ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

March 13, 2020

VIA E-MAIL

OPC-CPVPconsult2@priv.gc.ca

Re: Consultation on the OPC's Proposals for Ensuring Appropriate Regulation of Artificial Intelligence

The Electronic Transactions Association provides these comments in response to the Office of the Privacy Commissioner of Canada (OPC) *Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence* (Consultation Paper) on January 28, 2020.

The Electronic Transaction Association (ETA) is the leading trade association for the payments technology industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, mobile payment service providers, payment processors, mobile wallet providers, and non-bank online lenders that make commercial loans, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives. ETA member companies value the privacy protections that PIPEDA and other Canadian laws provide to protect the personal information of Canadian end users.

The payments industry deploys artificial intelligence (AI) to fight fraud, drive compliance with AML and anti-terrorist finance laws, and enhance small business financing. In the payments space, AI is used to examine each transaction for indicators of fraud in real time—looking at activities, patterns and more than 500 risk attributes—all in about one millisecond. Furthermore, the payments industry compares each transaction against known fraud schemes and it also uses the data to identify new or developing fraud schemes.

AI helps payment networks and banks detect anomalies in behavior that is outside the norm for a particular customer and their bank account. Anomalies could involve larger or more frequent transactions made in the US or in other parts of the world. Once anomalies are identified, the fraud fighting process continues. AI allows banks to flag a pending transaction and then follow up with the cardholder in real-time for further information about the transaction in question.

In the small business financing, AI also allows online small business lenders to analyze data to reduce underwriting time and thus accelerate credit decisions and the disbursement of capital. Additionally, AI allows financing companies to examine more

and different types of data, which enables the lender to better able to evaluate the health of small businesses and its ability to repay. This can lead to higher approval rates and lower default rates.

ETA believes regulatory focus of AI in the short term should be geared toward continuing to engage with industry and academic leaders to better understand this nascent technology and its potential benefits and risks. Premature or excessive regulation risks constraining innovation in AI and many of the benefits it provides to consumers, small businesses, and the economy.

ETA Feedback on Specific Proposals:

- 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.
    - AI should not be defined too broadly, otherwise many types of decision making could fall under the term. It should be clear that AI and AI programs are those which don't linearly analyze data in the way they were originally programmed. Instead, they learn from the data in order to respond intelligently to new data and adapt their outputs accordingly (see ICO Report). For example, it would not be desirable for any proposed definition of AI to have the potential for it to encompass decision trees or any other useful expert systems that produce outputs based on inputted data, but which do not learn independently from data in an intelligent way.
- 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.
    - Providing information regarding automated decision-making can, at times, be a practical impossibility due to the prevalence and nature of machine learning.
    - *Narrow* the scope of the requirements to disclose information regarding automated decision-making only in instances where bias can have a harmful impact on individuals (i.e., a legal or significant financial effect, such as a loan denied as a result of automated decision-making)
    - Or at least exempt decision making used to:
        - combat fraud and misuse of their services
        - comply with contractual obligations

- comply with the law
- comply with warrants, subpoenas, lawful law enforcement requests
- conduct other legitimate business purposes and provide services requested by the customer (such as payment processing, payroll, employment, loan offers that benefit the consumer, direct marketing to customers)
- defend or pursue litigation
- perform services and provide products
- process data that is lawfully made available to the general public
- secure their platform and respond to security incidents

- Proposal 4: Provide individuals with a right to explanation and increased transparency when they interact with, or are subject to, automated processing.
  - Overbroad transparency requirements can result in disclosure of trade secrets or other sensitive business information. This could also have a disparate impact on small businesses who rely on services by opening them up to undue competition.
  - The ICO acknowledges, in their recently published draft auditing framework guidance (link below), that it is not reasonable to assume a zero-tolerance approach to the risks imposed by AI systems. There needs to be flexibility to allow for organizations to balance risks, such as the trade-off between statistical accuracy and explainability of an AI system. As an example, the ICO explains that very complex 'black box' systems are difficult to explain in a transparent way, but the trade-off is that such complex systems may provide the most statistically accurate and effective outcomes for sophisticated applications. The algorithms relied on are likely to be proprietary and so accountability for the quality of the output of a machine's learning is a way of managing the risks of transparency. https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf
  - *Narrow* the scope of transparency requirements to information which would not reasonably cause competitive harm to organizations or consider an exception for that kind of information.
  - Transparency should be subject to exceptions, including when the automated processing is used to:
    - combat fraud and misuse of services

- comply with contractual obligations
- comply with the law
- comply with warrants, subpoenas, lawful law enforcement requests
- conduct other legitimate business purposes (such as payment processing, payroll, employment, loan offers that benefit the consumer, direct marketing to customers)
- defend or pursue litigation
- perform services and provide products
- process data that is lawfully made available to the general public
- secure the platform and respond to security incidents

- Proposal 7: Include in the law alternative grounds for processing and solutions to protect privacy when obtaining meaningful consent is not practicable.
    - Are there exemptions to consent? If not, propose that consumer consent should be required only where ***sensitive*** **data** is being used in ways that are *unreasonable* or *unexpected* in the context of the services provided.
    - In alignment with the European approach to consent in a privacy context, we agree that
      it is very difficult to obtain meaningful valid consent in AI applications, since the opaque nature of the algorithms make it difficult to clearly explain their underlying workings. Additionally, the nature of AI is that it the purposes can be ever evolving and may not be anticipated at the outset. Accordingly, it is imperative that other legal grounds are proposed, and that consent is not regarded as the default.
- Proposal 9: Require organizations to ensure data and algorithmic traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle.
    - Ensure this can be done in a way that isn't overly burdensome on companies and does not stifle innovation - limit the time and scope of recordkeeping is necessary (i.e., limit recordkeeping obligation to uses of AI that have a significant legal or financial impact, maybe a 3–5 year limit?)

- Proposal 10: Mandate demonstrable accountability for the development and implementation of AI processing. Demonstrable accountability would require organizations to be able to provide evidence of adherence with legal requirements on request. OPC proposes that the law also requires independent third-party auditing throughout the lifecycle of the AI system.
    - Ensure this can be done in a way that isn't overly burdensome on companies - limit the scope and time recordkeeping is necessary (maybe a 3–5 year limit?). Suggest that companies be able to choose their own auditors and that auditing is limited the AI process with a significant legal or financial impact.
- Proposal 11: Empower the OPC to issue binding orders and financial penalties to organizations for non-compliance with the law.
    - ETA supports enforcement by regulators, but we must ensure that there is no private right of action (none is proposed here, but to keep in mind).

Canada is uniquely positioned to help shape the future of AI and privacy and adopt best practices and market-led initiatives that can work within Canada's unique regulatory environment and market structure. Canada should carefully consider implementing a governance framework designed to drive specific market outcomes over a strictly rules-based approach. Organizations should be able to determine themselves the appropriate measures to address the risks posed by AI on the basis of broad principles rather than prescriptive rules.

In reaching our conclusion, we have reviewed the European Commission's White paper on AI which distinguishes high-risk AI applications from all other AI applications, and aims to apply the proposed new regime of regulation and conformity assessment only to the high-risk applications. According to the paper, high-risk AI applications are those used in a sector where "significant risks can be expected".

https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

* ** **

ETA thanks you for the opportunity to submit these comments.

Respectfully submitted,

ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

Scott Talbott

Senior Vice President of Government Affairs Electronic Transactions Association