The Standing Senate Committee on Transport and Communications

Study on the opportunities and challenges of artificial intelligence (AI) in the information and communication technology sector

Submission of Emily Laidlaw, Canada Research Chair in Cybersecurity Law and Associate Professor, University of Calgary (May 2026)

The broad scope of the Committee's study makes it possible to step back and ask: what would a healthy, resilient AI ecosystem look like for Canada? More specifically, what legal building blocks are needed to support it? The starting principles are as follows:

- Innovators and investors should have regulatory certainty about their compliance obligations in Canada.
- Our laws should provide rigorous accountability while remaining practical and avoiding needless complexity for businesses.
- Canada should strengthen digital sovereignty by investing in Canadian talent and training, reducing dependence on US-based technology companies, and developing strategic international partnerships.
- The cyber threats that AI can both exploit and help address should be governed within an appropriate framework built on trust and accountability.
- Individuals harmed by AI should have meaningful avenues for legal redress.
- Systemic discrimination embedded within AI systems should be identified, exposed, and remedied, while ensuring that the systems themselves are appropriately corrected and safeguarded against reproducing such biases.
- All levels of government—federal and provincial, and across departments and agencies—should work in coordination.
- Canadians should be educated about AI, cybersecurity, and information manipulation.

How can law help Canada achieve these goals? In short, we must respond to the demands of this moment.

Digital Coherence

As a starting point, Canada cannot continue to rely on outdated, piecemeal laws to address the scale and speed of AI. This point was emphasized by several privacy commissioners in the recent investigation of OpenAI's ChatGPT, noting that old laws were

being shoehorned to fit new circumstances.[1] Canada needs coherent and comprehensive digital laws, grounded in a whole-of-government and whole-of-society strategy. This means laws should not be drafted in isolation—whether because government agencies operate in silos or because federal and provincial governments legislate without sufficient coordination.[2] We also know that technology has always outpaced law, but that dynamic has accelerated substantially with the mainstreaming of AI. We should therefore start thinking about law-making differently: as modular, iterative, and nimble enough to respond to evolving technologies and social contexts. This translates into the following priorities.

Regulatory certainty is central to Canada's ambition to drive AI innovation and build global economic partnerships. The Government of Canada should therefore prioritize passing comprehensive digital laws and do so with careful attention to how they fit together. In recent years, several bills have been introduced to amend, replace, or create new laws relating to privacy,[3] AI,[4] online harms,[5] critical infrastructure,[6] age verification,[7] and consumer protection/competition.[8] Together, these initiatives address different dimensions of the AI policy challenge.

---

[1] See Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Information and Privacy Commissioner of Alberta, *Joint Investigation of OpenAI OpCo, LLC* (May 6, 2026), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2026/pipeda-2026-002/.

[2] A recent example is exploration of a social media and chatbot ban, with both the Government of Canada and Manitoba potentially legislating in this area, which may result in conflicting laws, creating a burdensome and complex regulatory space for companies, which coordination and collaboration, within governments' spheres of power, can minimize.

[3] Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Session, 44th Parliament, 2022.

[4] *Ibid*.

[5] Bill C-63, *An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts*, 1st Session, 44th Parliament, 2024.

[6] Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Session, 45th Parliament, 2025.

[7] Bill S-209, *An Act to restrict young persons' online access to pornographic material*, 1st Session, 45th Parliament, 2025.

[8] There have been various amendments to the *Competition Act*, RSC 1985, c C-34, in recent years, but most on point here is the Bill 49 recently introduced in Manitoba to address personalized algorithmic pricing, *The Business Practices Amendment Act*, 3rd Session, 43rd Legislature, 2026. See also my co-authored study of the economic impacts of price discrimination, summarized here, with a link to the article therein: Raymond A. Patterson, Jian Zhang and Emily Laidlaw "Price discrimination is getting smarter and low-income consumers are paying the price" (11 April 2025), The Conversation, https://theconversation.com/price-discrimination-is-getting-smarter-and-low-income-consumers-are-paying-the-price-252723.

Privacy and cybersecurity law form the foundation, because AI runs on data and can both intensify cybersecurity threats and assist in addressing them, as recent reporting on Anthropic's Mythos model suggests.[9] Canada has had public- and private-sector privacy laws for decades, but many have not been meaningfully updated. New on the block are AI and online harms laws, which have adopted a risk-management approach to regulating AI systems and digital platforms. Two bills that died with prorogation—Bill C-27 (including the Artificial Intelligence and Data Act) and Bill C-63 (the Online Harms Act)—were built on the premise that companies should be obligated to act diligently to mitigate the risks associated with the products and services they put out into the world. The devil is in the details, but the conceptual framework is sound and, at least for now, represents the leading model for regulating these technologies and the social challenges they generate.

