ONTARIO SOCIETY OF PROFESSIONAL ENGINEERS

Office of the Privacy Commissioner of Canada
30, Victoria Street
Gatineau, Quebec
K1A 1H3

RE: Consultation on Artificial Intelligence

About the Ontario Society of Professional Engineers (OSPE)

The Ontario Society of Professional Engineers (OSPE) is the voice of the engineering profession. We represent Ontario's 85,000 professional engineers and 250,000 engineering graduates.

The Canadian economy is going through a fundamental technological and economic shift. This creates demand for a highly skilled, technical workforce, that engineers can fulfill. Engineers are innovative problem solvers who develop solutions by considering costs, benefits, sustainability, public safety, and the complete lifecycle and integration of projects.

Engineers will lead Ontario's industries into the future and generate wealth for the nation through the development and commercialization of new technologies. By exporting technologies to global markets engineers will attract foreign direct investment and bolster Ontario's reputation.

Engineers play a key role in the development, implementation, and use of artificial intelligence technology. They are well positioned to ensure that this promising technology is put to good use, establish Canada as a leader in this field, and protect the public interest. Given the ambiguities surrounding the use of a new technology, the engineering community supports the Office of the Privacy Commissioner's study of the impact of AI on *Personal Information Protection and Electronic Documents Act* (PIPEDA). Determining which aspects of AI technology can be harmful and which can be beneficial is of utmost importance and we are happy to submit the following considerations.

Proposals for Consideration

Proposal 1: Incorporate a definition of AI within the law that would serve to clarify which legal rules would apply only to it, while other rules would apply to all processing, including AI.

Agree:
The lack of a clear and universally accepted definition of AI is impacting the ability to create effective frameworks and regulation for this technology. Industry experts report that most of the time what is referred to as AI is not true AI algorithm but rather, it is machine learning. A lack of a common definition means that academia, governments, and industry could be talking about different things when discussing AI. Stanford's *One Hundred Year Study on AI* provides a guideline for what to consider when developing a definition of AI.

1. Should AI be governed by the same rules as other forms of processing, enhanced as recommended in this paper (which would mean there would be no need for a common definition and the principles of technological neutrality would be preserved) or should certain rules be limited to AI due to its unique risks to privacy and, consequently, to other human rights?

AI regulation should be grounded in universal human rights principles (e.g. the EU's GDPR) while providing regulations tailored to technology-specific rules from a research and design perspective, as well as industry-implementation perspective.

2. If certain rules should apply to AI only, how should AI be defined in the law to help clarify the application of such rules?

Agreement must exist on a larger all-encompassing definition (such as the one crafted by the OECD). This should then be linked to regulations which further expand on these principles to account for specific areas of evolving AI research, such as but not limited to: large-scale machine learning, deep learning, reinforcement learning, robotics, computer vision, natural language processing, collaborative systems, crowdsourcing and human computation, Internet of Things (IoT), and neuromorphic computing.

Proposal 2: Adopt a rights-based approach to the law, whereby data protection principles are implemented as a means to protect a broader right to privacy—recognized as a fundamental human right and as foundational to the exercise of other human rights.

Agree:
The European Union’s foundational right to privacy could be used to inform this. Specifically:

Article 7 of the Charter of Fundamental Human Rights of the European Union: *"Respect for private and family life. Everyone has the right to respect for his or her private and family life, home and communications."* (anchor the right)

Article 12 of the UN declaration of human rights: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."* (outline prohibited actions)

Article 8 of the EU Convention on Human Rights modifies this broad principle with a public-interest exception: (outline a limited exception)

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right ***except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country****, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

1. **What challenges, if any, would be created for organizations if the law were amended to more clearly require that any development of AI systems must first be checked against privacy, human rights and the basic tenets of constitutional democracy?**

It would likely slow down product development and increase timelines for getting to market. Private entities would also likely raise concerns that having a clearance mechanism in place administered by a public entity would raise intellectual property (IP) issues. Having a specialized regulator could help address the delays faced by industry. In terms of IP related concerns, it is important that the government secures confidence from the private sector in the regulatory oversight. The data shared with the government should itself be private and secure. An exception to the patent regime's non-disclosure requirement could be implemented for any pre-filed patent applications. The government could also agree to an NDA or create a procedural status for the documents such that all product information shared is considered under seal. The publicly viewable license given to the entity is merely a "green light" (meets Canadian AI-privacy standards) or "red light" (does not meet Canadian AI-privacy standards).

Proposal 3: Create a right in the law to object to automated decision-making and not to be subject to decisions based solely on automated processing, subject to certain exceptions.

Disagree:
The power of automated decision making, and machine learning (ML), could improve the way Canadian businesses operate. The law should not prohibit this innovation. It should, however, strongly tie the liability for the results of all automated systems to private entities that create and profit off them.

