PEOPLE'S CONSULTATION ON AI

Submission: Proposal for a National AI Ethics Committee to Safeguard Democratic Integrity

Prepared By :

Miranda Woodland

(613)888-1285
miranda@mirandawoodland.com
www.mirandawoodland.com

"[I]n order to intelligently respond to the grave dangers we have created, we have to rethink our dominant values and habits, even the character traits we are used to thinking of as virtues. Moral and epistemic virtues are always a cultural adaptation to a specific environment for human flourishing. When that environment changes suddenly and radically, our virtues, or at least our customary pattern of expressing them, may become maladapted and even pose a danger to us."

Shannon Vallor, *The AI Mirror: How to Reclaim our Humanity in an Age of Machine Thinking*

About the Author

Miranda Woodland is a graduate student at Athabasca University in the process of completing a master's degree in interdisciplinary studies with a focus in Adult Education. She completed an Honours Bachelor of Arts degree at the University of Toronto in 2008 with a specialization in bioethics and minor in political science. She is a former director and officer of the board of a political party's chief agent and worked in the financial industry for over 10 years. Throughout this time, she has been involved both personally and professionally in testing and building computer software.

Given this background, Miranda has a specific interest in the ways technology impacts civic engagement and democracy. In the fall of 2025, she submitted an e-petition to parliament (Appendix) that is intended to regulate algorithmic transparency and require labels for bot generated and AI generated content. Unfortunately, there has not been a response from the Members of Parliament - including the Office of the Minister of AI and Digital Innovation - regarding a willingness to sponsor such a petition. The lack of urgency regarding regulations that would help safeguard Canadian democracy is disheartening and reflects political interest in technology corporations over public safety. This is the impetus behind this submission.

Contents

Executive Summary....3

Decision-Making Technologies & Data Transparency....4

- Data Collection Practices....4
- Storage & Retention....4
- Partnerships with Private AI Firms....4
- Transparency Gaps....5

Impact on Democracy....5

- Deepfakes & AI Images: Reputational Harm and the "Liar's Dividend"....5
- Politicians' Role in Misinformation....6
  - The Political Economy of Disinformation....6
  - Manipulation Machines....6
- Polarization & Trust: The Shrinking Public Sphere....6

Ethical Imperatives & Human-Centred Design....7

- Interdisciplinarity & Transdisciplinarity: Bridging the Divide....7

Proposal: Establishing a National AI Ethics Committee to Safeguard Democratic Integrity....8

- Strategic Mandate: Oversight of Federal and Foreign AI Engagements....8
- Composition: A Multidisciplinary Coalition for Cognitive Defense....8
- Institutional Independence: Funding and Oversight Mechanisms....9

Conclusion....9

Executive Summary

💡 The Canadian federal government is collecting and storing personal data in partnership with private AI firms without adequate transparency or accountability.

The Canadian federal government has utilized private cloud and AI services for several years, yet these partnerships with firms such as Google, Microsoft, and Amazon lack sufficient transparency and accountability[i]. By storing data with foreign-headquartered providers, the government creates a "digital backdoor"[ii] where sensitive personal and master data becomes subject to extraterritorial *long-arm* statutes, such as the US CLOUD Act, effectively stripping Canada of jurisdictional control. This mirrors risks seen in other jurisdictions where state data is treated as a nationally produced asset for monetization without adequate privacy safeguards[iii].

This structural dependency enables the use of "manipulation machines"[iv] that integrate generative AI with microtargeting algorithms to target individual vulnerabilities at scale. Such systems systematically distort the information environment by amplifying emotionally resonant falsehoods, fostering extreme political polarization and societal fragmentation[v]. Furthermore, reliance on these opaque systems concentrates power within a technological elite, eroding democratic norms and undermining public trust in institutions[vi]. This resulting "truth decay" and generalized uncertainty can paralyze the collective action necessary for a functioning democracy[vii]. In Canada, despite high formal democracy scores, over 30 % distrust the system and nearly half feel unrepresented, creating fertile ground for truth decay and automated propaganda that can alter election outcomes by targeting vulnerable individuals.

