

September 3, 2021

Manager of Access and Privacy Strategy and Policy Unit  
Ministry of Government and Consumer Services  
Enterprise Recordkeeping, Access, and Privacy Branch  
134 Ian Macdonald Blvd.  
Toronto, Ontario M7A 2C5

VIA E-MAIL: [access.privacy@ontario.ca](mailto:access.privacy@ontario.ca)

Re: Modernizing Privacy in Ontario - Empowering Ontarians and Enabling the Digital Economy

The Electronic Transactions Association (“**ETA**”) submits these comments in response to the Ministry of Government and Consumer Services’ (MCGS) whitepaper, “Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy”, and supplement ETA’s previous submission last fall. We hope that these comments will continue to assist the Government in understanding the key considerations of the payments industry with respect to privacy, data security, and innovation.

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA’s members include financial institutions, mobile payment service providers, 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 and its members support privacy protections designed to safeguard the personally identifiable information of Canadian individuals, and value the privacy protections that Canadian laws provide to protect the personal information of Canadian end users. Canada enjoys a robust, national framework under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This national approach, supported by industry, already provides a consistent and predictable framework that business must adhere to and is preferable over a patchwork of sub-national privacy regimes which create cumbersome compliance challenges for global payments technology providers. In the U.S., for example, privacy laws are on a state-by-state basis, creating a confusing and sometimes contradictory patchwork of laws which are challenging for consumers and businesses to comply with.

Prior to the federal election being called, this legislation was being modernized through the *Digital Charter Implementation Act* (DCIA), and it is expected that similar legislation will be introduced before Parliament later this year. ETA therefore once again encourages the Ontario government to commit to working at the Federal level to ensure that Canada’s Federal privacy framework is modernized in a way that meets its privacy reform goals.

Should Ontario proceed with its own legislative framework, ETA and its members are concerned by a few elements proposed in the whitepaper that are inconsistent with PIPEDA and other Canadian privacy regimes and which we would hope to see addressed in any final legislative framework. ETA addresses these concerns in the comments below.

### **Rights-based approach to privacy**

Safeguarding individuals' rights are a critical aspect of the Ministry's considerations. ETA believes that conformity across not only data protection principles but also established data protection regimes will be the most successful in achieving organizational compliance and provide for much needed clarity and certainty for individual consumers. Based on members' experience working with established privacy frameworks in other jurisdictions, ETA has several recommendations with respect to individual rights.

Regarding the proposed intent to enact a fair and appropriate purposes clause, ETA cautions that an overly narrow definition of what is deemed to be the fair and appropriate collection of information would have negative consequences for ETA members. The way in which personal information is used should be balanced against the risks to the individuals from the use of the data. Ontario privacy legislation should encourage organizations to take privacy protective measures and facilitate their ability to use data to innovate responsibly. De-identification of personal information is one such example of a privacy protective measure, and the resulting de-identified data should be excluded from the scope of personal information covered in an Ontario privacy legislation.

In the case of data from payment and payment systems, consumer data collected from financial transactions by members is used for services to protect Canada's banking system. They include products to detect and deter anti-money laundering activity and financial crimes. Collected data is aggregated and de-identified. Ensuring that this information can continue to be collected in a privacy enhanced way is critical to the integrity of the system, and ETA therefore recommends that Ontario's proposed privacy collection explicitly exempt from consent requirements data collected for fraud prevention and other mitigative activities of this nature.

Similarly, data insights and analytics that have been derived from personal information that do not identify the individual should also be excluded. Personal information should be considered de-identified where an organization has implemented technological, physical, legal, and administrative measures to reasonably prevent the risk of re-identification of the individual. In addition, Ontario legislation should provide incentives for companies to explore other privacy-enhancing technologies to protect data such as differential privacy, federated analysis and homomorphic encryption.

With respect to mobility, disposal, access and correction, ETA encourages government to adopt an approach consistent with updates to Canada's federal privacy regime and GDPR, that includes the same or similar instances in which an individual may make the request to be forgotten, in addition to the exceptions in which an organization would not erase the individual's personal information. For data portability as well, ETA once again encourages government to adopt an approach consistent with the GDPR. Namely, to provide individuals with their data "in a structured, commonly-used and machine-readable format." ETA believes that this language, in addition to providing this important individual right, also avoids being overly prescriptive in a manner that would be out-of-date with industry options, data storage and transmission. This alignment is essential to ensure interoperability between the two regimes and minimize compliance costs for organizations, many of which have already developed complex privacy compliance programs to comply with the high level of protections available under the GDPR.

## **Automated Decision Making**

While ETA and its members believe that the example provisions provided in this section offer adequate protection for Ontarians whose information is subject to ADS practices, we submit that there is still room for improvement. In particular, ETA submits that the Ontario government should revisit the definition of prohibited uses of ADS to make it fully interoperable with the GDPR. While the government intends to align the limitations on the use of ADS to those under the GDPR, in order for this to happen Ontario needs to ensure that a “decision that significantly affects” the individual is one that has legal effects or similar impact. Right now, the prohibited uses could be seen as going beyond those that under the GDPR are restricted to specific legal authorizations, which are also replicated in the white paper.

