Feedback to the Government of Quebec on proposed amendments to Quebec's private sector privacy law (Bill 64)

September 29, 2020

Executive Summary

As the voice of the marketing profession, the Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Government of Quebec on Bill 64's proposed amendments to Quebec's Act respecting the protection of personal information in the private sector.

In our modern digital economy, consumers increasingly expect organizations to deliver the intuitive products and services they want and need. Quebec's privacy law, now and into the future, must embrace the enormous social and economic benefits of data use for Quebecers while protecting their privacy. There must be a mechanism for Quebec's alignment on privacy reform initiatives underway across the country to avoid unnecessary complexity for consumers and business, and to prevent complications for interprovincial and international trade, and foreign direct investment in Quebec.

As the National Assembly considers the provisions of Bill 64, the CMA is pleased to provide the following recommendations:

1. Quebec's privacy law must be flexible, technology-neutral and proportionate to the privacy objectives to be achieved. Quebec's privacy law should be based on principles that are flexible in the face of rapidly evolving technologies, business models and consumer privacy expectations. It should be commensurate to the privacy goals at hand, without creating undue complexity for consumers, businesses and government.

2. There must be a mechanism for alignment with other privacy frameworks across Canada to prevent undue complexity for businesses and consumers, and barriers to trade and foreign investment in Quebec. In particular, there should be reasonable alignment with anticipated reforms to the federal Personal Information Protection and Electronic Documents Act (PIPEDA), as significant differences between the two laws will negatively impact Quebec's businesses and citizens.

3. Requirements for cross-border data transfers must include proven, workable alternatives to adequacy, such as standard contractual clauses.

4. **Accountability for outsourcing should be placed on the principal organization**, mandating service providers to follow the requirements set out by the principal organization.

5. The type of consent required must be based on an assessment of relevant factors, reserving express consent for when it is truly meaningful. The law should recognize the important role that implied consent plays in serving consumers and business.Alternatively the law could provide for express consent for "legitimate purposes", enabling organizations to justify their legitimate purposes through internal assessments, and identify them to individuals.

6. Enforcement measures should be reviewed and reduced to incentivize compliance without having a chilling impact on business and investment in Quebec. In particular, the application of fines must be based on specific factors using a proportionate approach that considers the nature of the violation, and the size and data processing activities of the organization that committed the violation.

7. Reasonable transparency should be required around profiling and decisions based on solely automated processing. Regulatory responses should be remedial, prohibiting or restricting only those activities where there is clear evidence of harm.

8. The consent exception for de-identified information should be broadened, provided certain standards for de-identification are met. The Act should further permit the collection, use and disclosure of de-identified information without consent for all reasonable purposes, if certain standards are developed and met.

9. Self-regulatory measures should be encouraged and incentivized to ensure regulatory efficiency. Voluntary codes, certifications and other standards (such as the Canadian Marketing Code of Ethics and Standards) play an important role in supplementing privacy legislation. The government should **e**ncourage self-regulated certifications and codes as tools for privacy compliance and accountability, and should further incentivize their use by selecting some for formal recognition.

10. The right to data portability should be postponed until its wider impacts are understood. Data portability creates serious new risks related to fraud, privacy and security, and its wider impacts on the economy and competition are not well-understood**.** It should only be achieved through a phased-in approach that allows for the implementation of sector-specific frameworks.

Introduction and Context

The Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Government of Quebec on Bill 64's proposed amendments to Quebec's Act respecting the protection of personal information in the private sector.

The CMA is the voice of the marketing profession, representing more than 50 corporate, not-for-profit, public, and post-secondary members across Quebec. We are committed to helping organizations maintain high standards of conduct and transparency through our mandatory Canadian Marketing Code of Ethics and Standards, and our privacy and data protection resources for marketers and consumers. As the recognized and longstanding leader in marketing self-regulation, we strive to ensure an environment where consumers are protected and businesses can thrive.

Quebec's marketing community highly values its customers, whose loyalty and trust provides the foundation for business success. Most organizations recognize that strong privacy and data protection practices serve as a competitive advantage and customer retention strategy, and they work hard to protect the privacy interests of the individuals they serve. Government and industry collaboration is essential to ensure Quebec's privacy framework is based on a balance between embracing the enormous social and economic benefits of data use while protecting the privacy of individuals.

