November 3, 2021

Diane Poitras
President
Quebec Information Access Commission
2045 Stanley Street, Suite 900
Montreal (Quebec), H3A 2V4

Madame President,

Object: Request for additional information regarding Bill 64

I am writing on behalf of the Electronic Transactions Association ("ETA") to obtain more information and clarity on Bill 64 (*An Act to modernize legislative provisions as regards the protection of personal information*), and how various new obligations may apply to our member companies.

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.

The Association has been following the adoption process of Bill 64 to gain a better understanding of the changes made by the Quebec government and the impacts of these changes on the operations of our member companies in Quebec, Canada and internationally. We would like to thank the Quebec government and parliamentarians for their approach and addressing concerns raised by ETA and its members. This approach led to the adoption of sensible amendments, including the ability for organizations to use certain information in the course of their business and for the benefit of consumers (section 102) to fight fraud.

However, some of the amendments adopted still leave important questions unanswered, and we would welcome clarifications to gain a better understanding of how the Bill will impact our members and the services that they provide virtually every minute to Quebecers and consumers around the world.

We understand based on the feedback we have received from the government that you may be developing guidelines to help with the interpretation and the understanding of the new measures that will come into force following the adoption of this Bill. In this context, and to provide industry feedback and guidance in the potential development of future regulation, we would welcome further clarification on the following elements:

a) Cross-border data transfer and adequate protection (section 103)

This section provides that "the information may be communicated if the assessment establishes that it would receive adequate protection to that afforded under this Act." The notion of equivalency has been replaced by the concept of adequacy. Our members would like to know what this term means specifically, if it is intended to be different than equivalent, and how it correlates with the possibility of a contractual protection added to section 70.1(3).

In cases where such an assessment would be required, what would be considered adequate is unclear, and so is the frequency at which the adequacy assessments should be conducted. Would they need to be conducted for every new piece of personal information that is communicated outside of Quebec? And what would be the obligations when the law in the foreign jurisdiction is amended? Does a new adequacy assessment need to be conducted for material amendments? If so, within what timeframe?

Recommendations (section 103)

⇒ To limit the burden on organizations, especially SMEs, we believe that Quebec should establish alternative transfer mechanisms that do not require assessments, such as standard contractual clauses and binding corporate rules.

⇒ We believe that the obligation to conduct an assessment should be limited to “high risk” cross-border data transfers, such as those involving a large volume of sensitive information.

⇒ We believe that businesses should be able to define “generally accepted data protection principles” based on a non-exhaustive and flexible list of considerations, which could include the foreign legal system’s similarity to Quebec’s legal system, the rule of law in the foreign country, the availability of effective and enforceable remedies, and the foreign country’s adherence to international privacy legal frameworks.

⇒ Additionally, and in accordance with the United States – Mexico – Canada Agreement (USMCA), we believe that all data transfers to US jurisdictions should be considered de facto adequate. The Quebec government should clarify that the same applies to transfers to and within all other Canadian provinces.

⇒ Our understanding from discussions during your consultation process was that a separate « adequacy assessment » was not required for each piece of personal information transferred. It would be very helpful for this to be clarified/confirmed in the guidelines and regulations.

<u>b) Consent must be clear, free, informed and given for specific purposes (section 102)</u>

The bill provides that consent must be requested for each purpose for use of personal information, in clear and simple language and separately from any other information provided to the person concerned. Some of our members offer services or work with service providers that are not directly involved with the customer, but that that are essential, such as protecting privacy and security. What would be the nature and level of consent required in such cases? We believe that any new measure should not become an obstacle for offering these indirect services that are essential in the ecosystem. Furthermore, it is not practical nor desirable for customers to receive pop-ups requesting separate consent for each type of personal information collected. This approach would be unique to Quebec, and raise several issues for companies, including extensive technical development.

It is our understanding that the second sentence in section 14 suggests that consent cannot be requested as part of a privacy policy. In this respect, how is a clear and simple privacy policy considered by this section? In addition, how is implied consent taken into account by section 14?

Section 102 provides an explicit carve out from express consent necessary for the prevention or detection of fraud. Other jurisdictions, including GDPR and US state-level privacy law in California, allow an entity to deny an individual's data request based on a fraud exemption. For example, if an entity (e.g. a payment network) needs to retain an individual's data to fight fraud, under the previously referenced laws, they do not have to fulfill a request to delete the data that falls under the exemption. This particular fraud exemption allows the entity to have more robust fraud prevention capabilities and aids in reducing fraud-related revenue losses and operational expenses.

