

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

**Law Commission of Ontario Submission**

**June 2024**



LAW COMMISSION OF ONTARIO  
COMMISSION DU DROIT DE L'ONTARIO



LAW COMMISSION OF ONTARIO  
COMMISSION DU DROIT DE L'ONTARIO

## Law Commission of Ontario Submission To Government of Ontario Bill 194 Consultations

June 11, 2024

### 1. Introduction

This is the Law Commission of Ontario's submission to the Government of Ontario's request for comments on Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*. The LCO is only commenting on the artificial intelligence sections of the proposed legislation.

### 2. About the LCO

The Law Commission of Ontario (LCO) is Ontario's leading law reform agency.

The LCO provides independent, balanced, and authoritative advice on complex and important legal policy issues. Through this work, the LCO promotes access to justice, evidence-based legislation and policies, and public engagement on important issues. The LCO is independent of stakeholder interests and is committed to a "public interest" perspective for every project.

The LCO has unparalleled experience analyzing AI, regulation, and the public sector. Recent LCO reports addressing these issues include:

- [Accountable AI](#) (2022)
- [Regulating AI: Critical Issues and Choices](#) (2021)
- [Legal Issues and Government AI Development](#) (2021)
- [The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada](#) (2020)

In addition, the LCO is currently undertaking two projects relevant to Bill 194 and this submission. The first is a project to develop an AI human rights impact assessment. The second is a project to evaluate the potential use and regulation of AI tools in Ontario's criminal justice system.

Many of the lessons and recommendations in this submission are drawn from these reports. This work is part of the LCO's ongoing [AI and the Justice System](#) project. More information about the LCO and this project is available at [www.lco-cdo.org](http://www.lco-cdo.org).

### 3. Summary of LCO Submission

Provincial public sector AI systems have the potential to affect the most significant issues and interests in Ontarian's lives, including their personal liberty, education, employment, health care, housing, access to economic opportunities, and income security.

Experience in other jurisdictions repeatedly demonstrates the need for comprehensive and thoughtful public sector AI legislation and regulations. The Government of Ontario can become a leader in successful AI deployment by applying hard-learned lessons to ensure trustworthy and accountable public sector AI systems in our province.

The context and background for AI governance is changing rapidly. AI legislation and regulations are much more sophisticated today than they were even three or four years ago. Initiatives such as the EU *Artificial Intelligence Act*, legislation and regulations in the United States, and the Government of Canada's *Artificial Intelligence and Data Act* and Directive on Automated Decision-making have established important benchmarks for public sector AI legislation and regulation.

The LCO believes Bill 194 must incorporate these benchmarks if it hopes to regulate public sector AI systems effectively. Unfortunately, as currently drafted, Bill 194 falls short of this ideal. Most critically, the Bill is brief and lacks key provisions needed to ensure public sector AI use is beneficial, lawful, and accountable. More specifically, the Bill does not address several widely acknowledged Trustworthy AI priorities, including:

- Human rights and procedural fairness.
- AI systems used in the criminal justice system.
- AI systems used in courts and tribunals.
- Public AI registries.
- Risk categories and mitigation strategies.
- Impact assessments.
- Explainability requirements.
- Governance.

The Government of Ontario has committed to many of these principles in its own Trustworthy AI Framework and Beta Principles.

These are significant gaps. For example, Bill 194 states that it is important to protect privacy but is silent on the need to protect human rights. Nor does Bill 194 address AI systems used by police or by courts

and tribunals, meaning that these institutions could adopt predictive policing, facial recognition and other forms of biometric surveillance, and automated risk assessments without having to comply with provincial AI accountability requirements.

It is not sufficient to state these issues will be – or might be – addressed in regulations. It is also not sufficient to state that these issues are effectively addressed elsewhere. LCO reports demonstrate the many gaps in existing case law and legislation. Absent legislative guidance/requirements, there is no assurance that regulations will address these subjects. Equally important, as drafted Bill 194 may mean that Ontarians cannot review or participate in significant AI policymaking, as most important decisions are left to regulations.

Comprehensive provincial legislation is necessary to provide the foundational governance framework for public sector AI systems in Ontario. Comprehensive legislation would provide consistent direction and accountability requirements to the actors, departments, and agencies within its scope. It would also ensure changes to the governance framework were subject to legislative and public review. Finally, and most importantly, comprehensive legislation would establish a level of public and legal accountability commensurate with the issues and rights at stake.

The Government of Ontario is at a crossroad: public sector AI systems offer significant potential to improve public services in Ontario. Absent appropriate legislation, however, public sector AI systems may increase bias, reduce accountability, and result in poorer public services.

Whether public sector AI systems are harmful or beneficial will depend on choices and decisions made by the provincial government in the coming months and years.

#### 4. Summary of LCO Recommendations

The LCO's recommendations are summarized in the table on the next page. The LCO's detailed recommendations are included in explanatory text below and in Appendix A.

The LCO's recommendations fall into two categories: First, the LCO recommends several amendments to Bill 194. Second, the LCO recommends the provincial government make several public commitments to assure Ontarians about the process and substance of AI legislation/regulation in Ontario.

Taken together, these recommendations enshrine trustworthy AI principles in Bill 194, address foreseeable risks and harms, and align Ontario with a growing national and international consensus on appropriate AI legislation.

## Summary of LCO Recommendations

1. Trustworthy AI principles should be enshrined into Bill 194.
2. The legislative objectives of Bill 194 should not be restricted to “protecting privacy.” Protecting human rights and complying with procedural fairness are equally important.
3. Bill 194 must address the most significant AI risks, including AI systems used in the criminal justice system (including policing), courts, and tribunals.
4. The province has committed to “no AI in secret.” To fulfill this commitment, Bill 194 must include a mandatory AI registry, disclosure of key elements of public sector AI systems, and disclosures to the person affected by an AI system.
5. The province has committed to developing “accountability frameworks” for public sector AI systems. To fulfill this commitment, Bill 194 must include a provincially mandated impact assessment that addresses privacy, human rights, and procedural fairness and provides assurances about how an AI system will comply with other legal obligations and policies.
6. Risk management is a key element of successful AI governance and regulation. The province must develop comprehensive and consistent criteria for assessing AI risks. Public entities must be required to evaluate their systems against these criteria and describe how an AI system’s risks will be mitigated and its performance will be monitored, evaluated, and reported.
7. The provincial government must develop comprehensive and consistent criteria for identifying Bill 194 exceptions and prohibitions. These criteria must be established in regulations. Public consultations on these criteria are crucial.
8. A new section should be added to Bill 194 to establish a transparent and accountable governance framework for public sector AI systems. This framework should include a provincial commissioner or officer responsible for public oversight of public sector AI systems.
9. A new section should be added to Bill 194 stating that the legislation and accompanying regulations will be publicly reviewed no later than two years after they are enacted.
10. Provincial entities should not procure, develop, or deploy high-risk AI systems prior to adoption of Bill 194 and accompanying regulations. Existing high-risk public-sector AI systems should not be grandfathered or exempt from Bill 194 or its regulations.
11. In the coming months, the provincial government should prioritize the development of the most important AI regulations and policies, such as the provincial risk assessment framework, prohibitions, an impact assessment tool, and governance structure. The provincial government should ensure there is meaningful public input and participation in the development of these regulations/policies.

## Recommendation #1: Trustworthy AI

Many governments have responded to the challenges of AI by announcing or adopting “trustworthy AI” legislation, frameworks, and policies. These initiatives are intended to assure the public and stakeholders that government AI development and use will be beneficial, lawful, and accountable.

The Government of Canada’s Directive on Automated Decision-making (“the Canada ADM Directive”) is the most notable Canadian “trustworthy AI” framework. Internationally, the most comprehensive and significant “trustworthy AI” frameworks are the European Union’s *Artificial Intelligence Act* and US *Executive Order on AI*.

