# 

# Consultation: Ontario’s Trustworthy Artificial Intelligence (AI) Framework

Submission by:

Bob Fay

Managing Director of Digital Economy

Centre for International Governance Innovation (CIGI)

3 June 2021

**No AI in Secret**

**The use of AI by the government will always be transparent, with people knowing when, why, and how algorithms are used and what their rights are if harm occurs.**

**How would you rank the following action items, in order of importance, using a scale where 1 is “very important” and 3 is “less important”, as part of "No AI in Secret"?**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1** | **2** | **3** |
| Provide clarity and transparency to the public on how Ontario collects data for use in algorithms (e.g. explore options to update provincial notices of collection to inform the public if data collected is used to develop algorithms for decision-making.). |  |  |  |
| Be fully transparent when using algorithms to interact with the public (e.g. rules to require the public be informed if they are interacting with a machine or have decisions made about them by an algorithm) |  |  |  |
| Create accountability for the use of AI in the government by giving people rights to address potential biases created by the AI (e.g. right to explainability, right to contest, and right to opt out) |  |  |  |

**Are there any additional action items to support "No AI in Secret" that you think should be included in Ontario's AI framework? (text box)**

Thank you for the opportunity to comment on this proposal.

The Ontario government is to be commended for undertaking this consultation. Artificial intelligence is likely to become pervasive in all aspects of society, and it has the promise to bring enormous societal gains. But to ensure that the gains are maximized, and the harms minimized governance needs to be improved. Indeed, appropriate governance is required for the public to trust the use of the technologies which will in turn assist in their diffusion and boost innovation. With the looming advent of 5G and IoT, it is particularly important that these governance frameworks be set up to fully harness the innovation possibilities while maintaining trust in the use of the technologies.

As discussed further below, AI should not be viewed in isolation and it is encouraging that the Ontario government also has consultations underway on whether to introduce private sector privacy legislation, and on a digital and data strategy. These consultations should not be considered in isolation from each other. There are important synergies among them, and potential trade-offs and they should all be considered together when recommendations are made related to AI. In addition, the Information andPrivacy Commissioner recently released it’s [Strategic Priorities](https://www.ipc.on.ca/about-us/ipc-strategic-priorities-2021-2025/#:~:text=The%20IPC%E2%80%99s%20external%20ad%20hoc%20strategic%20advisory%20committee%2C,range%20of%20stakeholders%20during%20the%20public%20consultation%20process.) developed in conjunction with the an advisory committee in which CIGI (Bob Fay) participated. It identifies many similar issues, and includes recommendations related to Responsible Use of Data for Good and Transparency and Open Government that are relevant. Please note that it is in this context that I have not ranked the action items – I believe that you have brought forth important items that need to be addressed together.

I would note that the questions raised in this consultation, while appropriate, also assume a level of knowledge that may not be resident in the general public and presumably the government is also consulting with specific groups. The questions also appear to place the emphasis on the individual to know and understand their “rights” and their obligations to object. The consultations should probe whether this is a suitable assumption. For example, would citizens have sufficient information on the implications of the use of their personal data use: how would a citizen know if they have been potentially harmed? If this information were available, would the process for appeal be transparent and clear, timely and affordable? What body would adjudicate harms? What would be the implications of opting out? What does explainability mean and how would you address different levels of knowledge by the public?

Turning to some general points. It is important to:

* Consider AI as part of a system and not view it independently from the data that drive the machine learning (ML) algorithms or how the AI may be used. For example, take the issue of bias. Bias could come from data and a lack of understanding of the properties of the data that are used to train algorithms; it could come from choices made on the suitability and choice of ML models and their parameterization; and it could come from how the models are implemented and used -- the AI – indeed the bias might not emanate from the AI itself but how a human uses that information if a human is (hopefully) in the loop. The focus in this question seems to be on bias created by one specific element and would not capture other relevant sources of bias.
* Develop governance frameworks to guide the use of AI prior to its widespread implementation. These frameworks need to consider the broad nature of both the benefits and harms that can emanate from the AI systems, and to consider interlinkages. The frameworks must be both comprehensive and they must be systematic, i.e. used consistently. The framework includes among other things:

