Recommendations for Addressing Impacts of AI on Women, Girls, and 2SLGBTQI+ People

Brief to the House of Commons Standing Committee on the Status of Women

Blair Attard-Frost
Canada CIFAR AI Chair
Fellow, Alberta Machine Intelligence Institute (Amii)
Assistant Professor, University of Alberta Department of Political Science

October 27, 2026

Summary

This brief draws on real-world incidents and relevant literature to show that women, girls, and 2SLGBTQI+ people experience gender-based harm as a result of four main types of AI applications: (1) *Hateful and nonconsensual AI-generated content*, (2) *use of AI in healthcare*, (3) *use of AI in HR and recruitment*, and (4) *biometric classification*. If risks to fairness, safety, and wellbeing are not effectively mitigated, these AI applications may cause physical, psychological, social, and economic harms to women, girls, and 2SLGBTQI+ people. Three key actions are recommended to address those impacts:

(1) **Develop legislation to mitigate the risk of AI systems being used to carry out discriminatory practices as defined in Canadian human rights law,** establishing requirements for fairness assurance, documentation, and disclosure for developers and operators of AI systems with human rights impacts.

(2) **Strengthen legislative protections granted by Bill C-16 and Bill C-34** to include stronger independent oversight and more proactive measures for preventing gender-based harm enabled by generative AI systems before it occurs.

(3) **Develop legislation to prevent developers and providers of highly impactful AI models from harming vulnerable groups**, establishing requirements for risk mitigation and transparency in high-impact model services, whistleblower protections, regulatory powers to restrict model services that pose a threat to public safety, and monetary penalties and criminal offences for non-compliance; in addition, amend Canadian cybercrime law to criminalize gaining unauthorized access to a computer system through reckless use of an automated system.

Background

If carefully governed and thoughtfully adopted, some applications of AI have the potential to enable greater inclusion and opportunity in the Canadian economy. Many organizations across Canada are taking great initiative to ensure women, girls, and 2SLGBTQI+ people are better represented in AI training programs, tech education, and the tech workforce. These efforts are important and should continue to be supported. However, to deliver on the promise of AI, various harms must also be prevented.

It is widely known that AI imposes disproportionate risks upon women, girls, and 2SLGBTQI+ people.[1] Harmful gender-based impacts of AI often relate to issues of discrimination, equity, safety, and wellbeing. Some of my recent research takes a closer look at those impacts. With funding and supports from CIFAR, Amii, and SSHRC, my research team and I have been working since July 2026 on reviewing literature and a global sample of over 1500 real-world AI incidents. Our goal is to identify incidents of gender-based harm caused by a range of AI use cases. Our study is still ongoing, but our initial findings re-affirm a decade of existing research while also adding new insights into areas of concern and policy options.

Harmful gender-based impacts of AI

The totality of AI applications that enable gender-based harm are myriad, and evidence of harm is often obscured by the limited transparency practices of AI developers and operators. In our review, we are finding that AI systems have the potential to enable gender-based harm across four main application areas.

Area 1: Hateful AI-generated content and nonconsensual sexual deepfakes

The type of harm we find most frequently is use of generative AI to create and distribute hateful content or nonconsensual sexual deepfakes. These kinds of incidents account for 35 of the 93 incidents of gender-based harm identified so far. Victims of nonconsensual sexual deepfakes are overwhelmingly women, girls, and 2SLGBTQI+ individuals.[2]

Area 2: Gender-based harms in healthcare

In healthcare, we find bias in diagnostic tools and decision support systems. For example, a 2020 study by a team from University of Toronto, Vector Institute, and MIT found that X-ray classification models trained on public medical datasets can exhibit racial and gender biases, resulting in disparate error rates between men, women, white patients, and Black

[1] For an in-depth synthesis of issues related to AI and technology-facilitated gender-based violence, see Khoo, C. (2021). Deplatforming misogyny: Report on platform liability for technology-faciliated gender-based violence. *LEAF*. https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf
[2] Le, T. D. & Döring, N. (2026). Perspectives on non-consensual deepfake pornography: A content analysis of Reddit discussions initiated by perpetrators, victims, and bystanders. *Sexuality & Culture*, *30*, 2319-2343. https://link.springer.com/article/10.1007/s12119-026-10566-x

patients.[3] In 2024, a suicide prevention algorithm used by the United States Department of Veterans Affairs prioritized care for white men over female veterans and survivors of military sexual trauma.[4] Reviews of research literature and real-world healthcare applications of AI find that gender bias and unclear de-biasing methods are common.[5]