Interoperability with other legal regimes is also essential. Technology is global, and a secure and resilient Canada depends on cooperation with others. This does not mean that our laws are the same, but that they have certain features in common and compatible underlying concepts. For example, risk-management duties are emerging as a common feature of AI and online harms legislation in numerous jurisdictions, which is why that foundation is so important for any law Canada adopts.[10]

AI-Facilitated harms

My colleague Florian Martin-Bariteau and I recently published a co-edited book, *Security of Self: A Human-Centric Approach to Cybersecurity*.[11] The book brings together scholars from various disciplines to examine the consequences of shaping cybersecurity policy and practice around national security and organizational risk, while paying minimal attention to the humans in the system except as weak links to be managed. A human-centric approach shifts the frame and places people at the centre as the objects of security—as a feature, not a bug, of the cyber environment. This more holistic perspective requires understanding how people work and think, and then building systems and policies around that reality, not only to protect people from threats but also to enable them to thrive.

---

[9] See Anthropic's Project Glasswing, https://www.anthropic.com/glasswing.

[10] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 22 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)*; *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*.

[11] (University of Ottawa Press, 2025), available open access at this link: https://press.uottawa.ca/en/9780776645605/the-security-of-self/.

Security of Self is a helpful lens through which to examine AI-facilitated harms. OpenAI and Character.AI have faced lawsuits after children took their lives following alleged encouragement from chatbots, in the latter case after the interactions with the chatbot became sexual.[12] Adults have also reported severe mental health crises associated with AI use.[13] A human-centric approach would ask, ideally before a product is launched: who are the most vulnerable users, and how might they be affected by this product? What safety features should be built into the tool to mitigate those risks? More broadly, what do we know about human psychology that can help us understand how people are likely to experience this product? Interactions with chatbots, for example, differ from curated social media posts or private group messaging. It is intimate and unguarded, at times feeling more like an invitation into our inner minds than what we choose to outwardly express or display.

A similar dynamic appears across a great swath of AI systems, from the design of a tool or application to its integration within an existing platform, which in turn points to the need for an ecosystem-level approach to AI-facilitated harms. For example, X's Grok AI tool allowed users to create intimate deepfakes by 'nudifying' real images of women and depicting them in sexually violent ways, including with a ball gag, bruising and blood.[14] The ease with which these deepfakes could be generated through Grok was itself one problem. The integration of Grok within X compounded the risks and harms, because images posted to X could be scraped and altered, and the same platform could then be used to amplify the images to the far corners of the world.

These examples reinforce the need for safety by design and risk-management measures, both of which appear in different forms in emerging AI and online harms laws. They demand proactive assessment, monitoring, and responses to risk. At the same time, risk management for AI—and for digital technologies more broadly—operates differently from risk management in domains such as finance or insurance, from which the model derives.[15] The term 'information technology' seems to have fallen out of use, but it serves as a helpful reminder that technology is about information. Information is something we

---

[12] *Garcia v character.ai* has settled, but it is helpful to read the initial the reasons of the court denying a motion to dismiss, available at this link: https://press.uottawa.ca/en/9780776645605/the-security-of-self/. The lawsuit of the family of Adam Raine against OpenAI is ongoing, and the statement of claim is available at this link: https://www.courthousenews.com/wp-content/uploads/2025/08/raine-vs-openai-et-al-complaint.pdf.

[13] Marlynn Wei, "The Emerging Problem of "AI Psychosis" (November 27, 2025), *Psychology Today*, https://www.psychologytoday.com/ca/blog/urban-survival/202507/the-emerging-problem-of-ai-psychosis.

[14] Amelian Gentleman and Helena Horton, "'Add blood, forced smile: how Grok's nudification tool went viral" (January 11, 2026), *The Guardian*, https://www.theguardian.com/news/ng-interactive/2026/jan/11/how-grok-nudification-tool-went-viral-x-elon-musk.

[15] Margot E. Kaminski, "Regulating the Risks of AI" (2023) 103 Boston University Law Review 1347.

seek, receive, produce, and share in the exercise of freedom of expression, and it is vulnerable to weaponization and surveillance, impacting privacy and equality. AI is also used to automate decision-making, obscuring reasoning in a black box, undermining due process. The takeaway is that the foundation of AI risk management should be fundamental rights. This is new territory, and embedding risk management into law is the first step in what must be a carefully calibrated approach centred on human flourishing and fundamental rights.

Recommendations

- Adopt a coordinated, whole-of-government and whole-of-society approach to digital law-making, ensuring that privacy, AI, online harms, and related laws are developed in tandem—not in isolation—to enhance coherence and regulatory certainty.
- Expedite the introduction and passage of updated private sector privacy and online harms legislation, with a focus on risk management, accountability, and robust safeguards for vulnerable populations.
- Launch broad consultations on the development of a general-purpose AI law that is modular, iterative, and nimble, capable of keeping pace with evolving technologies and social contexts.
- Undertake a comprehensive study of AI risk management frameworks, prioritizing the protection of fundamental rights and embedding a human-centric perspective that centres on safety by design, proactive risk assessment, and the flourishing of all individuals.