The Government of Ontario has developed its own Trustworthy AI Framework. This framework includes “three strategic priorities”:

- 1. No AI in secret:** *This means that we will provide a clear understanding of how and when AI is used.*
- 2. AI use the people of Ontario can trust:** *This means that we must clearly define risks of AI use and work to prevent them to proactively protect the people of Ontario.*
- 3. AI that serves all the people of Ontario:** *This guarantees that the right processes will be in place to challenge decisions made with the use of AI.<sup>1</sup>*

The provincial government has supplemented its Trustworthy AI Framework with Principles for Ethical Use of AI [Beta] (the “Beta Principles”).<sup>2</sup> The Beta Principles include six points to “align the use of data enhanced technologies within government processes, programs and services with ethical considerations and values.” The Beta Principles state that provincial AI systems should be:

- Transparent and explainable
- Good and fair
- Safe
- Accountable and responsible
- Human centric
- Sensible and appropriate

Unfortunately, Bill 194 does not fully incorporate its own Trustworthy AI principles or important elements of the Beta Principles. For example, the Trustworthy AI Framework commits the province to:

*AI that serves all the people of Ontario: **This guarantees that the right processes will be in place to challenge decisions made with the use of AI.** [Emphasis added.]*

Similarly, the Beta Principles state that:

***When automation has been used to make or assist with decisions, a meaningful explanation should be made available.** The explanation should be meaningful to the person requesting it. It*

*should include relevant information about what the decision was, how the decision was made, and the consequences.*

*Data enhanced technologies should be designed and operated in a way throughout their life cycle that respects the rule of law, **human rights, civil liberties, and democratic values.** These include dignity, autonomy, privacy, data protection, **non-discrimination, equality, and fairness.***  
[Emphasis added.]

As drafted, however, Bill 194 does not include provisions addressing human rights, civil liberties, non-discrimination, equality, or fairness. Nor does Bill 194 include provisions requiring explanations or guaranteeing a process to challenge decisions.

Simply stated, the problem is that the AI sections of Bill 194 are too brief (three sections, 1 ½ pages) and lack provisions that would ensure public sector AI use is beneficial, lawful, and accountable. More specifically, the Bill does not address the following widely acknowledged trustworthy AI priorities:

- Human rights and procedural fairness.
- AI systems in the criminal justice system.
- AI systems used in courts and tribunals.
- Public AI registries.
- Impact assessments.
- Risk categories and mitigation strategies.
- Explainability requirements.
- Governance requirements.

These are significant gaps. For example, Bill 194 states that it is important to protect privacy but is silent on the need to protect human rights. Nor does Bill 194 address AI systems used by police or in the criminal justice system, which are widely acknowledged to be the highest risk public sector AI systems.

It is not sufficient to state these issues will – or might be – be addressed in regulations. Nor is sufficient to state that these issues are addressed elsewhere. LCO reports demonstrate many gaps in existing case law and legislation.<sup>3</sup> Absent legislative guidance, there is no assurance that regulations will address these subjects. As a result, Bill 194 regulations may have important gaps or be insufficient to meet the needs of Ontarians. Equally important, Bill 194 may mean that Ontarians cannot review or participate in significant AI policymaking, as most important decisions are left to regulations.

Bill 194 should enshrine Trustworthy AI principles in the body of the legislation. Comprehensive legislation is necessary to provide the foundational governance framework for these systems. Comprehensive legislation would provide consistent direction and accountability requirements to the actors, departments, and agencies within its scope. It would also ensure important AI policymaking is subject to legislative and public review. Finally, comprehensive legislation would establish a level of public and legal accountability commensurate with the issues and rights at stake.

**Recommendation #1: Trustworthy AI principles should be enshrined in Bill 194.**

## Recommendation #2: Legislative Objectives

The legislative objectives of Bill 194 are currently restricted to “protecting privacy.”<sup>4</sup> Public entities in Ontario also have a legal duty to comply with *Ontario Human Rights Code*, *Charter of Rights and Freedoms*, and administrative law requirements.<sup>5</sup> As a result, protecting human rights and procedural fairness should also be explicitly included in the Act.

### Human Rights

Human rights have been a transcendent issue in AI design, development, operation, and oversight across the world for many years.<sup>6</sup>

AI systems can be biased or discriminatory against individuals on the grounds of race, age, disability, sex, family structure or other grounds protected in the *Ontario Human Rights Code* and *Charter of Rights and Freedoms*. Bias in an AI system can also intersect across multiple grounds at once. Equally troubling, bias is often embedded, unexpected, undetected, and coupled with the perception that machines are objective.

The most common human rights criticism of AI is the potential use of biased data. In these circumstances, because the training data or “inputs” used by an AI or algorithm (such as arrest, conviction, child welfare, education, employment or “fraud” data) may themselves be the result of biased practices, the results or outputs of an AI or algorithmic system may also be biased.

The “bias in, bias out” issue is the best-known AI bias issue, but not the only one. Discrimination and bias issues can also arise in questions regarding statistical “metrics of fairness”, AI or algorithmic scoring, and automation bias, to name a few. The effect of technology on bias can be subtle but significant. For example, AI may increase barriers for people with disabilities if systems are built without considering accessibility, or if they misinterpret a disability as cheating, an anomaly, or a red flag.

The Government of Ontario addressed the issue of AI bias in its 2019 discussion paper, *Promoting Trust and Confidence in Ontario’s Data Economy*, which noted bias and discrimination as a threat or risk associated with “data-driven practices” and which linked bias with “black box” concerns.<sup>7</sup> Human rights, civil liberties, non-discrimination, and equality are also explicitly acknowledged in the Beta Principles.<sup>8</sup>

Bill 194 does not acknowledge the province’s human rights obligations or the province’s earlier commitments. This is a significant gap. Bill 194 should be amended accordingly.

### Administrative Law and Procedural Fairness

Government decisions range from minor, inconsequential decisions to major decisions affecting significant personal rights and interests.<sup>9</sup> The Supreme Court of Canada has stated that administrative decision-making is “one of the principal manifestations of state power in the lives of Canadians.”<sup>10</sup>

Administrative law is the area of law that holds governments accountable for these decisions. The provincial government and its agencies and departments have a legal duty to be fair, transparent and accountable to Ontarians. The province’s duty to comply with administrative law requirements are acknowledged repeatedly in both the Trustworthy AI Framework and the Beta Principles (“...guarantees



that the right processes will be in place to challenge decisions”, “...a meaningful explanation should be made available”, “...designed and operated in a way that respects the rule of law...[and] fairness.”).<sup>11</sup>

A decision by government that affects the rights, privileges or interests of an individual triggers a duty of fairness. This duty has been held to translate into an entitlement to fair procedure, which is founded on open decision-making and transparency. Fair procedure is achieved through:

- Notice of the case one needs to meet.
- Participation in the form of an oral hearing and/or written submissions.
- A decision by an open-minded decisionmaker considering relevant factors.
- An explanation or reasons for the decision.

One of the most common and important strategies for addressing concerns about AI accountability, transparency and fairness is to frontload AI systems with procedural fairness safeguards. Fortunately, the Government of Canada has taken important first steps in this regard. The federal Automated Decision-making Directive (“Canada ADM Directive”)<sup>12</sup> and its companion Algorithmic Impact Assessment (“federal AIA”)<sup>13</sup> are leading examples of tools and strategies that incorporate procedural fairness protections into the design and operation of AI and automated government decision-making.

Administrative law and procedural fairness requirements are no less important or obligatory at the provincial level. As a result, Bill 194 should acknowledge these legal obligations and be amended to explicitly identify protecting procedural fairness as a legislative objective.

## **Recommendation #2**

**Bill 194’s Preamble should be amended to read:**

**The Government of Ontario...Believes that artificial intelligence systems in the public sector should be used in a responsible, transparent, accountable and secure manner that benefits the people of Ontario while protecting privacy, *human rights, and procedural fairness.***

## **Recommendation #3:      Applicability and Uses**

As drafted, Bill 194 excludes many of the most significant public sector AI risks from legislative oversight, including AI systems used in the criminal justice system (including policing) and by courts and tribunals.

Bill 194 s. 5(1) states that its provisions respecting AI systems “applies to such public sector entities as may be prescribed if they use or intend to use an artificial intelligence system in prescribed circumstances.” This section includes two important Bill 194 limitations:

First, s. 1(1) identifies which “public sector entities” will be subject to Bill 194. “Public sector entity” is defined as

(a) *an institution within the meaning of **subsection 2 (1) of the Freedom of Information and Protection of Privacy Act,***

(b) *an institution within the meaning of **subsection 2 (1) of the Municipal Freedom of Information and Protection of Privacy Act,***

(c) *a children’s aid society,*

(d) *a school board; (“entité du secteur public”).*

[Emphasis added.]