Recommendation (section 102)

⇒ *We believe that if privacy policies are clear and simple, they are ideal vehicles to ensure customers understand how the company proposes to collect, use, and disclose their information.*

⇒ Guidance should extend the fraud prevention exemption to allow an entity to deny an individual's data access or correction request where necessary to maintain a high standard of fraud prevention.

c) Criminal and administrative penalties (section 150).

The accumulation of penalties between jurisdictions in the event of a security incident was not addressed in detail by the committee during the clause-by-clause review. Could a company be sanctioned more than once for the same incident in several different jurisdictions?

Recommendation (section 150)

⇒ *We believe that clear mechanisms need to be implemented to avoid sanctions for the same offense in different jurisdictions, which could yield disproportionate outcomes and inapplicable sanctions.*

d) Highest level of confidentiality (section 100).

This section ostensibly requires a "default to off" approach for almost any product or service that involves data processing, irrespective of context, users' reasonable expectations, or the purposes for which the underlying product or service is being offered to the public. Although this is privacy by design, the Bill does not contain any specifics or proportionality principles. During the clause-by-clause review, this concept was not discussed in sufficient detail. Additional information to help understand the scope of this obligation would be helpful.

Recommendation (section 100)

⇒ *We believe that businesses should have the flexibility to consider certain criteria when determining what constitutes "the highest level of confidentiality," and the criteria should*

include the commercial and contextual circumstances, including reasonable expectations of individuals using the product or service. It may not always be appropriate or required to meet the "highest level of confidentiality" which could result in extreme and expensive measures which are not required in the circumstances.

e) Identification technology (section 99).

The bill creates an obligation to "inform" individuals of the use of technology that identifies, locates, or recognizes them, and the means to activate those functions. We would welcome further clarification on what constitutes "informing" an individual and what the exceptions to this obligation might be. To the extent that this provision is intended to focus on cookies and pixels, it would be useful to know the exact technology contemplated and the expectations surrounding that technology. In addition, the change to this section that requires companies to inform the individual of the means available to activate the identification, location, or profiling features instead of informing the individual of how to deactivate these features raises several questions, the most fundamental of which is how does this change apply in practice to the existing technologies that are used by our members and that are essential to their operations.

Recommendations (section 99)

⇒ *We believe that disclosure in a Privacy Notice is sufficient to inform individuals of identification technology.*

⇒ *We believe that activities related to fraud prevention and risk management, for instance, should not be negatively impacted by changes related to the activation or deactivation of certain functions.*

⇒ *We believe that organizations should be allowed to inform individuals that by using a product or service, they will activate identification technology.*

f) Automated Decision-Making (section 102)

Section 102 of the Bill requires organizations relying on automated means to make "decisions" to provide individuals with an explanation of the "reasons and principal factors and parameters" that led to such decisions. This requirement is overbroad in that it will require organizations to inform individuals of automated decisions that are unlikely to have significant consequences, leading to notification fatigue without promoting the privacy interests of the individual. Further, the level of detail required will at time be challenging to provide without revealing sensitive or proprietary information about the algorithm itself.

Recommendations (section 102)

⇒ *We believe that guidance should identify the acceptable content, format and procedure for the explanation required by Section 102.*

⇒ *We believe that the automated decisions referred to in section 102 should be limited to those that are likely to significantly affect an individual.*

⇒ *Clarification is required in terms of how this will apply in real life/who has accountability where a service provider is making a decision (e.g. fraud propensity) and has no direct relationship or personal information of the end user/card holder.*

g) Other (general comments)

Finally, we believe that the government should clarify how it expects each amended or new provision in the Private Sector Act to be practically implemented by businesses that are subject to the law. Specifically, what changes to existing practices, if any, will businesses be required to undertake to achieve compliance with the law – especially small and medium enterprises (SMEs) that often operate with limited resources. According to IAPP and Ernst & Young, businesses had to spend on average $1.8M to comply with the GDPR in 2018.

We thank you for your attention and consideration, and given the importance of this bill for all businesses operating in Quebec and to Quebecers, the ETA would be grateful for any clarification and details to assist our members as they will work diligently to comply with their new obligations.

We remain at your disposal for any questions you may have.

Yours respectfully,

Scott Talbott
Senior Vice President
Electronic Transactions Association