CANADIAN CENTER FOR WOMEN'S EMPOWERMENT | CENTRE CANADIEN POUR L'AUTONOMISATION DES FEMMES

Submission to the People's Consultation on Artificial Intelligence (AI)

Written by The Canadian Centre for Women's Empowerment (CCFWE)

Date: March 20, 2026

1.0 Introduction

1.1 About the Canadian Center for Women's Empowerment (CCFWE)

CCFWE is Canada's only nonprofit solely dedicated to addressing economic abuse and advancing economic justice. Through system change, research, policy leadership, and collaboration, we work to dismantle systemic barriers and build pathways to economic safety and inclusion. Learn more: https://ccfwe.org/

1.2 Why This Issue Matters

CCFWE has observed that technological tools are increasingly weaponized to facilitate control, intimidation, and financial harm against survivors of intimate partner violence. CCFWE's national research underscores the urgency of this issue:

- 1 in 3 women in Canada will experience economic abuse.
- The co-occurrence of economic abuse in domestic violence cases is 96%.
- Technology-facilitated abuse is a factor in 78% of economic abuse cases.
- 84% of survivors have debt accumulated in their name as a direct result of abuse.

The integration of artificial intelligence (AI) and digital financial technologies into essential services has created new vectors for perpetrating abuse. Technology-Facilitated Economic Abuse (TFEA) has emerged as a significant and rapidly evolving form of gender-based violence. Consequently, the governance of AI systems is not merely a matter of technological or commercial policy; it is a matter of gender equality, economic justice, and human rights.

Despite the widespread use of Technology for Effective Assistance (TFEA), there remain substantial deficiencies in public awareness, policy frameworks, and institutional protections. AI also relies on existing data, which holds unchecked historical inequities, creating the potential of

worsening cultural, gender, racial and other forms of harmful biases. The integration of AI into banking, housing, and employment systems presents risks of exacerbating and automating existing harms if adequate safeguards are not established. Conversely, AI possesses the capability to provide significant advantages, such as enhancing fraud detection, recognizing patterns of coercion, and creating tools focused on supporting survivors, provided these systems are thoughtfully designed with equity in mind from the beginning.

2.0 Experiences with and Impacts of AI Technologies

2.1 Impact on Communities

The rise of AI has transformed financial and digital ecosystems, making automated decision-making essential in areas like banking and credit scoring. This creates systemic challenges for survivors of economic abuse due to the context-insensitive nature of algorithmic decision-making.

- Loan denials due to coerced or fraudulent debt.
- Rental rejection due to damaged credit histories.
- Employment barriers tied to financial instability or gaps in work history.

2.2 How AI is Harmfully Used

AI is deployed *on* survivors by institutions and systems that control access to essential services:

- Credit scoring algorithms
- Fraud detection systems
- Tenant screening tools
- Platform moderation systems

These systems frequently misinterpret survival behaviors, such as regaining account control, as risk or fraud. Additionally, AI is expanding avenues of harm:

- Deepfakes used for reputational damage and blackmail.
- Voice cloning enables financial impersonation.
- AI-enabled doxxing exposing sensitive data.
- E-transfer systems used to send coercive messages.

2.3 Technology-Facilitated Economic Abuse (TFEA)

For the communities CCFWE serves, TFEA is a central and growing concern. It manifests when digital platforms are employed to surveil, restrict, or exploit an individual's economic resources. Tactics include:

- Persistent monitoring of online banking and financial activity.
- Unauthorized alteration of passwords or access controls to financial accounts.
- Accumulation of debt in a survivor's name through fraudulently obtained credit.
- Use of digital payment platforms, such as e-transfers, to harass or intimidate.
- Manipulation of smart home technologies to create financial or psychological strain.
- Disruption of online businesses or income streams via harassment or fraudulent activity.

2.4 Impacts of AI-Enabled Systems on Survivors

AI-driven financial systems have introduced systemic risks by facilitating the weaponization of standard financial products. For instance:

- Perpetrators use e-transfer message fields to transmit threatening or coercive communications.
- Jointly held credit accounts are misused to accumulate non-consensual debt.
- Access to shared accounts is exploited to dissipate funds or extend credit without consent.

CCFWE's advocacy led to the introduction of an opt-out feature by Interac, allowing users to disable harmful message fields from certain senders. This illustrates the effectiveness of survivor-informed advocacy in enhancing technology safety.