Second, s. 5(1) allows the province to prescribe AI “uses” or “circumstances” that are subject to Bill 194. Neither “use” nor “circumstances” is defined in the Act.

Notably, neither s. 2(1) of *Freedom of Information and Protection of Privacy Act* nor s. 2(1) of the *Municipal Freedom of Information and Protection of Privacy Act* include police services, courts, or tribunals. As a result, these institutions are not subject to Bill 194 governance or requirements.

The omission of AI systems used in criminal justice or courts and tribunals is a significant gap in public sector AI regulation in Ontario. AI systems such as predictive policing, biometric surveillance systems, and bail and sentencing risk assessment algorithms have demonstrably high risks to *Charter* rights, human rights, privacy, and procedural fairness.<sup>14</sup>

The risks of AI systems used in the criminal justice system, courts, and tribunals was discussed at length in the LCO’s *Accountable AI* and *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada* reports. Those reports and many others also document how the risks of these systems fall disproportionately on low-income, racialized, or otherwise vulnerable communities and individuals.<sup>15</sup>

In the United States, there has been an extraordinary backlash to the use of AI and related tools in American criminal justice and courts. Importantly, American AI tools in these contexts were introduced *before* comprehensive legislation. The American experience can teach Canadian policymakers many lessons.

The Canada ADM Directive does not include AI or automated decision-making systems in the criminal justice system. In contrast, the EU *AI Act* includes detailed provisions identifying AI tools in “law enforcement” and the “administration of justice” as being presumptively high-risk and thus subject to more detailed regulatory requirements.<sup>16</sup>

The LCO strongly recommends Bill 194 be amended to include AI systems used in the criminal justice systems (including police services), courts, and tribunals.

Absent this amendment, police services and courts in Ontario could adopt predictive policing, facial recognition surveillance, automated bail and sentencing risk assessments, and a myriad of other technologies without having to comply with the Bill 194’s accountability requirements.

**Recommendation #3: The definition of “public entity” in Bill 194 should be amended to include:**

- **Police service boards, the Ontario Provincial Police, municipal police services, and any other police service in Ontario, and,**
- **Courts, tribunals, and adjudicative agencies.**

## Recommendation 4: “No AI in Secret”

One of the three strategic priorities of in the provincial government’s Trustworthy AI Framework is:

*1. No AI in secret: This means that we will provide a clear understanding of how and when AI is used.*

Disclosure and transparency are key principles of trustworthy AI.<sup>17</sup>

### AI Registries

One of the most effective (and common) strategies for promoting disclosure and transparency is an AI registry.<sup>18</sup> These are websites that identify and document AI and ADM systems used by governments. The purpose of an AI registry is to centralize disclosure of AI and ADM systems, promote public and legal accountability, and to be a resource for developers, stakeholders, researchers, and the public.

The provincial government has itself explained why it is important to publicly disclose algorithms and AI systems:

*Transparency of use allows all of us to be aware of when, how and why decisions are automated, so we can all discuss the merits or appropriateness of use, availability of recourse options and necessary improvements to these tools, systems or algorithms to ensure they are benefiting everyone without causing harm.*

*Public notice is key to people’s ability to inform, question and hold accountable the unseen AI used to make government services simpler, faster, better. Starting with transparent use we are working towards a governance framework for AI in Ontario that is responsive, adaptive and fair.<sup>19</sup>*

The provincial government also has its own AI registry, the data catalogue for “algorithms, tools and systems powered by data across the Ontario Public Service.”<sup>20</sup>

In 2021, the LCO complemented the province’s data catalogue, but cautioned that it would be more effective if it were mandatory:

*The Government of Ontario’s data catalogue is a good start and demonstrates a significant commitment to algorithmic transparency. In the LCO’s view, this initiative would be significantly*

*improved if the disclosure requirement were a mandatory obligation across the provincial government.*<sup>21</sup>

Three years later, this recommendation has proven to be prophetic: In March 2021, the Ontario's data catalogue included eight "tools," including the COVID Self-Assessment Tool, the COVID-19 Courthouse Screening Tool and several tools used by the Ministry of Agriculture, Food and Rural Affairs. In June 2024, these are still the only AI or algorithmic systems listed on the data catalogue.<sup>22</sup> This situation underscores the need to create a mandatory legal obligation to add AI "tools" to the public registry.

### **Disclosure Requirements**

Simply adding "tools" to Ontario's data catalogue will not ensure "no AI in secret." It is also important to specify what will be disclosed, when it will be disclosed, and to whom.

Bill 194 includes several provisions (including s. 5(2), s. 6(2)(a), s. 7(c) and s. 7(i)) giving the province the authority to prescribe what information must be disclosed about a public sector AI system. As with many other provisions in the Act, however, the principles or requirements guiding the province's regulation-making powers are missing.

To fill this gap, the LCO recommends the province follow the disclosure example set in the Canada ADM Directive and federal AIA. The Canada ADM Directive includes a mandatory disclosure requirement. It also requires notice on websites when decisions will be made by or with the assistance of AI or an ADM system, regardless of the applicable impact level.<sup>23</sup> Those notices must be in plain language and prominently displayed.<sup>24</sup> Agencies are similarly required to provide meaningful explanations of their ADM -informed decisions to affected individuals.<sup>25</sup> In addition, systems with Impact Levels of III or IV, agencies must

*...publish documentation on relevant websites about how the [systems] works, in plain language, describing:*

- *How the components work.*
- *How it supports the administrative decision.*
- *Results of any reviews or audits; and*
- *A description of the training data, or a link to the anonymized training data if this data is publicly available.*<sup>26</sup>

The LCO believes these are appropriate specifications, and recommend they be incorporated into Bill 194. Later in this submission, the LCO recommends additional disclosure requirements, such as mandatory disclosure of AI impact assessments, performance.

### **Notice to Individuals**

Finally, the LCO reiterates that Bill 194 disclosure obligations should include a right for individuals subject to decision making by a public entity to notice about the use of an AI system; notice of their right to contest it; and possibly a right to opt-out in favor of human decision making. This commitment is necessary to ensure "No AI in secret" to the individuals directly affected by them.

**Recommendation #4:** The provincial government should develop comprehensive and consistent public information and disclosure requirements for public sector AI systems. These requirements should be consistent with the disclosure requirements set out in the Canada ADM Directive and other recommendations in this submission.

These requirements should include a mandatory AI registry and a requirement to disclose key elements of public sector AI systems.

Accordingly, Bill 194 section 5(2) should be amended to read:

*A public sector entity to which this section applies shall, in accordance with the regulations, provide information to the public about their use of the artificial intelligence system. This information shall be posted on an online registry of AI systems that is accessible to the public. Information to be included on the public registry shall include but not be limited to:*

- *A summary of key elements of the AI system.*
- *An impact assessment.*

Also, a new section should be added to Bill 194 specifying that individuals subject to decision making by an AI system be given notice about the use of an AI system; notice of their right to contest it; and, in appropriate circumstances, a right to opt-out in favor of human decision making.

## Recommendation #5      Accountability Frameworks

Accountability is the foundation of Trustworthy AI.

There are countless examples of Trustworthy AI regimes setting out detailed legal rules or policies specifying what AI developers/operators are accountable for and who they are accountable to.<sup>27</sup>

In contrast, Bill 194 contains almost no detail or guidance on the substance, timing, form, or locus of accountability for public sector AI systems. Bill 194 section 5(3) simply reads

*A public sector entity to which this section applies shall, in accordance with the regulations, develop and implement an accountability framework respecting their use of the artificial intelligence system.*

Bill 194 does not appear to anticipate robust accountability obligations. Regulatory provisions give the province the authority to prescribe the “form and content” and “documentation” to be included as part of an accountability framework, but no substantive requirements or principles are identified. Nor is it clear if or how s. 5(3) accountability frameworks will be different than Bill 194 requirements respecting disclosure (s. 5(2)), risk management (s. 5(4)), or prohibitions and restricted uses (s. 5 (4), (5), and (6)).