Area 3: Gender-based harms in HR and recruitment

In HR and recruitment, we find gender bias in tools used for hiring and employment decision-making. In 2017, an experimental resume screening tool made by Amazon was decommissioned when it was found to score women job applicants lower than men.[6] A 2020 study by a group at Cornell University found unclear or limited de-biasing methods across 18 hiring assessment tools,[7] and in 2024, the UK Information Commissioner's Office conducted an audit of several AI recruitment platforms and reported frequent issues of inaccuracy and bias.[8] Reviews of research literature and relevant incidents have found a high risk of gender bias, racial bias, and other forms of bias throughout the lifecycle of AI systems used for hiring and recruitment.[9]

Area 4: Gender-based harms of biometric classification

Facial recognition, gender recognition, and other forms of biometric classification pose risks of discrimination, particularly for women of color and for people whose gender differs from their sex assigned at birth. A 2018 study of three gender classification models showed the lowest error rates on lighter-skinned male faces and highest error rates on darker-skinned female faces.[10] In 2023, a pregnant Black mother was wrongfully arrested by Detroit police

---

[3] Seyyed-Kalantari, L., Liu, G., McDermott, M., Chen, I. Y., & Ghassemi, M. (2021). CheXclusion: Fairness gaps in deep chest X-ray classifiers. *Pacific Symposium on Biocomputing*, *26*, *232-243*. https://psb.stanford.edu/psb-online/proceedings/psb21/seyyed-kalantari.pdf

[4] Glantz, A. (2024). V.A. uses a suicide prevention algorithm to decide who gets extra help. It favors white men. *The Markup*. https://themarkup.org/news/2024/05/30/v-a-uses-a-suicide-prevention-algorithm-to-decide-who-gets-extra-help-it-favors-white-men

[5] See Cirillo, D. et al. (2020). Sex and gender differences and biases in artificial intelligence for biomedicine and healthcare. *npj Digital Medicine*, *3*, 81 (https://www.nature.com/articles/s41746-020-0288-5); Otokiti, A. et al. (2025). Gender and racial bias unveiled: Clinical artificial intelligence (AI) and machine learning (ML) algorithms are fanning the flames of inequity. *Oxford Open Digital Health*, *3*, oqaf027 (https://pmc.ncbi.nlm.nih.gov/articles/PMC12560773/).

[6] Goodman, R. (2018). Why Amazon's automated hiring tool discriminated against women. *ACLU*. https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against

[7] Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020). Mitigating bias in algorithmic hiring: Evaluating claims and practices. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 469-481. https://dl.acm.org/doi/epdf/10.1145/3351095.3372828

[8] UK Information Commissioner's Office (2024). AI tools in recruitment: Audit outcomes report. https://ico.org.uk/media2/migrated/4031620/ai-in-recruitment-outcomes-report.pdf

[9] Mujtaba, D. F. & Mahapatra, N. R. (2025). Fairness in AI-driven recruitment: Challenges, metrics, methods, and future directions. *arXiv pre-print 204519699* (https://arxiv.org/pdf/2405.19699); Köchling, A. & Wehner, M. C. (2020). Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research, 13*, 795-848 (https://link.springer.com/article/10.1007/s40685-020-00134-w).

[10] Buolamwini, J. & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Researc*h, *81*, 77-91. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

on the basis of false information provided by a facial recognition system.[11] Notable biometric incidents affecting transgender people include flagging for additional screening by airport body scanners due to gender misclassification[12] and loss of access to services requiring facial verification due to changes or gender non-conformance in facial structure.[13] Proposals to use gender recognition systems to restrict access to gender-segregated spaces have also been discussed.[14]

Recommendations

The three recommendations below should be implemented to prevent harmful gender-based impacts of AI. Recent research and civil society initiatives demonstrate that the federal government must meaningfully engage with Canadians on AI policy to build public trust in both AI technologies and in the government's approach to regulating AI.[15] Structural exclusion and barriers to participation for equity-deserving groups are a long-standing concern in federal AI initiatives.[16] Therefore, the below recommendations should only be implemented as part of a broader national AI regulation initiative that involves deliberative and iterative public engagement, identifies high-risk AI application areas in need of intervention, and faithfully acts upon public preferences for AI regulation.

