CARL ABRC
CANADIAN ASSOCIATION OF RESEARCH LIBRARIES
ASSOCIATION DES BIBLIOTHÈQUES DE RECHERCHE DU CANADA

Mr. John Roberts
Chief Privacy Officer and Archivist of Ontario, and Chief Information Security Officer (A)
Information, Privacy and Archives Division and Cyber Security Division
Ministry of Government and Consumer Services
134 Ian MacDonald Blvd
Toronto, ON, M7A 2C5
Sent via email: John.Roberts@ontario.ca

Dear John,

The following is the CARL submission to the Ontario government's Consultation on Developing Ontario's Artificial Intelligence (AI) Framework. The Consultation closed on June 4, 2021. **This information was also submitted on June 4 using the web form provided as part of the consultation process.**

Note: The following letter includes the "additional comments" submitted by CARL on June 4, but we did also submit a ranking of the action items in each category in the draft. Even with our submitted ranking, our stance is that each action item is needed as part of this process and should be fully investigated and implemented by the government.

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

The goal of this section - to ensure that the use of AI by the government is always transparent, fair, and equitable - is laudable, and the Ontario government and its citizens are rightfully concerned about association with AI companies and the government's use of algorithms for services or communication. Yet, as you will see from our comments, the evolving nature of AI complicates this goal.

There is no question that there must be clarity and transparency in the process, and transparency related to AI needs to be defined and utilized in the public interest. There must be laws or regulations on the length of time that citizens' data can be retained, how it will be used or reused, and restrictions on how it can be shared, resold or repackaged without the explicit permission of the subject.

Ontario citizens have a right to view and control their data, and to know how their data will be used and reused by the government, with no third-party access and no third-party advantage (such as building a dataset). As a trusted entity, the Ontario Government must ensure it places the ethical use of AI technology and algorithms and respect for the data of its citizens as a cornerstone principle. Citizens must be confident that their data will only be used for administrative purposes, and that they have the ability to opt out of sharing their data and receiving the service in an alternative way. Ontario citizens have the right to own their data and control its use and reuse.

The government must confront the fact that many of the companies that sell products that depend on AI are inherently problematic. These technologies can reinforce racial biases (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423, https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/) and invade the privacy of citizens. While there are many problematic examples of the latter, the most ominous are those companies that scrape images from the internet to build massive databases of biometric information about individuals. Clearview AI, for example, has used this model toward their facial recognition service, and their dataset has been used by large companies and by police departments to identify individuals. Fortunately, Clearview AI is now illegal in Canada (https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html) but it took an investigation by the NYT (https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html) and a study by the OPC (https://priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203) to make this happen.

There are many risks in providing biometric information - like passport or driver's license photos - to third-party companies. For example, it is not always known how biometrics will be used - even with assurances from the companies. Governments and citizens need the protection of robust laws to protect the use and privacy of data, and severe, crippling penalties for breaches of the law. Worryingly, many of these AI companies have links to the far-right and to white supremacy groups, (https://medium.com/@AINowInstitute/ai-and-the-far-right-a-history-we-cant-ignore-f81375c3cc57) and these viewpoints may be reflected in the outputs of their algorithms.

As opposed to data breaches of email addresses and passwords, which are easily changed, data breaches that include biometric information like an iris scan or a fingerprint or even an image of one’s face, which are forever tied to your identity, can cause incalculable damage. Ontario must distance itself from such companies and practices.

COVID-19 has led to the mass adoption of surveillance technologies by governments around the world. According to the Electronic Frontier Foundation (EFF):

> Governments around the world are demanding extraordinary new surveillance powers (https://www.eff.org/deeplinks/2020/12/covid-19-and-surveillance-tech-year-review-2020) that many hope will contain the virus’ spread. But many of these powers would invade our privacy (https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis), inhibit our free speech

(https://www.eff.org/deeplinks/2020/04/some-covid-19-surveillance-proposals-could-harm-free-speech-after-covid-19), and disparately burden vulnerable groups of people (https://www.eff.org/issues/covid-19).