In the LCO view, Bill 194’s lack of detail regarding the objectives, principles or elements of AI system accountability are troubling. At the very least, the lack of clear requirements appears to contradict the province’s Trustworthy AI policy, the Beta Principles, and well-established practices in AI regulation. More significantly, the failure to identify basic components of an accountability framework could seriously compromise public sector AI systems in Ontario and place many Ontarians at risk.

The LCO has written extensively about the components of “accountable AI” in public sector AI systems in our earlier reports. We also discuss how disclosure, risk management, prohibitions, governance, and consultations are related to AI system accountability elsewhere in this submission.

We will not repeat those discussions in this section, but rather focus on two crucial elements of AI accountability that should be explicitly addressed in Bill 194: purpose definition of AI systems and AI impact assessments.

### **Purpose Definition and Limitation**

The concept of "statutory purpose limitation" for AI is intended to ensure that AI systems are used only for specific, legally defined purposes. This principle is included in many data protection and privacy regulations, such as European Union's General Data Protection Regulation (GDPR).<sup>28</sup>

Statutory purpose limitations have two distinct but related objectives: 1) To promote public accountability and transparency about an AI system, and 2) to mitigate the risk of AI system “drift.”

### **Impact Assessments**

Algorithmic impact assessments (AIAs) and human rights impact assessments (HRIAs) have become a leading tool to identify and mitigate AI risks. The growth in the use and development of AIAs and HRIAs is a proactive response to the many documented risks of private and public AI to equality, fairness, privacy, transparency, and data security.<sup>29</sup>

AIAs and HRIAs are structured questionnaires that guide developers, operators, and institutions through a comprehensive checklist of issues and questions to assess an AI system against specified and transparent criteria. Many AIAs and HRIAs also identify risk mitigation strategies as well. AIAs and HRIAs are not designed or intended to be punitive. Rather, their objective is to help IT professionals and

organizations build better AI systems by minimizing foreseeable risks/harms and providing a level of due diligence compliance with important external obligations.

AIAs and HRIAs are gaining momentum as an AI governance strategy across the world. They are increasingly being required by legislation or adopted by governments, public institutions, and private enterprises to demonstrate and implement their commitments to “trustworthy AI.”

The development and use of these tools has been recommended by many governments, including the federal government<sup>30</sup>, the European Commission<sup>31</sup>, and the United States federal government.<sup>32</sup> Closer to Ontario, AIAs have been supported by the Vector Institute in a recent report stating that:

*Effective algorithmic impact assessments should be carried out regularly and cover AI-specific aspects such as bias, privacy, explainability, data and model drift. Assessing bias and fairness was understood to require attention to the context and the careful selection of an appropriate metric.*<sup>33</sup>

The leading AI impact assessment tool in Canada to date is the federal government’s 2019 *Algorithmic Impact Assessment* (AIA) for use by most departments and agencies in the federal government. The AIA was discussed extensively in the LCO’s *Accountable AI* report and our earlier *Regulating AI: Critical Issues and Choices* report. The federal Treasury Board Secretariat recently released an updated Federal Directive.

Sophisticated examples of AI impact assessment tools from other jurisdictions include the European Commission’s *Assessment List for Trustworthy AI*<sup>34</sup>; the Netherlands’ *Fundamental Rights and Algorithms Impact Assessment*<sup>35</sup>; the *AI Impact Assessment* developed by ECP, a Dutch civil society organization<sup>36</sup>; AI Now’s *Algorithmic Impact Assessment*; Microsoft’s *Responsible AI Standard and Impact Assessment* (2022)<sup>37</sup>; the Spanish Data Protection Agency’s *Guide to Algorithmic Auditing* developed by a research team at Etcas Research and Consulting<sup>38</sup>; Algorithm Watch’s *Impact Assessment Tool for Public Authorities*<sup>39</sup>; and the University of Oxford *capAI* tool, which helps organizations assess AI systems for conformity with the EU *Artificial Intelligence Act*.<sup>40</sup>

As noted earlier, the LCO is developing its own human rights impact assessment in collaboration with the Ontario and Canada Human Rights Commissions. The LCO expects to release this tool later in 2024.

Suffice to say, AIAs and HRIAs are an important and positive development to ensure trustworthy AI. Their success as a trustworthy AI tool is contingent upon several factors:

- They must assess an AI system against specific and consistent criteria. In the case of public sector AI systems in Ontario, this would include, but not be limited to, an assessment against privacy, human rights, and procedural fairness obligations.
- They must be developed inclusively by a broad team, including developers, legal professionals, compliance experts, program managers, and members of the community likely to be affected by the AI system being assessed.
- They must be mandatory. Voluntary AIAs or HRIAs are unlikely to be consistently used, diminishing their utility to improve AI systems and ensure public accountability.

- They must be disclosed in some fashion. This is to guard against the possibility that entities understate (through intention or inadvertence) the impact an AI system, and thus avoid the appropriate level of regulation and governance.
- They must be updated regularly. AI systems are dynamic and subject to “drift.” As a result, an impact assessment must be updated at regular intervals to ensure it is still accurate.

AIAs and HRIAs are not a panacea, and they must be used as part of an overall AI governance strategy including legislation, regulations, and policy guidance. The strengths, weaknesses, and complexities of AIAs and HRIAs will be discussed in a forthcoming LCO issue paper.

**Recommendation #5: The provincial government should develop comprehensive and consistent accountability frameworks for public sector AI systems.**

**These frameworks should include purpose limitations and a provincially mandated impact assessment that addresses privacy, human rights, and procedural fairness issues. The framework should also require assurances about how an AI system will comply with other important Trustworthy AI obligations and policies.**

**Accordingly, Bill 194 section 5(3) should be amended to read:**

***A public sector entity to which this section applies shall, in accordance with the regulations, develop and implement an accountability framework respecting their use of the artificial intelligence system.***

***The accountability framework shall include but not be limited to:***

- ***A description of the purpose of the AI system, including how the system will be used to fulfill a statutory objective.***
- ***An impact assessment, including identification of risks and mitigation strategies.***
- ***A description of how the AI system complies with applicable privacy, human rights, and procedural fairness requirements.***
- ***An assurance regarding compliance with other relevant legal obligations and applicable standards.***
- ***A description of how the performance of the AI system will be monitored, evaluated, and reported.***



## Recommendation #6

## Risk Management

Section 5(4) of Bill 194 states that: “A public sector entity to which this section applies shall take such steps as may be prescribed to manage risks associated with the use of artificial intelligence systems.” Section 7(e) gives the province the authority to “[prescribe] steps to be taken for the purposes of subsection 5(4), including reporting and record-keeping.”

Bill 194 does not identify the risks, principles, categories, or criteria that must be used to assess AI system risk. Nor does the Act specify how risks are to be reported, what mitigation strategies are required (if any), or whether an AI system’s performance must be monitored, evaluated, or reported.

Bill 194’s lack of detail in this area is contrary to recent trends in trustworthy AI legislation and regulation.<sup>41</sup> More importantly, these omissions heighten the foreseeable risks and harms of public sector AI systems in Ontario and reduce public trust and accountability.

Risk-based AI regulation is explicit in the EU *AI Act*<sup>42</sup>; *AIDA*<sup>43</sup>; the Canada ADM Directive<sup>44</sup>; American federal AI regulations<sup>45</sup> and the U.S. *AI Bill of Rights*<sup>46</sup>; and many other AI governance regimes.

Risk-based AI governance models assume that different AI systems will have different level of risk and that regulatory obligations should be tailored proportionately. Risks in these circumstances are evaluated through AI impact assessments, as was described in the previous section.

The risks addressed in these models typically include privacy risk, data security risk, bias risk, and, increasingly, other forms of human rights risk. A risk-based approach allows for the most optimal balance between encouraging innovation and safeguarding community and individual rights. It means that the most onerous regulatory obligations attach only to the AI systems causing the most concern.