1. *Develop legislation to mitigate discrimination in AI systems with human rights impacts*

The *Canadian Charter of Rights and Freedoms* and *Canadian Human Rights Act* guarantee protection against discrimination on the basis of attributes such as sex, sexual orientation, gender identity, and gender expression in legal matters, in services such as healthcare, and in hiring and employment-related matters.[17] Human rights law does not

[11] ACLU (2024). Woodruff v. Oliver. https://www.aclu.org/cases/woodruff-v-oliver
[12] Waldron, L. & Medina, B. (2019). When transgender travelers walk into scanners, invasive searches sometimes wait on the other side. *ProPublica*. https://www.propublica.org/article/tsa-transgender-travelers-scanners-invasive-searches-often-wait-on-the-other-side
[13]Factora, J. (2021). Trans drivers say Uber is still discriminating against them. *Them*. (https://www.them.us/story/uber-trans-drivers-aclu); Perrett, C. (2022). A social media app just for 'females' intentionally excludes trans women — and some say its face-recognition AI discriminates against women of color, too. *Business Insider*. https://www.businessinsider.com/giggle-app-uses-ai-to-exclude-trans-women-ceo-says-2022-1
[14] See for example the proposal put forward by the US National Institute of Standards and Technology in Ngan, M. & Grother, P. (2015). Face recognition vendor test (FRVT) performance of automated gender classification algorithms, NISTIR 8052. (https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8052.pdf); Kladzyk, R. (2023). Policing gender: How surveillance tech aids enforcement of anti-trans laws. *POGO*. (https://www.pogo.org/investigates/policing-gender-how-surveillance-tech-aids-enforcement-of-anti-trans-laws); Feeney, M. (2022). When AI meets the transgender community. *CATO Institute* (https://www.cato.org/blog/when-ai-meets-transgender-community);
[15] See for example the 2022 report of the Government of Canada's AI Public Awareness Working Group (https://ised-isde.canada.ca/site/advisory-council-artificial-intelligence/sites/default/files/attachments/2023/learning_together_for_responsible_artificial_intelligence_minisi_approved_20230303.pdf); Attard-Frost, B., Brandusescu, A., & Lyons, K. (2024). The governance of artificial intelligence in Canada: Findings and opportunities from a review of 84 AI governance initiatives. *Government Information Quarterly*, *41*(2), 101929 (https://www.sciencedirect.com/science/article/pii/S0740624X24000212); People's Consultation on AI (2026). Submissions. (https://www.peoplesaiconsultation.ca/submissions/).
[16] Attard-Frost, B. (2025). Transfeminist AI governance. *First Monday*, *30*(4), April 2025. https://firstmonday.org/ojs/index.php/fm/article/view/14121
[17] Canadian Human Rights Act, R.S.C. 1985, c. H-6. https://laws-lois.justice.gc.ca/eng/acts/h-6/

cease to exist when healthcare and employment decisions are made by an automated tool rather than by clinicians and hiring managers. In the age of AI, Canada must re-enshrine the protections guaranteed by the Charter and the CHRA. Developers and operators of AI tools with potential human rights impacts should be required to mitigate the risk of their systems being used to carry out discriminatory practices and to be transparent when incidents of discrimination do occur.[18] Legislation should be created with the following requirements:

- Developers of AI systems that may be used to carry out discriminatory practices should be required to maintain records of training data provenance and dataset composition, and to carry out and maintain records of model development and testing procedures such as de-biasing and fairness benchmarking prior to the system's deployment.
- Operators should be required to maintain records of system decisions and to disclose to authorities and affected individuals when discriminatory decisions occur.

2. Strengthen legislative protections that address harmful generative AI systems

In addressing harmful generative AI systems, the government has recently made progress by tabling Bill C-34 (the *Safe Social Media Act*)[19] and by amending the *Criminal Code* through Bill C-16.[20] However, gaps in the scope of these bills limit their effectiveness at preventing gender-based harm before it occurs.[21]

Bill C-16 criminalizes distribution of nonconsensual sexual deepfakes, but the creation and possession of these deepfakes should also be criminalized as a preventative measure against future distribution. Additionally, the scope of imagery covered by law should be expanded to cover nonconsensually sexualized uses of one's likeness rather than the definition set out in Bill C-16, which covers only imagery that is "likely to be mistaken for a visual recording of that person."[22]

Bill C-34 should be amended to include stronger independent oversight and more proactive measures that prevent AI-enabled gender-based harm before it occurs. Providers of generative AI services should be required to demonstrate that their systems have been tested and safeguarded against hateful and nonconsensual sexual uses prior to deployment, rather than shifting legal burden onto victims to report crimes and seek justice.