Regarding the regulatory approach for ADS, the safeguards discussed in the whitepaper could cause an overlap with the provisions on individuals because the right to access and right to correction are replicated under ADS. To maintain consistency and clarity, the provision should capture only those rights which are additional and specific to ADS, such as the request for explainability and human review, in addition to the right to comment and contest the decision. Going further, ETA submits there is no need for creating an additional layer of recordkeeping and traceability as this could result in confusion and excessive compliance costs. This is without prejudice of an organization’s obligation to comply with explainability requests.

When one considers the fast-evolving nature of technology and the varying definitions of AI, it is critical to determine what a workable scope of oversight can be. An appropriate scope would be to apply oversight to the more pressing public policy considerations relating to automated or algorithmic decision-making, irrespective of the technology used, which can harm individuals and their rights at scale by amplifying bias in ways which may be hard to detect.

This definition could spur a discussion of when it is appropriate to rely on machines for decision making compared to when it may not be appropriate, the degree of human oversight that should be involved, and that different technologies can cause similar potential impacts. This approach would be in line with, for instance, the approach taken by the European Union’s General Data Protection Regulation (GDPR), which includes the right for individuals not to be subject to a “decision based solely on automated processing [...] which produces legal effects concerning him or her or similarly significantly affects him or her.” This would allow for a more technology-neutral approach to the protection of personal data, consistent with the way the PIPEDA has successfully adapted and applied to evolving technologies.

Further, supporting the inclusion of human review over automated processing of personal information can serve as a powerful risk mitigant. While it is true that human-based decision making is not 100% free of biases and prejudices, humans do possess the ability to learn, to recognize their own biases and to improve their decision making over time. When complimented by strong internal governance processes and controls, these checks and balances serve to counteract potential harm to individuals.

It is critical to support safe, responsible use of technologies such as AI. AI objectively extracts correlations, classifications, and other predictive techniques based solely on the data on which it is trained. As such, the use of AI for decision making may cause harm to individuals on a much larger scale and in ways that are harder to detect than in other approaches to decision making if they are not checked along the way.

Finally, for the purposes of legal oversight, the definition needs to be considered in the context of the specific concerns that are to be addressed. Should the government decide to create a right in the law to allow individuals to object to automated decision-making and not to be subject to decisions based solely on automated processing, they must ensure that right is subject to certain exceptions.

GDPR contemplates the right to object to automated decision-making (ADM) under Article 21 and the right not to be subject to it under Article 22. It should, however, be highlighted that the right for an individual not to be subject to automated decision-making under GDPR is not absolute. It applies to those forms of decision-making based solely on automated processing that “produce legal effects concerning him or her or similarly significantly affect him or her”. Furthermore, the right not to be subject to automated decision-making under GDPR does not apply in the event an automated decision is necessary for performance of a contract; authorized by law; or when explicit consent is obtained. In the event automated decision-making is based on necessity for a contract or upon explicit consent, individuals may obtain human intervention, express their point of view and contest the decision. We believe if a similar right not to be subject to automated decision-making were to be included in Ontario’s privacy law, it should be coupled with similar parameters.

Moreover, the right to object under Article 21 of GDPR is not limited to automated decision-making but entails a broader right for individuals to object to the processing of their personal data carried out on the basis of legitimate interests or on the basis of a task carried out in the public interest or official authority.

The proposed right to prohibit use of automated decisions should be carefully defined. As with sector- and use-case-specific carveouts in the draft federal DCIA, sector specific legislation or regulation (e.g., credit and health care decisions) are far better placed to manage the specific due diligence to be taken in all aspects of decisions with significant impacts on individuals and the appropriate obligations to impose on organizations, and rights of recourse and redress to individuals than the currently blanket option proposed here under privacy law. In such event, to continue the processing, companies can demonstrate that there is a compelling reason for the processing overriding the individual’s interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

Finally, there are limitations to explainability. Data and factors used can be explained, though not necessarily the exact measures or evaluations for their precise decision, allowing for a reasonable balance between protection of intellectual property rights and meaningful transparency to individuals.

ETA and its members believe the protections and limitations envisioned in the white paper offer a high level of protection while staying interoperable with the DCIA, the GDPR and other longstanding privacy laws. Additional requirements could upset that balance and create compliance issues for organizations present in Ontario without clear privacy gains for Ontarians.

### **Consent Provisions**

ETA supports the requirement to receive explicit consent for collecting sensitive personal data. However, ETA believes that there are a few practical limitations that arise when gaining explicit consent. There are times when collecting explicit consent isn’t a reliable form of *informed* consent,

most notably, when there is an imbalance of power between parties, interacting with vulnerable people/groups, or where obtaining consent is simply not feasible. In such cases, organizations should still be able to collect, use, or disclose personal information based on other legal grounds which provide for equally robust privacy protections. For this reason, ETA submits there should be additional legal basis for processing personal information.