Not all risk-based models are the same: *AIDA* includes two levels of risk: high and low.<sup>47</sup> The Canada ADM Directive has four levels based on the system’s impact after an assessment using the federal AIA.<sup>48</sup> The EU also has four levels of risk: unacceptable risk (i.e. prohibited systems), high risk, limited/transparency risk, and minimum risk.<sup>49</sup>

### **Risk Criteria and Categories**

In principle, the LCO agrees with risk-based regulation. Risk-based regulation is both a practical response to the wide variety of AI systems and responsive to the principles and requirements of various areas of law. This view is subject to the following qualifications and comments:

First, it is crucial that risk assessment categories and criteria be consistent and transparent. Bill 194’s regulatory protections will be seriously undermined if entities are allowed to determine their own risk assessment categories and criteria. There will likely be circumstances in which entities in specific sectors need to tailor or customize their risk assessments. This kind of “fine-tuning” should be encouraged so long as it is consistent with provincially mandated risk categories and criteria.

Second governments and public entities should be publicly accountable for their decisions about the potential impact or risk of an AI system. As a result, it is crucial that risk assessment determinations be

transparent. This is to guard against the possibility that entities understate (through intention or inadvertence) the level of risk of an AI system, and thus avoid the appropriate level of regulation and governance.

Third, the LCO rejects simple or binary high/low risk classifications. The risk assessment levels in the federal Directive and the accompanying AIA appears sound. Experience will determine the federal Directive's four risks levels and the AIA represent an appropriate range or hierarchy of risk. Over time, the levels and AIA may be adjusted. The LCO emphasizes, however, that entities must be publicly accountable for any adjustments to the levels or risk assessment criteria.

Fourth, it is important that risk assessments and mitigation strategies be updated regularly. AI systems can "drift" and their performance needs to be monitored and reported at regular intervals.

Fifth, assessing the level of "risk" of any AI system is not the same as determining whether the AI violates human rights. A risk-based approach suggests that AI operators are to find a balance between operational risks/efficiency and individual rights. However, human rights are immutable and, with rare exception, paramount to other interests. That is, human rights are not to be balanced with other interests such as corporate efficiency, rather they take priority over other interests. Further, there will invariably be AI systems that are not captured by categories described as "high risk."

Finally, the LCO strongly supports the establish baseline requirements for all AI systems, irrespective of the level of risk. For example, the baseline requirements set out in Canada ADM Directive include a broad range of technical principles ("validating the quality of data collected and used"), best practices ("consultations with government legal services..."), and quasi-legal requirements ("recourse options that are available to challenge the administrative decision.").<sup>50</sup>

## **Mitigation**

Simply identifying AI risks is not enough. As a result, most of the AI impact assessment tools described in the previous section includes mandatory or suggested techniques and policies to minimize AI risks. As with risk assessment, the determination what mitigation measures should apply to a given AI system should be assessed on a sliding scale based on results of an impact assessment.

The province should look to the federal AIA and the LCO's forthcoming Human Rights Impact Assessment for guidance on how to create a "sliding scale" of mitigation measures in the context of procedural fairness and discrimination.

Mitigation measures included in other trustworthy AI models include:

- Third party independent audits of data validity, reliability and relevancy; design/source code; and unintended outcomes.
- Explainability requirements.
- Metrics testing.
- De-biasing techniques.
- Consultations.

## Public Engagement

Risk categories and criteria are complex, controversial, and consequential. As a result, the LCO recommends broad consultations to develop the provincial risk assessment framework. The LCO addresses this and other high priority consultation issues in Recommendation 11 below.

**Recommendation #6**      **The provincial government should develop comprehensive and consistent risk management and mitigation requirements for public sector AI systems. Among other criteria, public sector AI systems need to be evaluated for their risks to privacy, human rights, and procedural fairness.**

**Provincial risk management requirements should include provincially mandated risk categories, risk criteria, mitigation strategies, and evaluation/reporting obligations.**

**Risk assessments by public entities should be posted on the provincial AI registry and updated regularly.**

**Accordingly, Bill 194 section 5(3) should be amended to read:**

***This risk management strategy shall include but not be limited to:***

- An impact assessment evaluating the AI system against provincial risk categories and criteria.***
- A description of how the AI system's risks will be mitigated.***
- A description of how the performance of the AI system will be monitored, evaluated, and reported.***
- A requirement that Impact assessments be posted on the provincial AI registry and updated regularly.***

## Recommendation #7:      Prohibitions and Restricted Uses

AI system prohibitions, use case restrictions, and preemptive risk identification is probably the most controversial and consequential topic of AI legislation and regulation.

Governments must consider whether there are certain AI technologies or uses that should be prohibited outright. For example, new methods of mass profiling and surveillance – including facial recognition, biometric identification, predictive policing, social network behavioral analysis, and “smart cities” – have been cited as “red line” AI technologies that should be prohibited in whole or in part.<sup>51</sup>

Section 5 (40, (5) and (6) of Bill 194 gives the province the authority to prohibit or restrict the use public entity AI systems by regulation. The Act does not, however, identify the risks, principles, or criteria that will guide this important authority. Nor does the Act identify circumstances or AI uses in which systems will be preemptively prohibited or categorized as a high-risk system requiring more extensive accountability/mitigation measures. Nor has the province committed to publicly consult on these issues.

Bill 194's lack of detail or guidance on prohibitions and restricted uses is worrisome. Bill 194's lack of detail in this area is contrary to recent trends in trustworthy AI legislation and regulation. More importantly, these omissions heighten the foreseeable risks and harms of public sector AI systems in Ontario and reduce public trust and accountability.

Many governments have enacted or proposed bans on certain technologies or their use in specific circumstances. Most notably, the EU *AI Act* creates a category of "unacceptable risk" in which AI systems are prohibited, including:

- Subliminal or Manipulative techniques: Using subliminal or manipulative techniques to distort decision-making leading to significant harm.
- Vulnerability Exploitation: Exploiting vulnerabilities due to age, disability, or social or economic situations, causing significant harm.
- Biometric Categorisation: Inferring sensitive personal attributes such as race, political, religious or philosophical belief, trade union membership, through biometric systems, except for lawful law enforcement purposes.
- Social Scoring: Evaluating or classifying individuals based on social behaviour or personal characteristics, leading to unfair or disproportionate treatment.
- Real-time Biometric Identification: 'Real-time' remote biometric identification in public spaces for law enforcement, with specific necessary exceptions.
- Predictive Policing: Assessing the risk of criminal offences based solely on profiling or personality traits, except to support human assessments based on verifiable facts.
- Database Creation through scraping: Creating or expanding facial recognition databases through untargeted scraping from the internet or CCTV footage.
- Emotion Inference: Inferring emotions in workplaces or educational institutions, except for medical or safety reasons.<sup>52</sup>

The EU also preemptively identifies AI systems as high risk if it deployed in one of these areas:

- Biometrics systems.
- Critical infrastructure management.
- Education and vocational training.
- Employment.
- Workers management and access to self-employment.
- Access to and enjoyment of essential services.
- Law enforcement.
- Migration.
- Asylum and border control management.

- Administration of justice and democratic processes.<sup>53</sup>

Facial recognition and other biometric technologies have probably been subject to the most (and most variable and complex) bans and restrictions. In the United States, for example, it appears more than 20 jurisdictions have enacted various types of bans and limitations on use of facial recognition technology, especially in law enforcement.<sup>54</sup>

In our view, it would be preferable to include a list of prohibited or preemptively identified high risk systems or uses in Bill 194 directly. This would establish a high legal accountability threshold and promote public debate on these important issues.

At this point, the LCO is not prepared to recommend definitive prohibitions and restricted uses. The LCO has learned through many consultations that broad, participatory public engagement on these issues is crucial. The experience regulating facial recognition systems in US policing demonstrates the complexity and need for nuance in these areas.

Based on our extensive experience in this field, however, the LCO can recommend that the following systems or uses be strongly considered for prohibition:

- Facial recognition and biometric identification systems used for surveillance purposes.
- Scrapping of facial images for the building or expansion of facial recognition databases.
- Predictive policing systems.
- AI systems that include misleading information, misinformation, or dis-information
- AI systems that exploit vulnerabilities of people or communities.
- Emotion recognition technologies.
- Social scoring or social classification
- Behavioral tracking in certain contexts; and
- Social network behavioral analysis systems.