To safeguard democratic integrity, Canada must establish a national AI-ethics committee before entering any new partnerships with foreign AI firms[viii]. This multi-stakeholder body—comprising technologists, social scientists, ethicists, and civil-society representatives—should be empowered to conduct pre-emptive threat assessments and ensure that democratic values are embedded into the architecture of all government-AI integrations[ix]. Moving toward a "governance-by-design"[x] methodology is essential to ensure that technological advancement does not sacrifice legitimacy, equity, or jurisdictional sovereignty[xi].

Decision-Making Technologies & Data Transparency

Data Collection Practices

The Canadian federal government and its partners collect various data categories, including subscriber data (personal identifiers like names, addresses, and social insurance numbers), access data (IP addresses and connection logs), transactional data (metadata like geolocation and communication protocols), and content data (voice, video, and text). Advanced AI implementations also utilize biometric data for identity systems and behavioural tracking to monitor social media activity and public sentiment.

Data is gathered from major federal agencies and crown corporations; for example, the Canadian Broadcasting Corporation (CBC) moved over 12,000 accounts to Google Apps in a single migration. Furthermore, law enforcement agencies like the RCMP utilize AI for predictive policing and surveillance, while other departments use these technologies for automated debt recovery and predictive analytics. These agencies often source data through third-party AI vendors who maintain extensive datasets for training deep learning models.

Storage & Retention

While major providers like Microsoft Canada and Amazon Web Services (AWS) Canada offer to host data in domestic data centers, this does not guarantee digital sovereignty. Under the US CLOUD Act, domestically stored data can still be subject to "long-arm" production orders from foreign governments if the provider is headquartered in the United States. This creates an "un-territorial" environment where physical storage location is secondary to the legal jurisdiction of the parent company.

Research indicates a persistent tension between data protection regimes that demand purpose limitation and erasure (the "right to be forgotten") and the technical architectures of modern AI systems. In many cases, it is difficult for citizens to ensure the deletion of their records when they are replicated across multiple offshore data centers or integrated into complex model pipelines.

Partnerships with Private AI Firms

The Government of Canada has utilized services from major private firms, including Google, Microsoft, Amazon, Salesforce, and ServiceNow, for production workloads for over seven years. These partnerships extend into critical infrastructure, such as using Baidu's IoT platforms for connected smart appliances or utilizing foreign cloud capacities for sensitive internal communications.

Many existing contracts lack robust requirements for data provenance, purpose limitation, or auditability. Specifically, providers like Microsoft do not always reveal what kind of metadata is transmitted back to foreign headquarters, making it impossible for the government to guarantee the traceability of personal data processing.

Transparency Gaps

There is a significant lack of transparency regarding data flows between government agencies and private tech firms, with many critical areas of governance remaining in "silence". Citizens often have no control over—or knowledge of—where their data is located or which foreign jurisdictions' laws are currently governing it.

Citizens find it increasingly difficult to understand how their data influences automated decisions, such as credit scoring or predictive policing results. Current administrative doctrines often restrict public information access rights, preventing citizens from compelling the government or its private partners to provide systemic explanations for algorithmic decisions that profoundly shape their lives. This opacity can lead to "automated hyper-personalization," where citizens are targeted with political ads based on unique psychological vulnerabilities without their awareness or consent.

Impact on Democracy

The integration of Artificial Intelligence (AI) into the political landscape has introduced profound structural challenges to democratic integrity. Experimental data and systematic reviews reveal that the impact of AI extends beyond simple deception, fundamentally altering the relationship between citizens and the information environment.

Deepfakes & AI Images: Reputational Harm and the "Liar’s Dividend"

AI-generated images and deepfakes primarily influence democracy by creating generalized uncertainty rather than through widespread direct deception. Even when voters do not believe a deepfake outright, the resulting doubt undermines trust in legitimate political content.

