

August 26, 2024

The Honourable Todd J. McCarthy
Minister of Public and Business Service Delivery and Procurement
College Park 5th Floor, 777 Bay St.
Toronto, ON M7A 2J3

Re: Bill 194, *The Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*

Dear Minister McCarthy,

It was a pleasure to host you earlier this year to discuss the impact of Artificial Intelligence (AI) on Ontario's economic future. Since our meeting, we have been pleased to see the Ontario government take steps to enhance cybersecurity and tackle the emerging risks associated with AI adoption in the public sector through [*Bill 194, The Strengthening Cyber Security and Building Trust in the Public Sector Act*](#).

Trust is a critical enabler of technology adoption, and we are encouraged by this positive development in implementing stronger accountability and transparency standards. These measures align with recently amended legislation in [Québec](#), [British Columbia](#), and other jurisdictions.

However, we have concerns about the lack of enforcement mechanisms for non-compliance, ambiguous requirements, limited public consultation opportunities, and the potential for overly prescriptive standards that could hinder innovation and economic growth, particularly for SMEs.

In consultation with our [AI Hub](#) Steering Committee, the Ontario Chamber of Commerce (OCC) proposes the following recommendations, which balance accountability and safety with adoption, innovation, and economic opportunity.

Recommendations

1. Adopt a principles-based approach to privacy and the use of AI technologies.

The AI provisions in *Schedule 1* aim to regulate evolving technology by deferring detailed rulemaking to regulation. While this approach offers flexibility, it is essential to establish a principles-based framework that aligns with societal norms and values, ensuring rules are adaptable yet grounded in protecting Ontarians' fundamental human rights.

We recommend amending the proposed legislation to include statutory language that defines the basic parameters for future regulations. This should involve codifying clear statutory principles for public sector AI systems to ensure they are valid, reliable, safe, privacy-protective, transparent, accountable, and affirming human rights. This approach would provide necessary assurances to earn and maintain public trust in AI use while allowing for flexibility through additional regulations or technical standards.

2. Adopt a risk-based approach to regulation.

Many emerging AI regulatory regimes worldwide, like the [EU AI Act](#), adopt a risk-based approach. The rules and obligations for organizations developing or deploying AI systems vary based on the level of risk and potential harm to businesses and communities. Not all risks are created equal and focusing resources and requirements on the greatest risks is important.

We recommend the government adopt a risk-based approach with a frequent gap analysis to identify emerging and ongoing risks in AI use. This approach would offer the necessary flexibility for AI adoption and deployment while ensuring regulatory frameworks are periodically updated and calibrated for risk to provide appropriate protection for individuals and groups.

3. Develop interoperable privacy laws and standards in consultation with impacted stakeholders.

Alignment with frameworks such as the EU's [General Data Protection Regulation \(GDPR\)](#) and the upcoming federal [Consumer Privacy Protections Act \(CPPA\)](#) will support the adoption of globally recognized cybersecurity and privacy standards within Ontario's public sector. Interoperable privacy laws and standards can reduce ambiguity, minimize administrative burdens, and enable Ontario businesses to develop global compliance strategies, fostering greater competition. Before implementing an accountability framework, we recommend further consultations with industry, academia, legal experts, and the Information and Privacy Commissioner of Ontario (IPC), given the evolving nature of AI technologies.

4. Strengthen the governance and enforcement mechanism for effective implementation.

As currently drafted, Bill 194 lacks meaningful enforcement mechanisms for non-compliance. We recommend that the government develop a robust governance framework, including regulations, policies, risk management frameworks, and technical standards. At the same time, it will be crucial to provide public sector employees with the necessary training and resources, engaging technical experts for hands-on experience and guidance on responsible technology adoption and best practices.

A robust enforcement regime would also instill public trust in the legislation and the government's AI use. This could involve establishing an independent commissioner or regulator, such as Ontario's Information and Privacy Commissioner (IPC), with sufficient resources, regulatory oversight powers, and policy and technical expertise to ensure effective implementation across Ontario's public sector.

5. Balance privacy protection and business opportunity.

Ontario-based companies, especially SMEs, need access to data to compete and innovate in AI and analytics. Enhanced public data access drives economic growth and social good, but a system of checks and balances must ensure its use serves the public interest. Strict data minimization laws disproportionately benefit large, established companies and hinder new market entrants.

To foster competition and consumer interest, Ontario's governance frameworks should incentivize data portability and access, avoiding unnecessary restrictions on data transfers while ensuring accountability and security.

The government should also prioritize operationalizing the Ontario Data Authority (ODA) to implement effective data stewardship models, governance, and standards, as outlined in its first [*Digital and Data Strategy*](#). The ODA should develop and enforce data governance standards, enhance data security protocols, facilitate secure and ethical data sharing, provide independent analysis, and promote stakeholder engagement and transparency. A balanced approach will ensure responsible and accountable AI use, build public trust, and support market fluidity, fostering a competitive, innovative market environment while protecting individual rights.

6. Enhance transparency to build public trust.

As outlined above, as AI is deployed and used across Ontario, we must build an ecosystem of public trust. AI developers must transparently disclose system capabilities, behaviour, and limitations. A robust policy framework can balance privacy, cybersecurity, and public safety while fostering cross-organizational partnerships, reducing capacity challenges, and ensuring continued business competitiveness.

We appreciate the government's initiative to introduce legislation that keeps pace with rapidly evolving technology and addresses the specific risks and harms within provincial oversight. As the indispensable partner of business, representing over 60,000 businesses across the province, the OCC and its members are eager to participate in shaping this legislation. Further, we look forward to contributing to related regulations and directives to support secure and responsible technology governance in Ontario.

Sincerely,



Daniel Tisch, APR, FCPRS, ICD.D
President and CEO
Ontario Chamber of Commerce