ETA also believes the best outcome for citizens would be one unified, national standard that allows ETA members to offer citizens the same products and services in all regions of Canada, while offering robust consumer privacy protections to individuals irrespective of the jurisdiction in which they reside. ETA also cautions that an overly restrictive or complicated approach to consent could restrict the ability of members to offer new products and services to consumers. While we understand that at times processing consumer data, for legitimate reasons, is crucial to the success of these new products and services, ETA supports an approach that provides citizens the ability to restrict how their data is used; the critical point is that consumers must have *choice and control* over how their data is used and shared. The flexible, principles-based approach under PIPEDA is very balanced and supports far more appropriate and responsible levels of data collection and use where more implicit levels of consent are appropriate to use. For example, as applied to limited data to use a limited service, or where consent cannot be obtained (e.g., in the public realm). It actually incents the right behavior by data collectors to limit data and use and gives individuals a better, less confusing user experience.

### **Data Transparency**

The government intends to implement a requirement for organizations to develop a privacy management program, which would govern the collection, use and disclosure of personal information that is collected. ETA and its members welcome this requirement and believe that it is sufficient in ensuring that organizations are held accountable for the personal information they collect. Nevertheless, ETA submits that the Ontario government must prioritize alignment with the federal government's approach to avoid conflicting requirements within Canada or additional requirements that would apply only for Ontario and therefore create a complex compliance environment.

Further, various ETA members have implemented Privacy by Design and Security by Design approaches and embedded these principles in the core of their businesses. The GDPR's support of corporate accountability, and the use of tools such as Privacy by Design, has been a positive feature for companies interested in demonstrating data responsibility and respect for individual rights. By encouraging companies to adopt these approaches, individuals can feel more secure in giving their consent. However, prescribing the specifics of what a Privacy by Design regime looks like may result in an outcome that is one-size-fits-all, and not adaptive to industry, nature, complexity and scope of data use, and impact on individuals, making it less effective and adaptive to changes to the environment in future.

### **A Principles-Based Approach**

ETA is dedicated to continuously driving innovation in the payment space and values the importance of a Canadian financial ecosystem whose participants ensure that individuals and businesses are provided with financial products and services that are convenient, secure, and reliable. Access to financial data and information is an important issue that involves individuals, traditional financial institutions, financial technology companies (FinTechs) and other financial service providers, including data aggregators and third-party application providers. The Canadian

ecosystem also consists of multiple stakeholders, each with differing roles within data aggregation.

ETA and its members recognize the increased convergence between these groups and the need to preserve consumer access, choice, and control. To preserve market dynamism, ETA strongly encourages government to be sensitive to the risk of applying a prescriptive regulatory framework. ETA and its members support an industry-led and principles-based framework for open data access that facilitates collaboration, promotes innovation and competition among all industry participants in the financial data marketplace, that permits consent-based sharing and use of financial data, and that is protective of consumer interests.

Among the principles that should guide the government's direction, includes avoiding duplication and overlap with existing government or industry requirements, including those being considered at the federal level through the *Digital Charter Modernization Act*. Rather than issue prescriptive requirements, the Ministry should encourage industry to take the lead in developing solutions that preserve industry flexibility to continue to develop new and innovative products and services that benefits individuals while providing appropriate privacy protections. In this regard, the financial services industry, including ETA member FinTech companies, have demonstrated a robust and sustained commitment to ensuring consumer access to information, the protection of customer information, and the integrity of financial systems and networks.

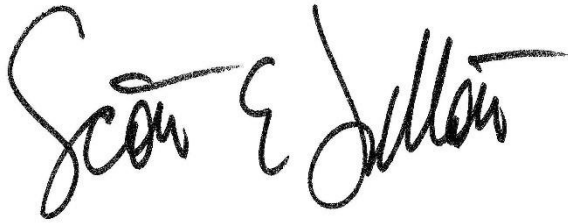
Specifically, ETA believes that industry solutions that consider the unique circumstances of the parties and the functionalities being contemplated will be more effective in addressing the risks and opportunities being presented. It is important to recognize that this is a highly dynamic space where players, technologies, and services offered may differ widely and present different or evolving risks. A one-size fits-all regulatory approach or solution will not keep pace with the dynamic nature of this space and will stifle innovation. The ETA therefore recommends the adoption of a technology neutral and principles-based legislative approach.

### **Conclusion**

In sum, as technology and innovation are constantly evolving and continue to shape how information is created, accessed, stored, and disposed of, regulations that are consistent with established data protection frameworks, such as the GDPR, and have a principles-based approach best enable innovation and compliance, while protecting individuals' rights to privacy. ETA therefore encourages the Government of Ontario to work closely with the Government of Canada to align the outcomes of both jurisdictions' privacy modernization efforts to ensure the two are compatible.

ETA would be pleased to discuss the comments herein with the Government of Ontario to ensure the perspective of the payments industry is well understood. ETA thanks you for the opportunity to submit these comments.

Yours respectfully,



Scott Talbot  
Senior Vice President  
Electronic Transactions Association