Experimental studies demonstrate that visual misinformation, regardless of technical sophistication, causes measurable reputational damage to politicians and significantly affects voter attitudes and voting intentions. In one case study involving a fabricated endorsement, 10% of viewers who believed the video reported they would no longer vote for the implicated candidate.

While journalistic factchecking can mitigate the effects of specific deepfakes, generalized warnings about the technology often backfire. These warnings create a "liar's dividend," where increased awareness of deepfakes induces voters to distrust *all* political videos, including authentic footage. This allows politicians to escape accountability for real misconduct by claiming incriminating evidence is a deepfake.

Politicians' Role in Misinformation

Political actors are increasingly transitioning from passive observers to active creators and amplifiers of AI-mediated false content.

The Political Economy of Disinformation

The accessibility of generative AI has democratized the production of propaganda, but the "political economy" of this space still favors well-resourced actors. Wealthy interests can subsidize large-scale deepfake production, while state-sponsored actors leverage these tools for strategic foreign interference to destabilize rival democracies.

Manipulation Machines

The synthesis of generative AI with micro-targeting algorithms has created "manipulation machines". These systems can autonomously target individuals based on specific psychological vulnerabilities without human intervention, shifting election outcomes by swaying only a few thousand individuals in key districts.

Polarization & Trust: The Shrinking Public Sphere

AI technologies systematically distort the political information environment, fostering societal fragmentation and institutional distrust.

Micro-targeting allows campaigns to bypass "under-mobilized" groups—such as the young or marginalized—to focus exclusively on narrow sections of persuadable voters. This shrinks the public sphere and can be used to send "demobilizing messages" to opposition supporters to suppress turnout.

Engagement-optimization algorithms prioritize emotionally resonant and divisive content, reinforcing filter bubbles and echo chambers. This process intensifies affective polarization, where emotional reactions override factual reasoning, making civil discourse increasingly difficult.

Ethical Imperatives & Human-Centred Design

Interdisciplinarity & Transdisciplinarity: Bridging the Divide

Research indicates that the "lack of sufficient interdisciplinarity and transdisciplinarity is a major barrier to effective AI ethics"[xii]. Without substantial bridging between these disciplines, AI ethics remains a theoretical exercise rather than a practical safeguard.

We require structural change in how research and development is conducted. It should involve joint teams comprising humanities scholars, social scientists, engineers, businesspeople, and policy experts to ensure diverse perspectives are integrated from the project's inception.

Proposal: Establishing a National AI Ethics Committee to Safeguard Democratic Integrity

Strategic Mandate: Oversight of Federal and Foreign AI Engagements

The National AI Ethics Committee must be empowered to audit the intersection of emerging technology and state power. Its mandate must ensure that AI deployment does not undermine national sovereignty or the cognitive liberty of the electorate.

The Committee mandates a rigorous review of all federal AI contracts, with an immediate focus on foreign vendors and "dark web" associations. Case studies of fabricated arrests[xiii] and manipulated campaign visuals[xiv] demonstrate that without strict audit logs, foreign intelligence can weaponize synthetic media to induce social turmoil.

To close the regulatory asymmetry gap, the Committee will enforce mandatory "data flow maps" and "audit logs." Platforms must disclose the behavioral profiling and algorithmic prioritization mechanisms that currently operate in a "black box" environment. [xv]

Based on previous findings[xvi], the Committee can monitor "structural distortions" where algorithms prioritize emotionally resonant disinformation over factual accuracy. This includes tracking the systemic degradation of institutional trust and the formation of polarized filter bubbles.