---

[18] For discussion of algorithmic bias and transparency challenges in Canadian human rights law, see Burkell, J. A. & Bailey, J. (2018). Unlawful distinctions? Canadian human rights law and algorithmic bias. *Canadian Yearbook of Human Rights*, 217-230 (https://ajcact.openum.ca/publications/unlawful-distinctions-canadian-human-rights-law-and-algorithmic-bias/); Law Commission of Ontario & Ontario Human Rights Commission (2024). Human rights AI impact assessment (https://www.ohrc.on.ca/en/human-rights-ai-impact-assessment).

[19] Bill C-34: https://www.parl.ca/Content/Bills/451/Government/C-34/C-34_1/C-34_1.PDF

[20] Government of Canada (2026). Protecting Victims Act: Legislation to protect victims and keep kids safe from predators. https://www.justice.gc.ca/eng/csj-sjc/pl/c16/index.html

[21] For a discussion of gaps in the scope of C-16 and C-34, see Kondrup, E. et al. (2026). Sharing non-consensual 'deepfake' porn in Canada is now a crime. The law still fails the victims. *The Conversation*. https://theconversation.com/sharing-non-consensual-deepfake-porn-in-canada-is-now-a-crime-the-law-still-fails-the-victims-291112

[22] For a detailed rationale for expanding this definition, see BSCC & LEAF (2026). Proposed amendments to Bill C-16. https://www.leaf.ca/wp-content/uploads/2026/03/Bill-C-16-Submission-BSCC-and-LEAF-FINAL.pdf

The proposed Digital Safety Commission should also be modified to keep the commission's appointments and powers accountable to Parliament and independent from cabinet. This will ensure that protections for women, girls, and 2SLGBTQI+ people will not be subject to political interference.

3. Develop legislation to mitigate safety & security risks of large AI model developers

Recent security incidents in which AI agents with insufficient operator oversight have infiltrated corporate and government systems have prompted concern about catastrophic AI risks.[23] As is the case in other types of catastrophes such as natural disasters, pandemics, and power grid failures, vulnerable and marginalized groups are especially at risk in large-scale catastrophic incidents.[24] As part of the "AI for All" strategy, the federal government has started building a regulatory architecture for AI developers that largely relies on voluntary certification mechanisms and extralegal safety investigations.[25] The government has not yet committed to put those safety measures on a statutory footing.

To protect women, girls, 2SLGBTQI+ people, and other vulnerable groups against the most harmful potential impacts of AI, Canada needs legislation that imposes stronger requirements for public safety, accountability, and transparency on developers of large AI models such as OpenAI, Anthropic, and Google. Legislative action should include:

- Pre-deployment risk mitigation, safety testing, recordkeeping, and incident disclosure requirements for developers and providers of AI models whose anticipated social or economic impacts exceed a mandated threshold (i.e., *regulated model services*).
- Whistleblower protections and regulatory powers to investigate developers and providers of regulated model services and to impose restrictions or temporary moratoria on the development, deployment, or operation of a regulated model when those activities present a reasonable threat to public safety.
- Monetary penalties for violations of the legislation, in addition to criminal offences for cases of reckless or malicious use of a regulated model service.
- Amending section 342.1 (1) of the *Criminal Code* ("Unauthorized use of a computer") to apply to persons who unintentionally obtain unauthorized access to a computer system through reckless use of an automated system.[26]

These actions will build upon Bill C-34's framework for targeted regulation of chatbot services with high use and impact, while also updating Canadian cybercrime law to better account for advances in AI technology. Legislation should be coupled with resources and training for regulators and judicial staff to ensure new provisions will be applied and enforced effectively.

---

[23] For an up-to-date database of AI security incidents resulting from insufficient operator oversight, refer to the Rogue AI Tracker (https://rogueaitracker.com/incidents/); see also Kierans, A. et al. (2025). Catastrophic liability: Managing systemic risks in frontier AI development. *arXiv:2505.00616v2.* https://arxiv.org/pdf/2505.00616v2

[24] United Nations Office for Disaster Risk Reduction (2020). Inclusive communities are safer communities. https://www.undrr.org/news/inclusive-communities-are-safer-communities

[25] For a discussion of regulatory gaps in the AI for All strategy, see Attard-Frost, B. in The Walrus (2026). Canada finally has a national AI strategy. Experts hate it. https://thewalrus.ca/canada-ai-plan/

[26] Criminal Code, R.S.C. 1985, c. C-46. https://laws-lois.justice.gc.ca/eng/acts/C-46/section-342.1.html