3.0 Systemic Problems and Concerns with AI

3.1 Algorithmic Bias and Context-Insensitive Decision-Making

AI-driven systems in critical sectors negatively impact survivors by applying uniform logic that overlooks their specific circumstances. Common issues arise from automated systems that fail to contextualize financial data, leading to credit denials and employment barriers. Key problems include algorithmic bias that perpetuates historical inequalities (such as racism, misogyny etc.), context blindness where abuse-related financial harm is seen as individual failure, and a lack of human intervention preventing survivors from explaining their situations. Additionally, decision-making processes are opaque and difficult to challenge, while people who are inflicting economic abuse may exploit financial tools and AI features against survivors.

3.2 The Invisibility of Coercion in Automated Systems

A significant limitation of current AI architectures is their failure to recognize coercion in financial contexts. This oversight leads to the misunderstanding that coerced debt is a legitimate liability and unauthorized activities are voluntary. As a result, financial instability is wrongly attributed to personal irresponsibility, embedding the consequences of abuse into automated decision-making, which causes systemic exclusion and mischaracterization of survivors.

3.3 Weaponization of Financial and AI Technologies

Financial technologies are routinely weaponized, and AI integration risks accelerating this trend. The misuse of e-transfers for harassment, the non-consensual accumulation of debt, and the exploitation of joint accounts for post-separation control are well-documented. AI systems can further enable abuse by automating surveillance, flagging a survivor’s legitimate defensive actions as suspicious, and facilitating faster, less detectable forms of financial harm.
There is a significant disparity between protections against external threats (e.g., hacking) and the lack of safeguards against abuse by intimate partners who often have legitimate access to accounts and personal information.

3.4 Emerging AI-Enabled Harms

Emerging AI applications pose new forms of economic harm, transcending traditional financial systems. Deepfakes and synthetic media can harm reputations, disrupt employment, and enable blackmail. Voice cloning may lead to impersonation in financial or legal scenarios, allowing fraudulent transactions. Additionally, AI-assisted doxxing threatens personal and financial privacy, jeopardizing the income sources of online business operators. The evolution of these risks is accelerating faster than policy responses can keep up.

3.5 Policy and Regulatory Gaps

Current financial and regulatory frameworks can’t keep up with the pace of technological advancements, resulting in several key issues for survivors of domestic abuse. These include joint financial products that can hinder separation, coerced debt for which survivors are still legally accountable, and open banking systems that risk enabling new forms of surveillance. Such challenges persist long after survivors separate, impacting their access to housing, employment, and financial independence. Existing policy measures are reactive and fragmented, allowing new forms of abuse to emerge rapidly. The most pressing risks stem from

automated decision-making systems that influence critical areas such as banking, housing, and employment.

4.0 Use Case Assessment

4.1 Worthwhile Applications

AI can be beneficial when designed with safeguards, particularly in:

- Fraud detection systems capable of distinguishing coercion from criminal intent.
- Financial literacy and digital safety planning tools.
- Secure communication platforms for at-risk individuals.
- Data analysis to identify and address systemic inequities.

4.2 Applications Requiring Restriction or Prohibition

CCFWE recommends clear financial and governmental regulatory boundaries to ensure safety, autonomy, and economic recovery. The following should be restricted or banned:

- AI-enabled surveillance technologies deployed without explicit, informed consent.
- Algorithmic decision-making systems in high-stakes domains (credit, housing, employment) that lack transparency, accountability, and avenues for human appeal
- Generative AI used for impersonation, or abuse, including deepfakes and voice cloning.
- Financial technology features that enable or facilitate coercion without embedded safeguards (e.g., unsecured joint account controls).

4.3 Mitigation Strategies

To maximize benefits and minimize harm in AI systems, CCFWE proposes several strategies for ethical AI development:

- Implementing survivor-centered and trauma-informed design for AI systems interacting with vulnerable populations.
- Requiring human oversight and an appeal process for all high-risk automated decisions in sectors like credit, housing, and employment.
- Enhancing data privacy and protections to avoid misuse of sensitive information.
- Creating clear reporting and accountability mechanisms for AI-related harms, with accessible avenues for challenging decisions and seeking redress.
- Banning the use of datasets from hateful or abusive platforms (ex. extremist forums)
- Promoting government investment in public datasets that undo the historical harmful data biases.

5.0 Gaps in the Current Discourse

5.1 What Is Missing from the Discussion

Key gaps include:

- The intersection of AI systems with Technology-Facilitated Economic Abuse (TFEA) and how automated systems compound harm.
- The distinctly gendered and racialized impacts of algorithmic decision-making.
- The role of AI in reinforcing coercive control, including surveillance and exclusion
- Centering survivor experience and leadership in system design and policy is imperative.
- The need to move beyond framing AI as a neutral innovation to analyzing it as a system that can reinforce or disrupt existing power structures.

