive approaches.

WomanACT welcomes the Government of Canada's consultation on enhancing trust in artificial intelligence (AI) through increased transparency. We strongly support the Government's recognition in *Canada's National Artificial Intelligence Strategy: AI for All* that protecting Canadians and safeguarding democracy must be a central pillar of Canada's AI strategy¹. AI is rapidly changing how we work, communicate, and access services, but it is also creating new risks for survivors of GBV². Canada's AI strategy needs to be able to address new risks associated with tech-facilitated gender-based violence (TFGBV), from non-consensual sexualized deepfakes to AI-enabled harassment, fraud, coercive control, privacy harms, online violence, and algorithmic bias.

Our submission focuses on a critical gap in AI transparency discussions: the gendered and intersectional impacts of AI and the ways AI can facilitate, intensify, and normalize gender-based violence.

Our recommendations draw on WomanACT's policy and research work, feedback collected from WomanACT members through a targeted consultation, and emerging Canadian and international research and policy analysis.

¹ <https://ised-isde.canada.ca/site/ised/en/canadas-national-artificial-intelligence-strategy-ai-all>

² <https://ised-isde.canada.ca/site/ised/en/have-your-say-advancing-ai-transparency-canada/enhancing-trust-artificial-intelligence-through-increased-transparency>



Executive Summary

Artificial intelligence is not gender-neutral³. AI systems are developed and deployed within existing social, economic, and institutional systems that contain gender inequality⁴, racism, ableism, misogyny, and other forms of discrimination. As AI becomes embedded across social services, healthcare, housing, employment, financial services, policing, education, online platforms, and everyday communications, these systems can influence how survivors are understood, assessed, treated, and supported.

For survivors of gender-based violence, the consequences can be particularly significant. AI can facilitate non-consensual sexualized deepfakes, image-based abuse, impersonation, stalking, surveillance, harassment, coercive control, and automated abuse. It can also introduce less visible harms when algorithmic systems influence risk assessments, eligibility decisions, service access, credibility assessments, or other consequential decisions affecting survivors.

Canada's *AI for All* strategy appropriately recognizes that deepfakes are already being used as a form of sexual violence, particularly against women, girls, and gender-diverse people, and that algorithmic bias can harm vulnerable communities. The current ISED consultation provides an important opportunity to translate this recognition into concrete transparency requirements.

WomanACT's consultation with frontline GBV organizations, survivors, and sector professionals found strong support for clear AI labelling and provenance requirements, mandatory platform accountability and rapid-removal mechanisms, safety-by-design obligations on developers, standardized and disaggregated incident tracking, and a national AI literacy initiative that addresses digital consent, manipulation, and coercion, not just how to spot AI-generated content. Responsibility must be shared across the AI value chain, and the burden of identifying and managing AI-related harm must not fall on survivors. WomanACT recommends that Canada adopt a gender-responsive, intersectional, and trauma-informed approach to AI transparency, anchored in an overarching AI and Violence Prevention Framework developed with meaningful involvement from the GBV sector and survivors.

Background: AI and the Escalation of Technology-Facilitated GBV (TFGBV)

Technology-facilitated gender-based violence (TFGBV), including image-based abuse, stalking, surveillance, and coercive control carried out or intensified through digital tools, is not new⁵. What has changed is scale and accessibility. Generative AI now allows perpetrators to fabricate sexualized images and videos of real people, clone voices, sustain automated grooming or harassment campaigns, and monitor survivors with a precision that was previously unavailable outside specialized surveillance tools. LEAF's *AI and Gender-Based Violence* explainer emphasizes that creating sexualized synthetic content of a person without their consent violates their integrity and

³ https://wp.oecd.ai/app/uploads/2025/05/towards-substantive-equality-in-artificial-intelligence_Transformative-AI-policy-for-gender-equality-and-diversity.pdf

⁴ <https://news.un.org/en/story/2026/06/1167776>

⁵ <https://techsafety.ca/resources/toolkits/what-is-technology-facilitated-gender-based-violence/>



autonomy⁶. It also documents the significant psychological, social, reputational, educational, and financial harms associated with this form of abuse⁷.

AI systems are trained on and operate within a digital environment already saturated with misogyny, racism, and harmful narratives about violence and survivors, and without deliberate intervention, they risk reproducing and scaling these biases rather than correcting them⁸.

Why Transparency in AI Matters for GBV

- **Sexualized deepfakes and non-consensual imagery:** AI has dramatically lowered the skill and cost required to fabricate convincing intimate imagery of real people without consent, with serious psychological, reputational, economic, and safety consequences for those targeted⁹.
- **AI incidents:** GBV-related AI harms are currently absorbed into broader categories such as "online harms" or "cybercrime," obscuring their scale, gendered nature, and the patterns needed to prevent them.
- **Coercive control:** AI-enabled location tracking, device monitoring, account access, and automated messaging are making surveillance and coercive control more sophisticated, persistent, and harder for survivors to detect or escape.
- **Gendered and intersectional harms:** A gender-neutral approach to AI transparency will miss how these harms disproportionately affect women, girls, and gender-diverse people, and how Indigeneity, race, disability, sexuality, gender identity and expression, immigration status, age and socio-economic status compound risk. Transparency measures must be designed with an intersectional lens from the outset, not retrofitted¹⁰.
- **Economic and financial abuse:** AI is lowering the barrier to voice-cloning and impersonation fraud, unauthorized access to survivors' financial accounts, and manipulation of benefit, credit, tenancy and hiring decisions through opaque algorithmic systems¹¹. These harms deepen the economic dependency that keeps survivors trapped and undermine their ability to leave and rebuild¹².