1. That rules and regulations related to privacy, cyber security, competition policy, public safety, health, consumer protection and so on are considered.
2. That consent for the use of data/AI is meaningful. Consent needs to be simplified, standardized and clarified on how personal (or other including commercial) data are used and reused. It would be insufficient to simply say whether information might be used in an algorithm. Consent should include how data may be shared, reused, under what conditions and so on. This framework should also consider the risks related to the uses of private and public information and tailor obligations accordingly.
3. That standards are created and incorporated. Standards can be used to create appropriate consent agreements; to define the different types of data and the controls around their uses and reuses, including data portability, as well as AI system interoperability and so on. Standards can be used to develop frameworks for transparency and auditing that form the basis of accountability. Standards should be created jointly between the public and private sectors, including civil society. Standards allow two things: they imbed our technical expertise and very importantly they also imbed our values for example respect to fundamental human rights. They can create a playbook for organizations to follow and a playbook for trust. They can bring predictability, which is required for businesses and consumers alike.
4. That coordinating mechanisms across government and across levels of government are set up. The elements of the framework may go beyond provincial jurisdiction and will likely require coordination with the federal government and there may be international developments and agreements that might also need to be considered, for example the Canada US Mexico Free Trade Agreement (CUSMA).
5. That the development of governance frameworks is inclusive, e.g. a multistakeholder approach is taken which will help to build trust among all citizens for the responsible uses of AI systems and minimize harms to particular groups.
6. That the public sector is equipped to deal with the implementation and monitoring of AI systems, e.g. training, knowledge diffusion and so on.

Some specific points related to this question:

* The “rights” as set out here could create confusion. One could argue that the use of AI should be consistent with a human rights framework and demonstrate accountability relative to that framework. The “rights” proposed here are not immutable like human rights and could be taken away if a different government has different views.
* Please define public. Does it refer to interactions with individuals, businesses, civil society, researchers, others? Are they all considered “people’s rights”? Each would likely have different levels of needs.
* Would these same requirements be imposed on vendors that develop AI systems or if they deliver services (e.g. via outsourcing)?
* Are there some situations where AI should not be used, for example where the risks of incorrect or unsuitable decisions could lead to significant harm? Which groups for example children?
* Which part of the government would be the one to assess algorithms and their implications? Does the public service currently have the skills to do so? How would the government coordinate across departments to deal with the many issues related to the uses and governance of AI?

**AI use Ontarians can trust**

**Rules and tools are in place to safely and securely apply algorithms to government programs and services based on risk.**

**How would you rank the following action items, in order of importance, using a scale where 1 is “very important” and 3 is “less important”, as part of “AI use Ontarians can trust”?**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1** | **2** | **3** |
| Assess whether to use an algorithmic assessment tool as a way to measure risk, security, and quality. |  |  |  |
| Deliver recommendations on ways to update Ontario’s rules, laws and guidance to strengthen the governance of AI, including whether to adopt a risk-based approach to determine when which rules apply. |  |  |  |
| Ensuring processes are in place so that algorithms are continuously tested and evaluated for bias/risk and whether audits or human oversight controls are needed. |  |  |  |

**Are there any additional action items to support "AI use Ontarians can trust" that you think should be included in Ontario's AI framework? (text box)**

Please define an algorithmic assessment tool. Is this an algorithm (it could be) and if so what risks would it represent? Is it something similar to the Algorithmic Impact Assessment questionnaire developed by the federal government that guides the use of AI? Could that be adapted to Ontario’s needs?

With respect to ways to an update Ontario rules and laws once again, please see the IPC report referred to earlier. Ontario should coordinate where possible with the federal government and should also be aware of developments taking place outside the country that may have implications, for example in Europe (General Data Protection Regulation, Digital Services Act etc).

Processes related to algorithms should be included in the transparency and metrics mentioned earlier. They should include periodic audits. A question is how to carry out the audits – skills to do it and interpret the results, track the algorithms that continually update and can be “black box” in nature, and so on. If the algorithmic tool is developed by the private sector, and implemented internally, could it be protected by intellectual property such as a trade secret that could limit auditing? Would this require new legislation and would it be consistent with CUSMA?

Any ability to address and put in place processes will require a public service that has the skills both technically, e.g. understand how big data and AI are used, but as well related to governance and how to innovate governance tools so that they are suitable to regulate big data and AI.