1. **Should PIPEDA include a right to object as framed in this proposal?**

No, the right to object should be limited to matters of (1) healthcare (2) justice (i.e. if the court ever adopts automation in its substantive decision-making process or procedural administration process) (3) taxes and (4) insurance rates & benefits

2. **If so, what should be the relevant parameters and conditions for its application?**

Dr. Aleksander Madry (MIT) outlines an ML design philosophy that provides transparency on the key decision-making factors in an automated system. This approach should be considered as a best practice. Citizens\consumers should be able to request a report from their governments\private companies outlining the reasons behind an automated decision. Once this report has been reviewed, the citizen\consumer should be able to appeal to a manager for the ML's programming and administration of its tasks. This first level discussion should be about deficiencies in the ML's analysis. A relevant discussion would be whether the ML operating parameters adequately took into account all relevant factors for the proper administration of the decisions it was meant to carry out. This first-level manager decision should be available to appeal to a higher authority that that has a broader view of policy as between the private\public entity utilizing the ML and the consumers\citizens whose lives are affected by it. Parameters would be:

(1) Is the ML behaving as intended by the owner (i.e. it is in fact carrying out its protocols in the way the tech team intended)?

(2) Are there deficiencies in the original ML protocol (i.e. circumstances that were not part of the original parameter setting) that should be adjusted?

(3) Does a new protocol need to be created for an exceptional case?

(4) Taking a step back, when the result of the disputed ML decision is compared against the private entity's mission\public entity's legislative mandate—is there a miscarriage of justice\violation of Canadian law?

Proposal 4: Provide individuals with a right to explanation and increased transparency when they interact with, or are subject to, automated processing.

Agree:
A standard design philosophy should be promoted within the AI community promoting a uniform way of reporting automated decision-making in non-technical language.

1. **What should the right to an explanation entail?**

   At a minimum, the protocols and data set used to train machine learning.

2. **Would enhanced transparency measures significantly improve privacy protection, or would more traditional measures suffice, such as audits and other enforcement actions of regulators?**

   New enhanced transparency measures that can provide real-time review of automated decisions as they are made are needed. The more traditional models are typically reactive to issue once they occur. Audit-standards are typically only refined after a breach has occurred.

Proposal 5: Require the application of Privacy by Design and Human Rights by Design in all phases of processing, including data collection.

Agree:
Embedding privacy principles into low-level design activities will create opportunities for private industry to develop comprehensive and efficient solutions that could minimize the amount of oversight required. An example of this is using embedded encryption vs. an entire system of response to handle an inevitable breach.

1. **Should Privacy by Design be a legal requirement under PIPEDA?**
   Yes. However, it should be considered further whether PIPEDA is where it should be included.PIPEDA could require that industry standards be followed (like IEEE, P7000) and industry experts could be responsible for specifying what "Privacy by Design" means.

2. **Would it be feasible or desirable to create an obligation for manufacturers to test AI products and procedures for privacy and human rights impacts as a precondition of access to the market?**
   Yes. Currently, the safety of machine equipment is tested for safety and security to prevent death or injury. Equipment such as engines is also subject to regulatory checks. A similar set of safety tests should be created for privacy and data management as the negative impacts of misuse or ineffective procedures could also be catastrophic.

Proposal 7: Include in the law alternative grounds for processing and solutions to protect privacy when obtaining meaningful consent is not practicable.

Disagree:
A consent-model of data protection is not an effective way to enforce privacy protection or foster innovation. When consenting, lay people often don't understand what they are agreeing and there is no follow-up with the data collector to ensure that the data disclosure is not subsequently used for a non-consented purpose. The consent model should be replaced by more comprehensive and robust technology designs requiring data "accessors" to seek permission from higher authorities for temporary use of data.

2. **Is it fair to consumers to create a system where, through the consent model, they would share the burden of authorizing AI (artificial intelligence) versus one where the law would accept that consent is often not practical and other forms of protection must be found?**

No, this is not fair to consumers who may not possess the technical knowledge and expertise of the law to truly understand what they are consenting to. Other forms of accountability should be considered and developed.

4. **Should consent be reserved for situations where purposes are clear and directly relevant to a service, leaving certain situations to be governed by other grounds? In your view, what are the situations that should be governed by other grounds**

Yes. Explicit consent should be required in two general cases:

Disclosure of medical history for the purpose of being considered for a new kind of treatment to a pre-existing condition and financial history for consideration of a loan or some other financial instrument.

Situations that should not be under a consent model include: the collecting of personal data by apps (particularly for minors) and insurance companies for the purpose of market research. Children downloading a game for entertainment should not have their data collected (usually under the guise of "market research") under the consent model. Those companies wishing to access that data should seek permission from a third party to unlock it. Online consent forms should be treated like waivers in tort. A waiver may be indicative of the service provider having outlined the risks to the consumer, but it is not an automatic defense if the service provider was negligent in their duty to protect privacy. In those cases, courts have ignored lengthy waivers that were signed by plaintiffs. Consent forms should be treated the same way. Commercial entity's duty of care to the public (with respect to privacy) outweighs whatever consent forms were signed by the data provider at the time of provision.