In addition, the LCO recommends the following systems or uses be strongly considered for preemptive designation as “high-risk” and thus subject to higher regulatory requirements:

- Social services, including benefits determination.
- Housing.
- Education.
- Health care.
- Child protection.
- Systems used in criminal justice, court or tribunal proceedings.
- Administrative decisions
- Employment including employee opportunity and management,
- Tax.
- A government decision that impacts an individual.

AI and related systems in all these areas have significant potential to affect the legal rights (including but not limited to human rights) of Ontarians. Many of these systems also have well-documented risks for relying on inaccurate, unreliable or racialized data; for being opaque; or for targeting poor, racialized or

vulnerable communities.<sup>55</sup> As a result, there are good reasons for these systems to be subject to prohibitions or higher regulatory standards.

**Recommendations #7:**      **The LCO recommends the provincial government engage in public consultations with legal professionals, technological developers, NGOs, community groups, and representatives from public entities, the police, social services, the justice system, and others to identify criteria, context and uses of public sector AI systems that should be prohibited, preemptively identified as high-risk, or otherwise subject to higher regulatory standards.**

## Recommendation #8      Governance

### Independent Oversight

Many Trustworthy AI proposals and AI legislative regimes include provisions creating independent oversight of public sector AI systems, designating officials responsible for overseeing AI systems within their organizations, and/or procedures to enforce AI regulatory requirements.

Bill 194 does not include any provision guaranteeing independent oversight. Nor does Bill 194 specify what mechanisms or remedies will exist to enforce Bill 194, notwithstanding the Trustworthy AI Frameworks' commitment to "guarantee that the right processes will be in place to challenge decisions."<sup>56</sup>

Bill 194's only governance provision (s. 6(2)(b)) specifies that a prescribed public sector entity "shall ensure that... an individual exercises oversight of the use of the artificial intelligence system in accordance with the regulations." This provision is a welcome, but rare, mandatory legislative requirement. This provision alone, however, will not ensure effective governance in public sector AI systems.

AI governance frameworks emerging around the world establish an independent oversight body or coordination office to oversee systemic AI development, deployment and evaluation. The rationale for this approach has been summarized by the New Zealand Law Foundation as follows:

*...[w]hile important, ..., regulatory models that rely on affected individuals enforcing legal rights are unlikely to be adequate in addressing the concerns around increasing use of algorithms. One, affected individuals will lack the knowledge or the means effectively to hold these tools and processes to account. They are also likely to lack the 'wide-angle' perspective necessary to evaluate their effective populations.<sup>57</sup>*

The New Zealand Law Foundation’s report, *Government Use of Artificial Intelligence in New Zealand*, includes a very comprehensive review of various oversight models, including regulatory agencies and self-regulatory models.<sup>58</sup>

In Europe, the European Commission established a new body to oversee the implementation of the EU *AI Act* and to work with member countries to help it carry out its duties. The European Commission will also establish an AI board, an advisory forum, and a Scientific Panel of independent experts.<sup>59</sup>

Under the EU *AI Act*, enforcement and sanctions depend on the type of AI and the scope the AI regulations fall into.<sup>60</sup> The Commission has the exclusive authority to oversee and enforce rules related to general-purpose AI models and their providers (article 88).<sup>61</sup>

In the U.S., there are many coordinated or independent AI oversight models. For example, an Executive Order adopted by the City of New York Office of the Mayor establishes an “Algorithms Management and Policy Officer” who will be responsible for matters

*...relating to the fair and responsible use of algorithmic tools and other emerging technologies in city agency decision-making, coordinate efforts to create and strengthen related best practices citywide, and support agencies in implementing such practices.*<sup>62</sup>

In Canada, the federal Directive states that the Assistant Deputy Minister responsible for a program using an ADM system is responsible for:

*6.4.1 Providing clients with any applicable recourse options that are available to them to challenge the administrative decision.*<sup>63</sup>

Finally, *AIDA* includes provisions creating an AI and Data Commissioner who is largely responsible for enforcing the Act.<sup>64</sup> It should be noted that many have voiced concerns about the Data Commissioner’s a lack of independence.

The LCO is concerned about Bill 194’s failure to create an Ontario equivalent of the offices cited above. We agree that an individual should be designated within prescribed organizations to be responsible for that organization’s compliance with Bill 194’s legislative requirements, regulations, policies, and standards. The effectiveness, accountability, and public trust in provincial AI systems will be significantly enhanced, however, with the addition of some kind of provincial AI officer who is responsible for systemic oversight, policy guidance, and potentially, investigations.

The LCO supports the principle of independent oversight of public sector AI systems. The LCO is less certain about the institutional design or placement of these functions. The provincial government will have to give considerable thought to the best way to achieve independent oversight, especially considering the complementary mandates of existing government agencies, such as the Office of Privacy Commissioner and the Ontario Human Rights Commission.

**Recommendation #8:** A new section should be added to Bill 194 to establish a transparent and accountable governance framework for public sector AI systems.

This framework should include a provincial commissioner or officer responsible for public oversight of public sector AI systems and designated officials within applicable organizations responsible for that organization’s compliance with applicable laws, regulations, policies, and standards.

## Recommendation #9: Mandatory Review

The LCO recommends that Bill 194 be amended to add a mandatory review no later than two years after the legislation and regulations are enacted. This requirement is an acknowledgement of the pace of technological change and the need to update the legislation and regulations with experience. More broadly, mandatory review is also an important good governance principle.

The Canada ADM Directive has had three such reviews. After the third review (completed in 2022), the federal Treasury Board expanded the scope of the Directive to internal government services in addition to external impacts. Several requirements were expanded also, including adding more questions to the AIA concerning the reasons for pursuing automation, additional explanation criteria, and a requirement to release of AIAs prior to the production of a system.<sup>65</sup>

**Recommendation #9** A new section should be added to Bill 194 stating that the legislation and accompanying regulations will be subject to a mandatory review no later than two years after they are enacted.

## Recommendation #10: No Grandfathering Existing AI Systems

It would severely compromise the purpose and credibility of Bill 194 and any provincial Trustworthy AI Framework if the province or provincial entity were to deploy high-risk AI system *prior* to the adoption of its comprehensive Bill 194 regulatory regime. Similarly, high-risk systems currently in operation or under development should not be “grandfathered” or exempt from the Bill 194 requirements. Risk is risk, irrespective of whether an AI system was developed/deployed before or after an arbitrary proclamation date.



**Recommendation #10**      **Neither the provincial government nor any provincial entity should procure, operate or deploy high-risk AI or automated decision-making technologies prior to adoption of Bill 194 and accompanying regulations.**

**High risk provincial AI systems that may have been developed, purchased, or deployed prior to the adoption of Bill 194 and accompanying regulations should not be grandfathered or exempt.**

## **Recommendation #11:      High Priorities and Meaningful Consultations**

It is a truism of Trustworthy AI that there must be broad participation in the design, development and deployment of AI systems.<sup>66</sup> This participation must include technologists, policymakers, legal professionals, academics, public sector managers, and, crucially, the communities who are likely to be most affected by AI systems. Broad consultations promote better AI systems, improve the public’s understanding and acceptance of complex technologies, and reduce the possibility AI systems will worsen existing biases and inequality.

In the coming months, the provincial government should prioritize the most important AI regulations and policies, including a provincial risk assessment framework, prohibitions, an impact assessment tool, and governance structures. The provincial government should ensure there is meaningful public consultations in the development of these regulations and policies.

**Recommendation #11**      **The provincial government should prioritize the development of high priority AI regulations or policies. The provincial government should also ensure there is meaningful public input and participation on the development of these regulations/policies. High priority regulations and policies should include:**

- **A provincial AI impact assessment tool.**
- **A provincial AI risk management framework (including risk categories and mitigation strategies).**
- **Identification of prohibited systems or systems whose purpose, category or use will be limited.**
- **A provincial AI governance strategy.**

## Contacts and More Information

The LCO would be pleased to answer any questions about this submission or provide relevant source materials.

The LCO can be contacted through:

- Nye Thomas, LCO Executive Director ([athomas@lco-cdo.org](mailto:athomas@lco-cdo.org)).
- Susie Lindsay, LCO Policy Counsel ([slindsay@lco-cdo.org](mailto:slindsay@lco-cdo.org)) and lead of the LCO's AI in the Civil Justice System project.
- Ryan Fritsch, LCO Policy Counsel ([rfritsch@lco-cdo.org](mailto:rfritsch@lco-cdo.org)) and lead of the LCO's AI in the Criminal Justice System project.