This type of "security theatre" should be resisted at all costs, as many meagre or perceived benefits come at the expense of the privacy (and other) rights of citizens. The entire EFF statement includes a number of questions that governments must ask when considering these types of technologies (https://www.eff.org/issues/covid-19).

Educational and research tools that enable academic surveillance and potentially commodify the personal and professional data of individuals at universities and colleges should be carefully examined and regulated. Examples of the issues caused by AI technologies in this sector are described in the following articles:

- Addressing the Alarming Systems of Surveillance Built By Library Vendors https://sparcopen.org/news/2021/addressing-the-alarming-systems-of-surveillance-built-by-library-vendors/
- Elsevier Has Deployed an End-user Tracking Tool for Security. Should Users Be Concerned About Their Privacy? https://scholarlykitchen.sspnet.org/2020/10/13/elsevier-has-deployed-an-end-user-tracking-tool-for-security/
- Student Privacy and the Fight to Keep Spying Out of Schools: Year in Review 2020 https://www.eff.org/deeplinks/2020/12/student-privacy-and-fight-keep-spying-out-schools-year-review-2020
- Cheating-detection companies made millions during the pandemic. Now students are fighting back https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/ (One of the companies mentioned in this story (Proctorio) is in litigation with an educational developer from the University of British Columbia for posting a series of tweets linking to Proctorio faculty training videos, which the company considers to be confidential. Linkletter is a vocal critic of "academic surveillance software" tools, and this action demonstrates the aggressive stance that this industry can take in silencing its critics https://www.insidehighered.com/quicktakes/2020/10/20/ed-tech-specialist-fights-proctorio-lawsuit).

As for transparency, what does it mean in this context? How would a citizen know if an algorithm is transparent? Is there a transparency standard? Transparency must be defined in a way that benefits citizens and provides an avenue for all who interact with AI algorithms to have the algorithm reviewed by unbiased authorities. This process must happen in a timely manner, and the results of this review should then be open to public view. Ontarians must be made aware when they are interacting with artificial intelligence algorithms, or AI machines, and be given the ability to opt out of such interaction, and be presented with an alternative, non-AI way, to interact with the government for information for services. A citizen must be able to request an alternative method of contact, and in no case must a citizen be denied service due to opting out of AI-facilitated tools.

The Government of Ontario and Ontarians need to confront the problems with AI in general, and specifically determine appropriate Terms of Use that respect citizens' rights and prevent overreach of companies or governments involved in AI. The acquisition of citizens' data is already occurring and regulations are long overdue. We need to carefully consider how the Ontario government plans to approach the often-egregious lack of accountability of current AI collection practices of private citizens' data. It must be a condition of every third-party contract that all citizens' data be completely deleted after its use, including anonymized data as it can be easily re-combined to identify an individual, unless permitted by each individual.

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

At a minimum, there should be rules and tools put in place to safely and securely apply algorithms to government programs and services based on risk. Yet, this is once again complicated by the nature of AI and its lack of penetrability for the average citizen.

As reflected in our response to question 1, a risk-based approach to determine which rules apply in artificial intelligence governance is an unsatisfactory approach to protecting citizens' rights. Citizens' rights must come first, and government regulations must be implemented to prevent abuse of rights. The current business model used by many big tech companies like Google and Amazon – do it until you get sued or are brought before a government committee – tramples on citizen rights to privacy and data protection. Citizens are in a "David and Goliath" scenario where average citizens may be alarmed but unsure how to protect their rights. Proper governance of artificial intelligence algorithms and regulation of use of AI by large corporate online intermediaries and publicly funded educational institutions, are crucial for the protection of Ontario citizens' rights. The idea that private companies or the provincial or federal governments can govern themselves without laws and regulations and appropriate oversight is anathema to good government tenets of accountability, integrity, stewardship, and transparency.

At the core, governments must respect principles of ethics, fairness, explainability, transparency, and opt-out options for uses of AI algorithms for government purposes and decision-making.