Proposal 8: Establish rules that allow for flexibility in using information that has been rendered non-identifiable, while ensuring there are enhanced measures to protect against re-identification

Agree:

However, there should also be rules on the destruction of the dataset after a defined period. Creating a culture of impermanence around data that is created\collected will further eliminate the risk of re-identification.

1. **What could be the role of de-identification or other comparable state of the art techniques (synthetic data, differential privacy, etc.) in achieving both legitimate commercial interests and protection of privacy?**

If properly executed de-identification could warrant relaxation of existing PIPEDA requirements (e.g. consent). It could also lower the threshold required for those seeking a license to use that data set for innovation\product development.

2. **Which PIPEDA principles would be subject to exceptions or relaxation?**

P 3 - Consent: Discussed above. While no consent model is as strong as an anonymous default system.

P 6 - Accuracy: This principle states that personal information must be as accurate, complete, and up to date as possible in order to properly satisfy the purposes for which it is to be used. For the quality of the work that will be done with the de-identified data set, the data should be accurate and up to date. But if it is de-identified, from a liability standpoint the obligation decreases as no one person or commercial entity within the dataset would suffer an adverse inference or consequence from inaccurate data since it is being used in an anonymized fashion. This principle serves to protect situations where decisions are made about an individual who has disclosed his or her information to a third party.

P 7 - Safeguards: This principle requires entities to protect personal information (in a way that is appropriate to how sensitive it is) against loss, theft, or any unauthorized access, disclosure, copying, use or modification. If the data has been de-identified its sensitivity and risk decreases.

All other PIPEDA principles should not be relaxed.

3. **What could be enhanced measures under a reformed Act to prevent re-identification?**

Include a sunset clause on the retention of data. PIPEDA should champion data deletion even if it is after a period of 10 years. In other words, expand Principle 5 which limits the use disclosure and retention of data.

Proposal 9: Require organizations to ensure data and algorithmic traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle
Agree:

In other professions, such as medicine, law, and accounting, professionals are required to keep a log of decisions made in doing work that could affect another's personal health, financial or personal interest. The same should be true for handling of sensitive data particularly where AI is applied.

1. **Is data traceability necessary, in an AI context, to ensure compliance with principles of data accuracy, transparency, access and correction and accountability, or are there other effective ways to achieve meaningful compliance with these principles?**

Data traceability is necessary, simple and effective. Documenting the design process and the current state of the decision-making protocols should be a minimum requirement. Mechanical engineers need to provide records of design development and safety testing for products that are sold to the public, and so too should software engineers keep up-to-date logs of ML protocols for the public should they be asked to prove privacy compliance.

Proposal 10: Mandate demonstrable accountability for the development and implementation of AI processing

Agree:

However, While the ODC's position is that PIPEDA's accountability requirement should be reframed to ensure an accountability for the algorithms and ML protocols that are developed. Organizations need to be responsible for not only the data that they store and use but also for the scripts driving automated outcomes.

1. **Would enhanced measures such as those as we propose (record-keeping, third party audits, proactive inspections by the OPC) be effective means to ensure demonstrable accountability on the part of organizations?**

To an extent, but record-keeping, third party audits, and inspections wouldn't be nearly as effective as encryption of data and other far-left measures implemented at the beginning of the data collection process.

2. **What are the implementation considerations for the various measures identified?**

The above suggestions risk being bureaucratic, slow to respond, inefficient and reactive.

3. **What additional measures should be put in place to ensure that humans remain accountable for AI decisions?**

Enforceable penalties in the way of fines should be put in place to ensure accountability.

Proposal 11: Empower the OPC to issue binding orders and financial penalties to organizations for non-compliance with the law

Agree.

1. **Do you agree that in order for AI to be implemented in respect of privacy and human rights, organizations need to be subject to enforceable penalties for non-compliance with the law?**

Yes, this is in large part why European companies and public entities have become more proactive on this matter. The actual enforcement of these laws is what make entities (public or private) change behaviour and build privacy-awareness into their R&D and product development cycles. It would also help fund a new specialized regulator to manage these matters.

2. Are there additional or alternative measures that could achieve the same objectives?

No, there is no method that would be equally effective.

OSPE believes that these recommendations are essential for the continued economic prosperity of our province. More importantly, these recommendations reflect the importance of guarding the public interest and safety. We look forward to working with the government to further develop these recommendations.

Sincerely,

Dr. Tibor Turi, P. Eng.
President and Chair
Ontario Society of Professional Engineers

Sandro Perruzza
Chief Executive Officer
Ontario Society of Professional Engineers

Contribution:
Beatrice Sze, P.Eng., JD, Subject Matter Expert, OSPE's Research and Innovation Task Force