## Appendix A

### List of Recommendations

**Recommendation #1:** Trustworthy AI principles should be enshrined in Bill 194.

**Recommendation #2:** Bill 194's Preamble should be amended to read:

The Government of Ontario...Believes that artificial intelligence systems in the public sector should be used in a responsible, transparent, accountable and secure manner that benefits the people of Ontario while protecting privacy, *human rights, and procedural fairness*.

**Recommendation #3:** Bill 194's definition of "public entity" should be amended to include:

- Police service boards, the Ontario Provincial Police, municipal police services, and any other police service in Ontario, and,
- Courts, tribunals, and adjudicative agencies.

**Recommendation #4:** The provincial government should develop comprehensive and consistent public information and disclosure requirements for public sector AI systems. These requirements should be consistent with the disclosure requirements set out in the Canada ADM Directive and other recommendations in this submission.

These requirements should include a mandatory AI registry and a requirement to disclose key elements of public sector AI systems.

Accordingly, Bill 194 section 5(2) should be amended to read:

*A public sector entity to which this section applies shall, in accordance with the regulations, provide information to the public about their use of the artificial intelligence system. This information shall be posted on an online registry of AI systems that is accessible to the public. Information to be included on the public registry shall include but not be limited to:*

- *A summary of key elements of the AI system.*
- *An impact assessment.*

Also, a new section should be added to Bill 194 specifying that individuals subject to decision making by an AI system be given notice about the use of an AI system; notice of their right to contest it; and, in appropriate circumstances, a right to opt-out in favor of human decision making.

**Recommendation #5:**

The provincial government should develop comprehensive and consistent accountability frameworks for public sector AI systems.

These frameworks should include purpose limitations and a provincially mandated impact assessment that addresses privacy, human rights, and procedural fairness issues. The framework should also require assurances about how an AI system will comply with other important Trustworthy AI obligations and policies.

Accordingly, Bill 194 section 5(3) should be amended to read:

*A public sector entity to which this section applies shall, in accordance with the regulations, develop and implement an accountability framework respecting their use of the artificial intelligence system.*

*The accountability framework shall include but not be limited to:*

- *A description of the purpose of the AI system, including how the system will be used to fulfill a statutory objective.*
- *An impact assessment, including identification of risks and mitigation strategies.*
- *A description of how the AI system complies with applicable privacy, human rights, and procedural fairness requirements.*
- *An assurance regarding compliance with other relevant legal obligations and applicable standards.*
- *A description of how the performance of the AI system will be monitored, evaluated, and reported.*
- *An impact assessment, including identification of risks and*

**Recommendation #6**

The provincial government should develop comprehensive and consistent risk management and mitigation requirements for public sector AI systems. Among other criteria, public sector AI systems need to be evaluated for their risks to privacy, human rights, and procedural fairness.

Provincial risk management requirements should include provincially mandated risk categories, risk criteria, mitigation strategies, and evaluation/reporting obligations.

Risk assessments by public entities should be posted on the provincial AI registry and updated regularly.

Accordingly, Bill 194 section 5(3) should be amended to read:

*This risk management strategy shall include but not be limited to:*

- *An impact assessment evaluating the AI system against provincial risk categories and criteria.*
- *A description of how the AI system's risks will be mitigated.*
- *A description of how the performance of the AI system will be monitored, evaluated, and reported.*
- *A requirement that Impact assessments be posted on the provincial AI registry and updated regularly.*

**Recommendations #7:**

The LCO recommends the provincial government engage in public consultations with legal professionals, technological developers, NGOs, community groups, and representatives from public entities, the police, social services, the justice system, and others to identify criteria, context and uses of public sector AI systems that should be prohibited, preemptively identified as high-risk, or otherwise subject to higher regulatory standards.

**Recommendation #8:**

A new section should be added to Bill 194 to establish a transparent and accountable governance framework for public sector AI systems.

This framework should include a provincial commissioner or officer responsible for public oversight of public sector AI systems and designated officials within applicable organizations responsible for that organization's compliance with applicable laws, regulations, policies, and standards.

**Recommendation #9** A new section should be added to Bill 194 stating that the legislation and accompanying regulations will be subject to a mandatory review no later than two years after they are enacted.

**Recommendation #10** Neither the provincial government nor any provincial entity should procure, operate or deploy high-risk AI or automated decision-making technologies prior to adoption of Bill 194 and accompanying regulations.

High risk provincial AI systems that may have been developed, purchased, or deployed prior to the adoption of Bill 194 and accompanying regulations should not be grandfathered or exempt.

**Recommendation #11** The provincial government should prioritize the development of high priority AI regulations or policies. The provincial government should also ensure there is meaningful public input and participation on the development of these regulations/policies. High priority regulations and policies should include:

- A provincial AI impact assessment tool.
- A provincial AI risk management framework (including risk categories and mitigation strategies).
- Identification of prohibited systems or systems whose purpose, category or use will be limited.
- A provincial AI governance strategy.

---

<sup>1</sup> Ontario, “Trustworthy AI ‘Framework’”, online: <https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework> [Ontario Trustworthy AI].

<sup>2</sup> Ontario, “Principles for Ethical Use of AI [Beta]”, online: <https://www.ontario.ca/page/principles-ethical-use-ai-beta> [Beta Principles].

<sup>3</sup> See generally, Law Commission of Ontario. *Accountable AI*, (2022) [LCO Accountable AI]; Law Commission of Ontario, *Regulating AI: Critical Issues and Choices*, (2021) [LCO Regulating AI], online: <https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/regulating-ai-critical-issues-and-choices/>; Law Commission of Ontario, *The Rise and Fall of Algorithms in American Criminal Justice: Lessons for Canada*, (2020) [LCO Criminal AI Issue Paper], online: <https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf>.

<sup>4</sup> Ontario, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* [Bill 194], First Reading May 13, 2024, online: <https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194>, Preamble.

<sup>5</sup> See generally, LCO Accountable AI, LCO Regulating AI, and LCO Criminal AI Issue Paper.

<sup>6</sup> For an extensive discussion of AI and human rights in Ontario, see LCO Accountable AI at 40-56.

<sup>7</sup> Ontario, “Promoting Trust and Confidence in Ontario’s Data Economy” [Ontario Promoting Trust], online: <https://www.ontario.ca/document/consultation-ontarios-digital-and-data-strategy/discussion-paper-1-promoting-trust-and-confidence> at 6-7.

<sup>8</sup> Beta Principles.

