Beyond Infrastructure: A Rights-Based Approach to AI Governance in Canada

Submission to the Standing Committee on Industry and Technology (INDU), in their study on *Opportunities, Risks, and Regulation of AI in Canada's Strategic Industries*

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

June 3rd, 2026

Authors: Jennifer Turliuk, David Fewer, and Kunal Pandya. Contributor: Aaranya Alexander

About CIPPIC

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is Canada's first and only public interest technology law clinic. Based at the Centre for Law, Technology and Society at the University of Ottawa's Faculty of Law, our team of legal experts and law students works together to advance the public interest on critical law and technology issues including privacy, free expression, intellectual property, telecommunications policy, and data and algorithmic governance.

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
57 Louis Pasteur St.
Ottawa, Ontario K1N 6N5
www.cippic.ca

Executive Summary

Artificial intelligence presents Canada with a genuine strategic opportunity - and a real accountability crisis. Canada has world-class AI research talent, established institutions, and a rights-centred legal tradition. What Canada lacks is an AI legal framework that reflects our strongest traditions: rights, accountability, and the rule of law.

CIPPIC, Canada's only public interest technology law clinic, offers this brief to argue that Canada's AI strategy will fail on its own terms - economically and democratically - unless it is grounded in rights, accountability, and the rule of law. Legal certainty is an economic asset. The absence of a robust framework drives innovation elsewhere, leaves Canadians unprotected, and risks Canada's adequacy status under EU privacy law with consequences for transatlantic data flows and Canadian competitiveness.

Much of the evidence before this Committee has focused on infrastructure, sovereignty, and industrial competitiveness. This brief addresses issues from innovation to intellectual property, privacy, the rule of law, and the environment - with particular focus on areas that have received comparatively little attention in the Committee's proceedings: civil liability for AI harms, the failures of the existing Directive, Indigenous data sovereignty, constraints of the CUSMA review, and Canada's GDPR adequacy risk. This brief focuses on areas where CIPPIC has unique expertise to contribute, while recognizing that a complete AI framework must address autonomous and physical AI, military, and catastrophic risks.

CIPPIC urges the Committee to recommend federal AI legislation that is rights-based, risk-tiered, and enforceable. Such legislation should:

- Convert the *Directive on Automated Decision-Making* into statutory rights
- Create civil liability for AI harms and private rights of action for individuals affected
- Establish transparency and accountability obligations
- Protect privacy for data sharing with AI systems
- Enact laws that respect OCAP principles to promote Indigenous data sovereignty
- Ensure government AI use is consistent with the *Charter* and the rule of law
- Affirm that copyright and patents require human authorship and inventorship, while confirming a scoped text and data mining exception

Canada has the legal tradition, the talent, and the institutional capacity to be a global leader in trustworthy AI. The question is whether Parliament will act before the window of opportunity closes.

Background: The Need for AI Legislation

Legal certainty is an economic asset. Canada's trading partners are offering their citizens and industry that certainty. Canada should as well. With dozens of jurisdictions globally - including the European Union, China, and other key trading partners - actively implementing formal AI frameworks, Canada's legislative delay increasingly isolates our domestic tech sector. Reactive, voluntary frameworks create public anxiety, increase legal uncertainty for businesses, and stall commercialization. These frameworks also fail to protect *Charter* rights from algorithmic harms in sectors such as security, health, and immigration.

Relying on an existing patchwork of laws that are not meant specifically for AI is insufficient; new harms unique to AI require additional regulation. The longer Canada waits to introduce robust AI legislation, the more AI-related harms may occur, and the less competitive Canada could become.

Recommendations

1) How to Approach Canadian AI Legislation

1.1. Legislate AI at the federal level - There is a need for federal legislation versus a patchwork of provincial laws that would be difficult for companies in the AI space to follow. In areas of federal jurisdiction, Canada should have federal legislation for AI.

1.2. Align with the EU AI Act - Canada should consider adopting the regulatory model of the *EU AI A*ct and complying with its provisions. While AIDA represented an important first attempt at federal AI legislation, its definitions, governance structure, and enforcement model attracted substantial criticism. Future legislation should build on lessons learned rather than reintroducing.

Canada should adopt a risk-based framework inspired by the *EU AI Act* while ensuring compliance obligations remain proportionate for open-source development. Canada should have a risk classification matrix of harms as the EU does but grounded in Canadian legal traditions and the public interest. Different AI systems have various levels of risk and require differentiated treatment.