Composition: A Multidisciplinary Coalition for Cognitive Defense

Protecting democracy requires a synthesis of technical, ethical, and cultural intelligence. The Committee's architecture should mandate a multidisciplinary defense to ensure that democratic norms are paramount in decision-making regarding the implementation and use of new technologies. The committee should be comprised of:

- **AI/ML Researchers:** Mandated to conduct technical audits of Generative Adversarial Networks (GANs) and engagement-optimization algorithms to detect "Visual Primacy" manipulations.
- **Ethicists:** Tasked with evaluating hyper-technocracy[xvii] and paternalism inherent in automated decision-making.

- **Indigenous Knowledge Holders:** AI systems often bypass under-mobilized and marginalized voters[xviii]; these experts ensure inclusive representation and prevent the disenfranchisement of non-traditional voter blocks.
- **Civil-Society Representatives:** Required to provide a democratic check against "technological elites" (or *Tech Bros*) who operate in an unaccountable, proprietary manner.
- **Legal Scholars:** Directed to establish a "Digital Right of Reply"[xix] for victims of synthetic media and navigate the constitutional complexities of regulating deepfakes circulated with dark money.

Strategic resilience requires an ex-ante posture. The Committee will move beyond post-hoc *factchecking* to *mandatory ethics reviews* prior to any federal AI deployment.

Institutional Independence: Funding and Oversight Mechanisms

To resolve the regulatory paralysis documented in existing systems such as the United States the Committee must possess structural autonomy.

- **Treasury-Direct Funding:** A dedicated budget prevents the influence of "dark money" and ensures the Committee can outpace the technical sophistication of state-sponsored disinformation actors.
- **Parliamentary Oversight:** The Committee will report to an independent, non-partisan parliamentary body. This provides democratic legitimacy without making the Committee a tool for partisan "electoral incentives."

By insulating the Committee from the immediate political pressures that stifle current regulation, we create a permanent safeguard for democratic norms against automated propaganda.

Conclusion

Canada’s current approach - partnering with foreign private AI providers to collect, store, and operationalize sensitive personal and public-interest data - creates accountability and jurisdictional vulnerabilities that can erode democratic self-determination. When these systems are deployed without transparent data-flow governance, auditable decision logs, and ex-ante ethical oversight, they enable manipulation at scale: intensifying polarization, accelerating “truth decay,” and undermining citizens’ trust in both institutions and each

other. To address this structural risk, Canada should urgently establish an independent, multidisciplinary National AI Ethics Committee with authority to require data provenance and auditability, map, and constrain data flows, and conduct mandatory risk assessments before any new AI partnership or deployment. By embedding democratic values, Canada can ensure that innovation strengthens its democratic future.

---

[i] Kushwaha et al., “Up in the Air: Ensuring Government Data Sovereignty in the Cloud.”
[ii] Ibid.
[iii] Arner et al., “The Transnational Data Governance Problem.”
[iv] For example, Dobber, *Democracy Political Microtargeting : A Threat to Electoral Integrity ?*
[v] Mansur, “AI and Cyber-Enabled Threats to Democracy through Algorithmic Manipulation and Generative AI in Undermining Democratic Integrity”; Cupać et al., “Democratization in the Age of Artificial Intelligence: Introduction to the Special Issue.”
[vi] Coeckelbergh, *AI Ethics*; Gibson et al., “Learning Theories for Artificial Intelligence Promoting Learning Processes”; Imran et al., “The Role of Generative AI in Undermining Electoral Integrity: A Study on AI-Driven Election Interference.”
[vii] Momeni, “Artificial Intelligence and Political Deepfakes: Shaping Citizen Perceptions Through Misinformation.”
[viii] Coeckelbergh, *AI Ethics*; Imran et al., “The Role of Generative AI in Undermining Electoral Integrity: A Study on AI-Driven Election Interference.”
[ix] Imran et al., “The Role of Generative AI in Undermining Electoral Integrity: A Study on AI-Driven Election Interference.”
[x] Coeckelbergh, *AI Ethics*.
[xi] Kushwaha et al., “Up in the Air: Ensuring Government Data Sovereignty in the Cloud.”
[xii] Coeckelbergh, *AI Ethics*.
[xiii] Images of Donald Trump were circulated online in 2023 \" Onder and Koç, “DISINFORMATION WITH ARTIFICIAL INTELLIGENCE IN ALGORITHMIC SOCIETIES:AN ANALYSIS OF POLITICAL LEADERS.”
[xiv] Kemal Kılıçdaroğlu was a target of disinformation images and videos in Turkey \" Onder and Koç, “DISINFORMATION WITH ARTIFICIAL INTELLIGENCE IN ALGORITHMIC SOCIETIES:AN ANALYSIS OF POLITICAL LEADERS.”
[xv] Jansen et al., “Pushing Boundaries: An Empirical View on the Digital Sovereignty of Six Governments in the Midst of Geopolitical Tensions.”
[xvi] Mansur, “AI and Cyber-Enabled Threats to Democracy through Algorithmic Manipulation and Generative AI in Undermining Democratic Integrity.”
[xvii] Cupać et al., “Democratization in the Age of Artificial Intelligence: Introduction to the Special Issue.”
[xviii] Gibson et al., “Learning Theories for Artificial Intelligence Promoting Learning Processes.”
[xix] Judge and Korhani, “A Moderate Proposal for a Digital Right of Reply for Election-Related Digital Replicas: Deepfakes, Disinformation, and Elections.”