**AI that serves all Ontarians**

**Ontarians benefit economically and socially from AI technologies that are rooted in individual rights and reflect the diverse communities across the province.**

**How would you rank the following action items, in order of importance, using a scale where 1 is “very important” and 3 is “less important”, as part of "AI that serves all Ontarians"?**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1** | **2** | **3** |
| Assess whether the government should prohibit the use of AI in certain use cases where vulnerable populations are at an extremely high risk. |  |  |  |
| Embed equity and inclusion in the use of data and digital tools by requiring organizations to take steps to mitigate potential harms (e.g. data set requirements, documentation requirements for traceability, accountability provisions). |  |  |  |
| Engage with sector leaders and civil society to develop a standard for “trustworthy AI” and a process to certify that vendors are meeting the government’s standard. |  |  |  |

Clear privacy rules and data governance standards will help to eliminate data silos and promote the sharing of data provincially, nationally, and internationally with the enormous economic opportunities that can be achieved via aggregated and well curated data that respect privacy. Indeed, governance framework conditions for Ontario should recognize that privacy is an essential element of good governance and builds trust with individuals, creates a business opportunity for firms and will create wealth for the province.

Data can and should be used for the common good, e.g. socially beneficial purposes. This requires the careful management of data which can be done via different structures, including data trusts that contain rules which are consistent with the values of those who have provided their data to that trust. These structures do not pertain solely to personal data. They could also include how to share and combine corporate data. These data structures can also be sectoral based, such as health or manufacturing, and create the rules for data sharing and reuse upon which firms can innovate. These structures might be particularly useful to small and medium size enterprises. Managing data and AI systems requires a new set of skills that goes beyond STEM, including behavioural sciences, and new occupations such as data stewards. It is also important to have a multi-stakeholder approach to develop governance over AI systems given how different communities may be affected. This approach should be systematic. Note the use of the term governance and not “standard”. Standards are an important element of governance, but governance is much broader and can include different forms of regulation and laws.

One framework to consider to govern the use of AI systems is a “duty of care” approach, something that is proposed in the [UK on-line safety bill](https://www.gov.uk/government/publications/draft-online-safety-bill). This approach focusses on the potential risks from AI and mandates that such risks are identified before AI systems are used, and where deemed relevant by the regulator, that mitigation measures are put in place prior to use. The report from the IPC dealt with these issues, particularly with respect to children. It is clear that some groups require different treatment where informed consent is not possible.

**Are there any additional action items to support "AI Serves all Ontarians" that you think should be included in Ontario's AI framework? (text box)**

In conclusion

1. Need to focus on the value chain – data, AI, platforms and uses of technologies, not simply AI.
2. Need to develop frameworks that recognize the links and interconnected nature of this value chain. It is important to indicate how does this consultation fits in with those that have taken place recently on private sector privacy and related to the digital and data strategy. They should all be considered together and integrated.
3. Need to use appropriate governance tools, e.g. standards, regulations, laws and to decide which ones to implement based on an assessment of risks and harms. They should reflect the different needs and risks related to different types of data.
4. Standards for trustworthy AI are essential -- see CIOSC standards on data and ethical AI.
5. Need to create a transparency and metrics framework that can be used for accountability of the uses of data and AI systems.
6. Need to update the skills of public servants and create new roles such as data stewards.
7. There is a lot being done outside the province and frameworks would likely need to be consistent with areas outside of its jurisdiction for example our trade agreements (see chapter 19 of CUSMA); and other jurisdictions, e.g. (EU DSA, GDPR etc).

Please find a list of relevant CIGI publications that may assist, and we would be happy to discuss further.

[Models for Platform Governance - Centre for International Governance Innovation (cigionline.org)](https://www.cigionline.org/models-platform-governance/)

[A Canadian Framework for Data Reuse - Centre for International Governance Innovation (cigionline.org)](https://www.cigionline.org/publications/canadian-framework-data-reuse/)

[Statistics Canada Should Be Central to a National Data Reuse Framework - Centre for International Governance Innovation (cigionline.org)](https://www.cigionline.org/articles/statistics-canada-should-be-central-national-data-reuse-framework/)

[The Next Wave of Platform Governance - Centre for International Governance Innovation (cigionline.org)](https://www.cigionline.org/articles/next-wave-platform-governance/)

[Standards for a Secure 5G Infrastructure - Centre for International Governance Innovation (cigionline.org)](https://www.cigionline.org/publications/standards-secure-5g-infrastructure/)

[Modern Conflict and Artificial Intelligence - Centre for International Governance Innovation (cigionline.org)](https://www.cigionline.org/publications/modern-conflict-and-artificial-intelligence/)

[Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves - Centre for International Governance Innovation (cigionline.org)](https://www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves/)