The *EU AI Act*'s regulatory approach imposes positive obligations on its member states regarding the importing and usage of AI. This approach differs from those in the US and China. The US has taken a deregulatory approach, focusing on innovation and not constraining early development; yet there is a patchwork of state laws with varying levels of obligation. China employs a state-led, centralized, vertically integrated, and action-oriented governance model, in contrast to the fragmented approach of the US.

1.3. Align with international standards and frameworks - Canada should comply with internationally recognized AI standards and frameworks such as the OECD AI principles, NIST AI Risk Management Framework, UN principles for AI, ISO AI risk management standard, and ISO AI impact assessment. The *EU AI Act* largely complies with these standards and frameworks. Complying with them signals internationally that the country intends to respect responsible AI use and reduces risk for companies and consumers.

1.4. Align trade agreements with public policy - Canada should proactively leverage the upcoming CUSMA review to negotiate a specific exemption for "Public Interest Algorithmic Audits." This will ensure that the current CUSMA Article 19, which prohibits requiring the disclosure of source code, does not inadvertently immunize foreign "black box" models from the domestic safety and transparency audits necessary to protect Canadian public safety and human rights.

1.5. Promote public trust through transparency, explainability, and public accountability - There is a need for transparency and enforcement. Canada should create AI safety evaluations, AI transparency legislation, public reporting obligations, model and dataset disclosures, and notice requirements for when AI is used in significant decisions. Reporting requirements must address the “black box” barrier of AI, including a requirement for companies to disclose policies on user account bans or police reporting. This could help prevent further incidents such as the OpenAI / Tumbler Ridge incident.

1.6. Create individual rights and redress, and civil liability for AI harms - AI regulation should be grounded in human rights rather than just commercial law. Canada’s AI legislation should address the rights citizens have when an AI system harms them or makes a consequential decision about them, which entities are liable, and what meaningful redress includes. Canada should introduce rights-based AI regulations like those in the EU, including algorithmic transparency requirements, and data localization for sensitive sectors - as well as provisions regarding bias, discrimination, and youth. High-risk AI must respect fundamental rights. Regulatory tools can help achieve this, including mandatory impact assessments, human review rights, restrictions on automated decisions, protections for vulnerable groups, and safeguards in government use.

1.7. Provide AI assurance and independent oversight - Canada’s AI legislation should be insulated from industry lobbying and develop in an independent and transparent legislative process, and mandate public-interest oversight, transparent audits, complaint mechanisms, and regulatory accountability.

Beyond static, pre-deployment Algorithmic Impact Assessments (AIAs), Canada must mandate a "Run-Time Layer of Control" for AI systems deployed in safety-critical strategic

sectors, such as energy grids, telecommunications, and healthcare. Unlike traditional software, physical AI systems learn and adapt post-deployment, creating lifecycle risks that static checks cannot mitigate. A run-time layer acts as a technical "kill switch," continually observing system behaviour and intervening in real-time if an agent initiates unauthorized processes or evades human instructions.

1.8. Do not govern with a sole AI regulatory authority - Similar to how Canada does not have a single internet regulatory authority, Canada should not have one AI regulatory authority. AI affects different sectors, so government departments and regulators must possess AI capacity relevant to their jurisdictions. For example, the government must support the Office of the Privacy Commissioner of Canada in its need to develop capacity related to AI's implications for privacy rights.

1.9. Regulate public sector use of AI - Canada's AI legislation must address the rights Canadians have when a federal or provincial AI system makes or informs a decision affecting them, e.g., when the government uses AI in immigration, tax assessment, benefits, policing, or border services. There are structural issues with the *Directive on Automated Decision-Making*, which Canada has had since 2019 and requires federal institutions to complete Algorithmic Impact Assessments before deploying automated decision systems, with explanation and human review rights scaling with impact level. It applies only to the federal public service; compliance is self-assessed with no audit or enforcement; its impact level thresholds predate generative AI and no longer reflect actual risk; and individuals have no private right of enforcement when departments fail to comply. Canada's AI legislation should convert the Directive principles into statutory rights applying across sectors - mandatory Algorithmic Impact Assessments, explanation and human review rights, independent audit authority, and a private right of action. It should also resonate with *Charter* values. Procedural fairness, the right to reasons, and judicial review must apply (as appropriate to the import of the decision) to government AI systems, which do not map cleanly onto doctrines designed for human decision-makers.