Also reflected in our response to question 1 is the harmful impact of Automatic Decision Systems. Automated Decision Systems, which are used in government decision-making, suffer from the "person behind the machine" – whoever created the system and what biases are built-in as a result. Excluding bias is extremely difficult and ADS has been shown to have harmful effects on equity-deserving or equity-deprived groups. Third-party technology companies may not have the proper expertise to do a thorough review of bias that governments and public interest organizations would demand, nor should they be trusted to do so. How such review is tendered or how many reviewers are used will have significant consequences on true screening for bias. Absolutely, there must be processes in place to ensure that algorithms are continuously tested and evaluated for bias/risk.

As stated by the AI Now Institute, “When artificial intelligence and related technologies are used to make determinations and predictions in high stakes domains such as criminal justice, law enforcement, housing, employment, hiring, and education, they have the potential to impact basic rights and liberties in profound ways.” (https://ainowinstitute.org/).

3. Are there any additional action items to support "AI Serves all Ontarians" that you think should be included in Ontario's AI framework?

The Ontario government is fully aware of the frameworks used by the federal government and by other jurisdictions that will help with this goal. The federal government has a Directive on Automated Decision-Making (tbs-sct.gc.ca): https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592&section=html that makes it a requirement to have an Algorithmic Impact Assessments as a practice and attempts to embed more transparency in the process for Canadians. Yet, there are many other resources and tools that can help the Ontario government design a framework that serves all Ontarians to only use “AI technologies that are rooted in individual rights and reflect the diverse communities across the province.”

The Ontario government should, at minimum:

- Read all of the reports created by the AI Now Institute at New York University. This is an interdisciplinary research center dedicated to understanding the social implications of artificial intelligence. See their list of publications here: https://ainowinstitute.org/reports.html
- Carefully consider the points raised by the EFF in their Covid-19 and Digital Rights post referenced above: https://www.eff.org/issues/covid-19 and their general page on AI: https://www.eff.org/issues/ai
- Examine the critiques of systems in place in other jurisdictions, for example, AlgorithmWatch has a comprehensive critique of the shortcomings of trustworthy AI here: https://algorithmwatch.org/en/trustworthy-ai-is-not-an-appropriate-framework/ While writing from a European perspective, many algorithmwatch publications can help inform what we are doing in Ontario: https://algorithmwatch.org/en/publications/

As this process is designed, the government of Ontario must pay careful attention to the requirements of indigenous communities, who are entitled to full sovereignty over their data under the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). Data sovereignty would require that governments and researchers allow these peoples and their communities to retain ownership and control of their own data, and that any use of this data be fully transparent and used only after thorough consultation.

More information is available here:

- The First Nations Principles of OCAP® | The First Nations Information Governance Centre https://fnigc.ca/ocap-training/
- Indigenous Data Sovereignty: https://fnigc.ca/wp-content/uploads/2020/09/bbe195ddc231e3b1222d71ca4c09ae62_indigenous_data_sovereignty_toward_an_agenda_11_2016.pdf
- United Nations Declaration on the Rights of Indigenous Peoples https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html

Until the public understands the ownership and rights in their data and the substantial threats posed by AI facilitated interfaces, one option that should be considered is a moratorium or extremely limited use by the government of AI algorithms and the associated tools. The Ontario government must begin with a statute vesting ownership of data to each individual citizen and prevent contracts from stripping citizens of their privacy rights.

The ability for citizens to freely express ideas and views is essential to a free and democratic society and it should also be their choice if they want to opt-out of AI algorithms and AI operations. Freedom of expression is a fundamental human right and a cornerstone principle of libraries, archives, and museums (LAMs). Surveillance and fear of oversight of ideas and opinions fundamentally interfere with the most vital of human rights. The potential to track the online activity of individuals through AI invades privacy rights and impinges on other human rights, such as intellectual freedom, and the increased regulation of the Internet threatens the principle of net neutrality, further impinging human rights, such as freedom of access to information.

As it stands, AI poses a significant risk to the rights of all Ontarians, and we applaud the government in taking steps towards understanding and mitigating the risks involved.

Thank you for giving us the opportunity to respond to this consultation. If you have any further questions or you would like us to follow up on any points of interest, please do not hesitate to contact us.

Susan Haigh
Executive Director