- 
- <sup>9</sup> For an extensive discussion of AI and administrative law in Ontario, see LCO Accountable AI at 56-71.
- <sup>10</sup> *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 at para. 4.
- <sup>11</sup> Trustworthy AI Framework and Beta Principles.
- <sup>12</sup> Canada, *Directive on Automated Decision-Making*, (2019) [Canada ADM Directive], online: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.
- <sup>13</sup> Canada, *Algorithmic Impact Assessment*, (2019) [Federal AIA], online: <https://open.canada.ca/data/en/dataset/5423054a-093c-4239-85be-fa0b36ae0b2e>
- <sup>14</sup> See generally, LCO Criminal AI issue Paper.
- <sup>15</sup> See, for example, LCO Regulating AI at 38-45.
- <sup>16</sup> EU *Artificial Intelligence Act* [EU AI Act], *Annex III: High-Risk AI Systems* [EU AI Annex III], online: <https://artificialintelligenceact.eu/annex/3/>
- <sup>17</sup> See generally, LCO Regulating AI at 29-33.
- <sup>18</sup> *Ibid.*
- <sup>19</sup> Quoted in LCO Regulating AI at 30. The original quote is from the webpage for the Ontario Data Catalogue, Artificial Intelligence and Algorithm group. The LCO could not find this text on a recent search of the same webpage. (Website accessed June 5, 2024.)
- <sup>20</sup> Ontario, *Data Catalogue, Artificial Intelligence* [Ontario Data Catalogue], online: <https://data.ontario.ca/group/artificial-intelligence>
- <sup>21</sup> LCO Regulating AI at 32.
- <sup>22</sup> Ontario Data Catalogue, accessed June 10, 2024.
- <sup>23</sup> Canada ADM Directive, s. 6.2.1.
- <sup>24</sup> *Ibid.*, s. 6.2.2.
- <sup>25</sup> *Ibid.*
- <sup>26</sup> *Ibid.*, Appendix C – Notice.
- <sup>27</sup> See generally the examples cited in this submission and related LCO reports. Notable examples include the EU AI Act; the Canada ADM Directive; and the White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* [US Executive Order] (2023), online: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>. See also the survey of AI regulation in the United States at Electronic Privacy Information Center, *The State of State AI Laws: 2023* (2023), online: <https://epic.org/the-state-of-state-ai-laws-2023/>. The LCO can provide more examples/information upon request.
- <sup>28</sup> See, for example, Article 5, s. 3.1.2 (b) of General Data Protection Regulation (GDPR), online at: [https://gdprhub.eu/Article\\_5\\_GDPR](https://gdprhub.eu/Article_5_GDPR). See also Office of the Privacy Commissioner, “*Principles for responsible, trustworthy and privacy-protected generative AI technologies*” (December 7, 2023), online at: [https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd\\_principles\\_ai/](https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/) at sections 1 (“Legal Authority and Consent”) and 2 (“Appropriate Purposes”).
- <sup>29</sup> See generally, Data and Society, *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest* [Assembling Accountability] [2021], online at: <https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/>
- <sup>30</sup> Federal AIA.
- <sup>31</sup> European Commission, *Impact Assessment of the Regulation on Artificial Intelligence* (2021), online: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence>
- <sup>32</sup> US AI Bill of Rights at 5, 23, and 28.
- <sup>33</sup> Vector Institute, *Managing AI Risk Thought Leadership Project*, March 2023. On file with the LCO.
- <sup>34</sup> European Commission, High Level Expert Group on Artificial Intelligence, *Assessment List for Trustworthy AI*, [2020], online: <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.
- <sup>35</sup> Government of the Netherlands, *Fundamental Rights and Impact Assessment*, (2021), online: <https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms>.
- <sup>36</sup> ECP, *AI Impact Assessment*, (2018), online: <https://ecp.nl/publicatie/artificial-intelligence-impact-assessment-english-version/>.

- 
- <sup>37</sup> Microsoft Corporation, *Responsible AI Standard and Impact Assessment*, (2022), online: <https://www.microsoft.com/en-us/ai/tools-practices>.
- <sup>38</sup> Eticas AI, *Guide to Algorithmic Auditing*, (2022), online: <https://eticas.ai/guide-to-algorithmic-auditing/>.
- <sup>39</sup> Algorithm Watch, *Impact Assessment Tool for Public Authorities*, (2021), online: <https://algorithmwatch.org/en/adms-impact-assessment-public-sector-algorithmwatch/>
- <sup>40</sup> Floridi, Luciano and Holweg, Matthias and Taddeo, Mariarosaria and Amaya, Javier and Mökander, Jakob and Wen, Yuni, *capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act* (2022), online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4064091](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4064091)
- <sup>41</sup> Notable examples include the EU AI Act and the US Executive Order on AI. Other recent and interesting examples include the *California Consumer Privacy Act*, (updated 2024), online: <https://oag.ca.gov/privacy/ccpa>; the *California Generative Artificial Intelligence Accountability Act* (California Senate Bill 896, 2024), online: <https://legiscan.com/CA/text/SB896/id/2868456>; and the Massachusetts *Relative to Cybersecurity and Artificial Intelligence Act* (Mass. Bill S.2539, 2023), online: <https://malegislature.gov/Bills/193/S2539>. See also generally, LCO Accountable AI.
- <sup>42</sup> See generally, European Commission, “*Shaping Europe’s Digital Future, AI Act*”, online: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.
- <sup>43</sup> See generally, Canada, *The Artificial Intelligence and Data Act (AIDA) – Companion Document* [AIDA Companion Document], online: <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s6>.
- <sup>44</sup> Canada ADM Directive, Appendix B – Impact Assessment Levels.
- <sup>45</sup> US Executive Order on AI.
- <sup>46</sup> The White House, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (2022), online: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>.
- <sup>47</sup> AIDA Companion Document.
- <sup>48</sup> Canada ADM Directive, Appendix B – Impact Assessment Levels.
- <sup>49</sup> EU AI Annex III.
- <sup>50</sup> Canada Federal Directive, s. 6.
- <sup>51</sup> LCO Regulating AI at 22-23.
- <sup>52</sup> EU AI Act, Chapter II: Prohibited Artificial Intelligence Practices, Article 5, online: <https://artificialintelligenceact.eu/article/5/#:~:text=The%20EU%20AI%20Act%20prohibits,risk%20of%20committing%20a%20crime>.
- <sup>53</sup> EU AI Act, Chapter III: High-Risk System, online: <https://artificialintelligenceact.eu/chapter/3/>
- <sup>54</sup> The LCO can provide a compendium upon request.
- <sup>55</sup> See generally, Algorithm Watch, *Auto-check – Mapping Risks of Discrimination in Automated Decision-making Systems* (2021), online at: <https://algorithmwatch.org/en/autocheck/>.
- <sup>56</sup> Ontario Trustworthy AI Framework.
- <sup>57</sup> New Zealand Law Foundation, *Government Use of Artificial intelligence in New Zealand* [NZ Government AI] (2020), online: [https://www.researchgate.net/publication/338701988\\_Government\\_Use\\_of\\_Artificial\\_Intelligence\\_in\\_New\\_Zealand\\_at\\_4](https://www.researchgate.net/publication/338701988_Government_Use_of_Artificial_Intelligence_in_New_Zealand_at_4).
- <sup>58</sup> NZ Government AI.
- <sup>59</sup> EU AI Act, Chapter VII: Governance, online: <https://artificialintelligenceact.eu/chapter/7/>
- <sup>60</sup> EU AI Act, Chapter XII: Confidentiality and Penalties, online: <https://artificialintelligenceact.eu/chapter/12/>
- <sup>61</sup> EU AI Act, Article 88, Enforcement of Obligations on Providers of General Purpose AI Models, online: <https://artificialintelligenceact.eu/article/88/>
- <sup>62</sup> New York City, Executive Order 50, *Establishing An Algorithms Management And Policy Officer* (2019), online: <https://www.nyc.gov/office-of-the-mayor/news/554-19/mayor-de-blasio-signs-executive-order-establish-algorithms-management-policy-officer-at-1>. Note that this role has been updated by the current New York City administration in a “New York City Artificial Intelligence Action Plan” which includes a new Office of the Technology and Innovation. See generally, New York City, “Mayor Adams Releases First-of-Its-Kind Plan for Responsible Artificial Intelligence Use in NYC Government” (October 16, 2023), online:



---

<https://www.nyc.gov/office-of-the-mayor/news/777-23/mayor-adams-releases-first-of-its-kind-plan-responsible-artificial-intelligence-use-nyc#/0>

<sup>63</sup> Canada Federal Directive at 6.4.1.

<sup>64</sup> *AIDA*, s. 33.

<sup>65</sup> Bitar, Omar and Deshaies, Benoit and Hall, Dawn, *3rd Review of the Treasury Board Directive on Automated Decision-Making* (2022), online at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4087546](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4087546)

<sup>66</sup> For example, the US AI Bill of Rights states:

*Consultation. The public should be consulted in the design, implementation, deployment, acquisition, and maintenance phases of automated system development, with emphasis on early-stage consultation before a system is introduced or a large change implemented. This consultation should directly engage diverse impacted communities to consider concerns and risks that may be unique to those communities, or disproportionately prevalent or severe for them.*

US *AI Bill of Rights* at 18. Similarly, the Government of Ontario has stated that “Ontario’s AI framework will be developed following Open Government Partnership principles to demonstrate the province’s commitment to transparency, accountability **and working in open with the people of Ontario**.” [Emphasis added.] Government of Ontario, “Consultation: Ontario’s Trustworthy Artificial Intelligence (AI) Framework, online at:

<https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework-consultations>