2) AI and Sovereignty

2.1. Prioritize Canadian commercialization of AI innovation - Create a publicly owned national compute utility, tying public funding to IP retention within Canada. Canada has been a pioneer in AI research, but commercialization of Canadian AI technology has largely happened in the US and elsewhere. The government needs to ensure that Canada's AI innovations boost Canada's GDP. Canada should look to stimulate the creation of domestic AI companies instead of becoming a regional market for large US AI companies. Contributing factors include talent education, attraction, and retention; IP development; private/VC funding; access to compute resources, etc.

2.2. Establish Canadian data sovereignty - Data sovereignty without legal rights is not meaningful sovereignty. Sensitive Canadian data should be kept in domestic jurisdiction. Standard data residency does not protect Canadian data from foreign legal overreach (like the U.S. CLOUD Act) if the corporate infrastructure relies on international parent companies or data brokers. True sovereignty requires that critical infrastructure be hosted on systems that are 100% Canadian-owned and managed, ensuring that sensitive Canadian industrial data and personal information remain exclusively under Canadian jurisdiction and are not subject to exfiltration by foreign parent companies. Canada's AI strategy should be grounded in democratic accountability, privacy, transparency, and human rights. Investments in AI infrastructure and industrial competitiveness should be matched by equally robust protections for Canadians affected by AI systems.

2.3. Promote Indigenous data sovereignty - Canada should codify respect for Indigenous autonomy and control consistent with OCAP principles (Ownership, Control, Access, and Possession), so that Indigenous communities can maintain autonomous control over their cultural data. A truly sovereign framework must respect these principles, ensuring that Indigenous communities retain authority over their data and cultural knowledge.

3) AI and the Rule of Law

3.1. Regulate the use of AI in law - AI is being used in legal environments – in adjudicative settings and by lawyers and self-represented litigants for legal research and drafting. Such use raises access to justice considerations. Canada should mandate how AI can be used in legal environments and disclosure requirements when it is used.

3.2. Regulate the use of AI in democracy - Specific legal and regulatory tools are needed, including liability for synthetic media, and rules regarding election communications, voter deception, political advertising, content provenance, and campaign transparency.

4) AI and Climate and Energy

4.1. Regulate the environmental impacts of AI - AI poses meaningful climate harms that worsen climate change. Climate harms at scale undermine the economy. In Ireland, data centers already consume 20% of electricity (Wired). Canada should implement a meaningful carbon price (widely considered the most effective climate change solution), require the disclosure of AI use and environmental impacts (California has introduced legislation along these lines), regulate AI-related emissions and resource use, promote energy efficiency, stimulate renewables, and prevent AI greenwashing (Turliuk & Sterman). Algorithmic Impact Assessments should include a mandatory Environmental Footprint Assessment (measuring compute efficiency, projected water utilization, and grid load) before a large or high-impact system can be cleared for procurement or high-risk

commercial deployment. Other jurisdictions have a right to a healthy environment in their constitutions and Canada should consider the same.

4.2. Invest in innovation that reduces the environmental impacts of AI - Canada should focus on environmentally sustainable solutions and investment into innovation that reduces the climate impacts of infrastructure, hardware, and software. Examples include additional renewable energy and the introduction of green data centers.

5) AI and Innovation

5.1. Provide education and frameworks on using AI to boost productivity - Canada's productivity has gone down and is lower than that of other geographies. AI is predicted to help boost economic productivity. However, AI has been shown to decrease productivity in some cases. Canada should provide education to workers on how to boost productivity using AI. Canada should identify barriers to AI adoption in strategic sectors and the specific regulatory frameworks required to foster trust and competition.

5.2. Stimulate domestic AI capacity - There is a need for domestic compute capacity e.g., chips, data centers, energy, etc. Canada must provide this or risk companies and innovators going elsewhere.

5.3. Public procurement as an engine - The government should be a first customer for promising AI companies; currently many Canadian companies sell to other countries first due to not being able to access the Canadian government (Ottawa Business Journal).

5.4. Encourage domestic AI models that are open rather than closed - Encourage AI models that are open, rather than closed. This approach can help boost innovation.

5.5. Provide open funding calls for AI - Funding opportunities should involve open calls for submission rather than cherry-picking known companies.

6) AI and Education/Workforce

6.1. Build Canadian AI workforce capacity - There is a need for upskilling. Invest in stable core funding for Canada's AI strategy for recruitment and training.

6.2. Introduce initiatives to attract foreign AI innovators - Canada should work to attract foreign innovators and academics through funding and targeted recruitment.