⁶ <https://www.leaf.ca/factsheet/ai-and-gender-based-violence/>

⁷ <https://www.leaf.ca/factsheet/ai-and-gender-based-violence/>

⁸ https://wp.oecd.ai/app/uploads/2025/05/towards-substantive-equality-in-artificial-intelligence_Transformative-AI-policy-for-gender-equality-and-diversity.pdf

⁹ <https://techsafety.ca/resources/toolkits/what-is-technology-facilitated-gender-based-violence/>

¹⁰ https://www.researchgate.net/publication/414089985_Digital_Harassment_Against_Women_Need_for_a_Gender-Sensitive_Legal_Framework

¹¹ <https://womanact.ca/publications/innovative-practices-for-identifying-and-responding-to-tech-facilitated-financial-abuse/>

¹² <https://womanact.ca/publications/infographic-economic-and-financial-abuse-key-terms/>



Recognizing Positive Legislative Momentum

WomanACT recognizes and welcomes emerging Canadian legislative efforts that reflect growing recognition of these harms. Bill C-16, the Protecting Victims Act, received Royal Assent on June 18, 2026¹³, creating new Criminal Code offences for coercive or controlling conduct in intimate relationships and for threatening to distribute non-consensual intimate images, including AI-generated sexual deepfakes¹⁴. Bill C-34, the Safe Social Media Act, introduced in June 2026, proposes a Digital Safety Act that would extend safety and transparency duties to social media platforms and AI chatbot services¹⁵. This momentum is an important foundation. Its impact, however, will depend on consistent enforcement, adequate resources, and accessible mechanisms for survivors to obtain protection and remedy — recognition in law is necessary but not sufficient.

WomanACT also notes that criminal law is not an accessible or safe pathway for every survivor. Indigenous, Black, and racialized survivors, survivors with precarious immigration status and 2SLGBTQ+ survivors may face significant risks in engaging with police and courts, and many survivors do not want a criminal justice response. AI transparency, reporting and removal mechanisms must therefore operate independently of criminal proceedings and civil, administrative, and platform-based remedies must be available to survivors without requiring them to contact police or disclose their immigration status.

What We Heard From Our Members

WomanACT surveyed frontline GBV professionals, survivor-engagement participants, and sector partners on AI transparency. Members consistently identified deepfakes, AI-enabled surveillance and account hacking, and AI-generated harassment as active, present-day risks. Several respondents described being unable to find any service, including police, equipped to respond when a survivor's accounts or devices were being monitored using AI-enabled tools.

Recurring themes included:

- The need for clear, prominent labelling of AI-generated or altered content, paired with fast (24–48 hour) removal processes and digital fingerprinting/hashing to prevent re-upload of harmful content.
- Mandatory disclosure whenever a person interacts with AI, including what data is collected, whether it trains future models, and who can access it.
- Safety-by-design obligations on developers, including content-moderation filters that block attempts to generate non-consensual sexual content of real people.

¹³ <https://www.parl.ca/documentviewer/en/45-1/bill/C-16/royal-assent>

¹⁴ Department of Justice Canada, [“Major Criminal Code reforms to protect Canadians are now law,”](#) news release, July 7, 2026. Bill C-16, the Protecting Victims Act, received Royal Assent on June 18, 2026.

¹⁵ Department of Canadian Heritage, [“Bill C-34, the Safe Social Media Act,”](#) Government of Canada, introduced June 10, 2026 (as of this submission, Bill C-34 has not yet received Royal Assent).



- Federal civil remedies giving survivors direct legal recourse for unauthorized use of their image, voice, or likeness, without relying solely on criminal prosecution.
- Practical AI guidance for GBV/VAW professionals — covering both risks to clients and responsible use of AI in their own practice.
- AI and technology-facilitated GBV education embedded in school curricula, addressing consent, manipulation, and where to seek help.