PETITIONS

Withdraw petition

e-6854

Awaiting authorization for publication

Submitted on October 1, 2025, at 11:53 a.m. (EDT)
The e-petition will be open for signature for 120 days following its publication on the petitions website.

Petition details

Petition to the House of Commons in Parliament assembled

Whereas:

- The Online Streaming Act (C-18) excludes “content of social-media creators, including podcasts,” yet studies show recommendation algorithms—especially for political content—can raise affective polarization up to 54% and boost partisan video viewing by 37%.
- The Standing Committee on Canadian Heritage (National Forum on the Media, 2024) found recurring media crises where digital-first outlets lie outside regulatory frameworks, threatening informed democratic discourse.
- Without legal requirements, platforms may keep using opaque recommendation systems that create echo chambers and amplify harmful or misleading content, undermining safety and citizenship.
- The Online Harms Act (Bill C-63) (not enacted) proposed labelling for bot-distributed harmful content to curb disinformation while respecting free expression.
- Labelling rules should explicitly cover AI-generated content as well as bot-disseminated material.

We, the undersigned, **Citizens and Residents of Canada who value a healthy, deliberative democracy,**, call upon the **House of Commons in Parliament assembled** to 1. Amend the Online Streaming Act — Modify §9.1(1)(e) and §9.1(8) to expressly include podcasts and social-media-style creators.

2. Pass an Online Transparency Act (drawing on Bill C-63) with key provisions:

- Algorithmic transparency: require platforms to disclose recommendation logic/data sources for political content and submit quarterly reports on algorithm changes, reach metrics, and harms.

- Label bot-disseminated harmful content: require labels where content is automated and gains undue prominence via bots.

- Label AI-generated content: require clear, user-readable labels for content produced or substantially altered by AI.

3. Enforcement: empower the Minister of Innovation, Science and Industry to impose fines, injunctions, or other remedies scaled to breach severity and public-safety/democratic impact.

4. National oversight body: create a Parliament-co-appointed regulator to review reports, investigate complaints, and advise on policy as technology evolves.

Supporters

- ☑ Mark Woodland (*mark_woodland@yahoo.com*)
- ☑ Julie Trus (*j.a.Trus@hotmail.com*)
- ☑ Matthew Harrison (*matt_harrison@bell.net*)
- ☑ John Willson (*johninparis@gmail.com*)
- ☑ Lynn Shwadchuck (*lshwadchuck@gmail.com*)

Member of Parliament

✗ Declined by Jenny Kwan on October 31, 2025, at 3:50 p.m. (EDT)

Choose a new Member of Parliament

History

Disclaimer regarding petitions