5.2 What Policymakers Must Understand

To address these gaps, policymakers must recognize that:

- Algorithms encode historical inequities and amplify discrimination at scale.
- Automation amplifies harm at scale.

- Economic abuse is a systemic issue. Survivors should not bear the burden of navigating systems designed without their realities in mind.
- Equity and safety must be embedded from the design stage.

6.0 Policy Recommendations

1. **Recognize TFEA:** Minister of Artificial Intelligence and Digital Innovation must integrate Technology-Facilitated Economic Abuse into AI and financial regulations and apply GBA+ across all AI policy. Civil society brings frontline evidence to ensure frameworks reflect survivors' realities.
2. **Strengthen Bill C-27:** Minister of Artificial Intelligence and Digital Innovation must reintroduce the now dead Bill C-27. The proposed bill should include amendments to the Consumer Privacy Protection Act to guarantee survivors redress, credit restoration, and protection from impersonation. Civil society and philanthropy can support navigation and fund legal advocacy.
3. **Mandate Human Oversight:** Fully automated decisions in housing, credit, and employment must be prohibited. Businesses must provide human review and appeals; civil society helps define survivor-informed oversight.
4. **Establish an AI Regulator:** Prime Minister and Minister of Artificial Intelligence and Digital Innovation should create an independent regulator with enforcement powers to mandate risk assessments, incident reporting, and strong technical standards. Civil society and philanthropy can support independent monitoring.
5. **Require Survivor-Centered Design:** Minister of Finance should work with Minister of Artificial Intelligence and Digital Innovation to require financial institutions and tech developers to embed abuse-prevention features. Civil society and philanthropy can co-design solutions and fund innovation grounded in lived experience.
6. **Strengthen Data Protection:** The Office of the Privacy Commissioner of Canada must strengthen privacy laws so survivors can revoke data access and prevent misuse. The financial and tech sectors must embed default protections; civil society and philanthropy can deliver digital safety education and tools.
7. **Invest in Literacy Programs:** The Ministry of Women and Gender Equality should continue to fund national, trauma-informed digital and financial literacy programs. Civil society delivers programming; philanthropy supports scaling and reach.
8. **Create a Research Network:** Establish a national network connecting academia, industry, and civil society to co-develop inclusive AI solutions. Philanthropy can support community-led research participation.
9. **Strengthen Cross-Sector Collaboration:** All stakeholders must formalize partnerships to implement equitable solutions. Philanthropy can serve as convener and fund collaborative work.
10. **Expand Equitable Access:** Government should expand AI infrastructure access beyond major institutions through grants for community-based and survivor-led organizations. Philanthropy can fund capacity-building.
11. **Ensure Continuous Review:** Government must mandate regular policy reviews with formal consultation of survivor-serving organizations. Philanthropy can support sustained community engagement.
12. **Measure Success:** Track reductions in AI-facilitated harm, increased inclusion of women and survivors in AI sectors, and improved financial security outcomes. Civil society and philanthropy can support independent evaluation.

7.0 Conclusion

AI is being used to perpetuate economic abuse and deepen inequality. CCFWE's work demonstrates that centering survivor experiences leads to safer, more effective systems. A human rights-based, intersectional approach to AI governance is essential to ensure technology supports empowerment rather than exploitation. Canada's leadership in AI should be measured not only by innovation, but by its ability to advance safety, equity, and economic justice for all communities.

8.0 Sources

1. Understanding Technology-Facilitated Economic Abuse: https://ccfwe.org/understanding-technology-facilitated-economic-abuse/
2. Technology-Facilitated Economic Abuse Fact Sheet: https://ccfwe.org/wp-content/uploads/2024/10/TFEA-Fact-Sheet-English-ver.pdf
3. Leveraging Technology to Combat Gender-Based Violence and Economic Abuse: https://ccfwe.org/2025/05/22/leveraging-technology-to-combat-gender-based-violence-and-economic-abuse/
4. Technology Safety, AI and Economic Abuse: https://ccfwe.org/technology-safety-ai-and-economic-abuse/
5. HELP US RISE 2024 - NATIONAL ECONOMIC ABUSE AWARENESS MONTH: https://ccfwe.org/help-us-rise-2024/

Contact us

Denna Berg
Director of Policy, CCFWE
denna.berg@ccfwe.org

Meseret Haileyeus
Executive Director
mesi.haileyesus@ccfwe.org