Recommendations

WomanACT recommends that the Government of Canada:

- **Establish mandatory, gender-responsive transparency and safety requirements for AI-generated and AI-modified content.**
Require clear, prominent and accessible labelling, supported by interoperable provenance, metadata and watermarking standards. For sexualized synthetic content, transparency must be accompanied by prevention, rapid removal, evidence preservation, re-upload prevention and accessible remedies. Responsibility for prevention and action should rest primarily with developers, deployers and platform regulators, not individuals or survivors. Detection, hashing, filtering and identity or age verification tools must themselves be designed with a survivor-safety lens: they must not create new surveillance infrastructure, compromise the anonymity and privacy that survivors rely on to stay safe online, or over-remove survivors' own disclosures, advocacy and educational content about GBV.
- **Require meaningful disclosure and human accountability wherever AI interacts with or affects people.**
AI use should be disclosed prominently whenever it informs communication, service delivery, assessment, classification or decision-making, with enhanced requirements in high-impact contexts such as child welfare, immigration, family court, healthcare, housing, employment, financial services, policing, social services and GBV services. Disclosure obligations must go beyond terms-of-service and privacy-policy language. AI should not replace qualified human judgment in decisions affecting survivor safety, rights or access to essential services, and individuals should have meaningful avenues for human review and appeal.
- **Require transparency across the AI lifecycle, including gender-responsive and intersectional impact assessment.**
Developers and deployers should provide meaningful information about training data, data sources and limitations, known biases, privacy and retention practices, system capabilities and failure modes, intended uses, and governance and accountability arrangements. Systems should undergo ongoing gender-responsive and intersectional testing that considers GBV, discrimination, privacy, surveillance, coercive control and differential impacts on marginalized communities.
- **Establish a complementary national framework for identifying, reporting and monitoring AI-facilitated gender-based violence.**
Canada should recognize AI-facilitated GBV as a distinct and evolving category of technology-facilitated GBV, with standardized incident categories and reporting requirements covering sexualized deepfakes, non-consensual intimate imagery, harassment, threats, impersonation, stalking, surveillance, coercive



control and other emerging harms. Reporting should capture cumulative, psychological, reputational, privacy, economic and safety harms, not only physical or financial impacts, and include near misses and emerging risks.

- **Create coordinated, privacy-protective mechanisms for incident reporting, data collection and accountability.**

Government should bring together developers, platforms, researchers, GBV organizations and people with lived experience to identify emerging harms and systemic risks. Platforms and developers should report relevant information on complaints, response and removal times, repeat uploads, detection effectiveness and remedies. Data collection must protect survivor privacy, minimize identifying information and ensure that survivors are not made responsible for documenting or repeatedly reporting harms. GBV organizations, researchers, and survivors with lived experience must be meaningfully and continuously involved in designing AI transparency standards, incident-reporting frameworks, and safety-by-design requirements, not consulted only after systems are built. Disaggregated data on AI-facilitated GBV must be governed by clear limits on use: it must never be repurposed for immigrant enforcement, policing, or surveillance of the communities it describes.

- **Embed safety-by-design and violence prevention framework into Canada's AI governance strategy.**

Canada should move beyond reactive disclosure and incident response by requiring developers and deployers to identify and mitigate foreseeable harms throughout the AI lifecycle. This should include gender-responsive impact assessments, safety testing, safeguards against misuse, incident monitoring, enforcement, survivor support and public education, accessible reporting and removal mechanisms, and clear accountability for high-risk applications. Existing international Safety by Design approaches used in the [UK](#) and [Australia](#) provide useful models that Canada can adapt to its context.

- **Invest in AI literacy and capacity-building for prevention and the GBV sector.**

Canada should ensure that AI literacy initiatives address not only how AI works, but also digital consent, bodily autonomy, deepfakes, impersonation, grooming, coercive control, surveillance, gendered algorithmic bias and pathways to support and redress. Dedicated guidance and resources should also support GBV organizations and frontline professionals in the safe and responsible use of AI, including privacy, confidentiality, consent, cybersecurity, case documentation and survivor disclosure. This capacity building must be resourced. The GBV sector is already operating beyond capacity, and frontline agencies cannot absorb the cost of responding to AI-facilitated abuse without dedicated, sustained federal investment in training, technical support, and coordination. GBV organizations should be funded partners in the National AI Literacy Initiative, not unpaid consultees.

- **Ensure that recognition in legislation is matched by consistent implementation and enforceable accountability.**

Canada's emerging legislative measures demonstrate growing recognition of AI-enabled and technology-facilitated harms. However, legislative recognition must be matched by adequate enforcement resources, clear standards, consistent application across platforms and jurisdictions, and accessible mechanisms for protection and remedy. Voluntary transparency measures should not be relied upon where significant risks to safety, privacy, equality or fundamental rights exist.



Conclusion

Transparency is a necessary foundation for trust in AI, but for survivors of gender-based violence, transparency alone does not prevent harm or guarantee safety. Knowing that content is AI-generated does not stop its circulation, and disclosure requirements mean little without accessible remedies, platform accountability, and meaningful survivor involvement in designing the systems meant to protect them.

WomanACT urges the Government of Canada to ensure that its AI transparency framework is built with a gender-responsive, intersectional, and trauma-informed lens from the outset, and welcomes the opportunity to continue contributing our sector's expertise to this work.

Transparency should be a foundation for accountability—not a substitute for it.

Endorsed by

Andrea Coe, Individual WomanACT Member

Canadian Network for the Prevention of Elder Abuse, Organization WomanACT Member

Clausework, Organization WomanACT Member

Shivangi Sawh, Individual WomanACT Member

Women's Habitat of Etobicoke, Organization WomanACT Member

Women's Hostels Inc., Organization WomanACT Member