6.3. Provide AI literacy training for each citizen - Provide free AI education for each citizen, like Singapore has done. Include training on topics such as privacy, misinformation, deepfakes, AI hallucination, bias, AI safety, mental health impacts of AI, rights when engaging with AI systems, using AI for productivity, and preventing cognitive decline and moral suasion from usage of AI, etc.

6.4. Address labour impacts of AI - Canada's unemployment is rising. AI is expected to affect labour markets and may contribute to displacement in some occupations. Canada must address AI's labour impacts by creating a labour strategy that includes reskilling training, welfare payments for potential unemployment, taxation, etc.

7) AI and Intellectual Property

7.1. Prohibit patent protection for purely AI-generated assets - Under current Canadian law, inventors must be natural persons. This should be maintained. Where AI is the sole inventor without meaningful human inventive contribution, no patent should issue. CIPO should develop clear guidance on the line between unpatentable AI-generated and patentable AI-assisted inventions.

7.2. Maintain copyright's requirements for a human author - Canada's current position - that AI-generated content is unprotected by copyright - is correct because it recognizes that copyright arises from the creative act of authorship. Where a human elaborates on an AI output by contributing additional original expression, copyright can attach to those contributions. Whether purely AI-generated outputs warrant legal protection is a question for Parliament. If warranted, Parliament can design a *sui generis* regime to suit the market, cultural, and public interests engaged by those outputs.

7.3. Create a formalized Text and Data Mining (TDM) exception to data mining – Canada should amend the *Copyright Act* to include a tailored safe harbour for text and data mining where the user has lawful access to the work and uses it for computational analysis, model development, or training. The exception should not require individual permission or a general licensing scheme. A permission-based model would let the content industry control who may train AI systems, favour incumbents, exclude SMEs and academic researchers, and chill socially valuable innovation. If Parliament wants rightsholder compensation, the better model is a permissionless statutory remuneration regime: users retain the right to conduct TDM, while eligible rightsholders may claim compensation through a collective mechanism. Amendments should include an obligation for developers to disclose enough information about training datasets to support accountability, rights enforcement, and informed policy.

8) AI and Privacy

8.1. Address cybersecurity concerns - Provide legislation, guidance, and appropriate cybersecurity measures regarding foreign AI models and protect against AI threat actors.

8.2. Comply with EU AI Act privacy standards - Canada should proactively seek an adequacy assessment under the *EU AI Act* framework. Canada's PIPEDA adequacy status under the EU GDPR is not guaranteed if Canada's privacy and AI framework falls

significantly behind EU standards. A weakened or delayed privacy law, combined with no AI Act equivalent, risks Canada losing its adequacy finding - which would have enormous consequences for data flows and the tech sector. Losing adequacy would significantly increase compliance costs and legal uncertainty for Canadian firms engaged in transatlantic data transfers.

8.3. Ensure users' rights to privacy in AI data processing - Laws should address users' rights regarding meaningful consent, automated decision-making, AI-generated inaccuracies, and limits on training models with personal information - as well as enforcement powers for privacy regulators. Legal limits - "red lines" - should also be placed on workplace surveillance. People and companies are sharing their most personal details with AI, yet AI privacy policies regularly change without meaningful user consent. There is a problem of intimate data flowing into AI systems - including financial information, relationship details, health, and mental health disclosures - and consent and purpose-limitation frameworks must address this.

Conclusion

Canada is at an important moment. The country that produced foundational AI research, that trained much of the world's AI talent, and that was first to propose a national AI strategy now risks being the last among its peers to translate those advantages into a coherent legal framework. The cost of delay is the accumulation of harms without recourse, the erosion of public trust, the flight of innovation to jurisdictions with clearer rules, and the potential loss of Canada's adequacy status under European privacy law.

The submissions and testimony before this Committee have made the case for infrastructure, compute capacity, and industrial competitiveness with force and detail. CIPPIC argues that this paints only half of the picture. Canadian data centres and Canadian compute capacity are worth building. But they do not, on their own, protect Canadians from AI systems that discriminate, surveil, deceive, or make consequential decisions without explanation or recourse. Infrastructure sovereignty and legal sovereignty are different things, and Canada needs both.

Canada's AI future will be shaped by the choices Parliament makes, or fails to make, in the coming years. CIPPIC urges this Committee to recommend legislation that makes Canada not merely a participant in the global AI economy, but a model for how democratic societies can govern it.

CIPPIC remains available to assist the Committee in that work.