Quebec was the first North American jurisdiction to enact privacy legislation governing commercial activities. The modernization of Quebec's privacy law is an important step to ensure that Quebec continues to be a champion of privacy protection, striking a balance between consumers' privacy expectations and leveraging data to support economic growth and innovation. We appreciate current reform efforts underway by the National Assembly, and believe Quebec has a significant opportunity to pursue a solution that is practical for both consumers and businesses.

Alignment with other privacy frameworks across Canada is critical to ensuring the success of organizations operating in Quebec, for the betterment of Quebec citizens who value the range of products and services that are available to them. There must be a mechanism for alignment on privacy reform initiatives underway across the country to ensure businesses can operate seamlessly across international and provincial borders, and to ensure Quebec remains an attractive foreign direct investment destination. If these approaches are not aligned, it will create a patchwork of privacy legislation, resulting in unnecessary complexity and barriers for businesses, and disruptions for consumers. It will also reduce Quebec's attractiveness as a business destination for companies in other countries and provinces, negatively impacting Quebec's economy and consumer choice.

The marketing community supports many improvements proposed in Bill 64, including new consent exceptions for research and sale of business transactions, and an exclusion of business contact information from the definition of personal information. Other areas of the Bill require a closer look by the National Assembly to ensure Quebec's privacy framework achieves its dual goal of protecting consumers while supporting responsible innovation and competitiveness, and to avoid the issues that have arisen in jurisdictions governed by more prescriptive, EU-inspired data protection laws.

As the National Assembly considers the provisions laid out in Bill 64, the CMA is pleased to provide the following recommendations:

Recommendations

1. Quebec's privacy law must be flexible, technology-neutral and proportionate to the privacy objectives to be achieved

Data underpins the digital economy. It informs better decision-making and enables the development of important new technologies, like artificial intelligence (AI), for which Quebec is a world leader.

The ability of organizations to collect, use and disclose personal information is key to providing value to consumers, and to ensuring Quebec's innovation and competitiveness. It is important that Quebec's privacy law remain adaptive to a changing business environment and function within operational realities and context-specific risks. This is especially important for Small and Medium Enterprises (SMEs) so that compliance is not unduly onerous.

Quebec's privacy law must be based on principles that can be thoughtfully applied to all technologies and business models, in order for it to remain relevant. Bill 64 takes an important step away from static and outdated concepts such as "files". A further review of the law should ensure there are no remaining technology-specific provisions that would not stand the test of time.

It is also important that the law provide for the evolving expectations and preferences of consumers**,** without the need to repeatedly introduce legislative amendments to keep up with the times.

Technological advancements have provided organizations with the agility to offer relevant, useful offerings to consumers. As a result, consumers demand much greater speed and quality of information than ever before to use services provided by companies, and to make informed purchase decisions. A strong majority of consumers (76%) are willing to share personal data in order to receive benefits, as long as the data is properly protected[1]. Many consumers, including younger generations, recognize that data exchange is increasingly fundamental to accessing many of the beneficial services they interact with daily.

Quebec's privacy law should be commensurate to the privacy goals at hand, without creating undue complexity for government, business and consumers. Privacy law should be based on sound principles that allow organizations to account for context. The law should be flexible enough to impose measures proportionate to the privacy interests involved and the individual's reasonable expectation of privacy in the circumstances.

A reformed law should include a new purpose clause requiring the law be interpreted in a proportionate manner, reasonable to the circumstances. We recommend the following changes to the Act:

> *The object of this Act is to establish, for the exercise of the rights conferred by articles 35 to 40 of the Civil Code concerning the protection of personal information, particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code.*
>
> *Those particular rules are to be applied in a manner that recognizes the right of privacy of individuals under the Civil Code and the need of organizations to collect, hold, use or communicate personal information for purposes that a reasonable person would consider appropriate in the circumstances.*

[1] Foresight Factory, 2018: Data Privacy Study: What the Canadian Consumer Really Thinks

2. There must be a mechanism for alignment with other privacy frameworks across Canada to prevent undue complexity for businesses and consumers, and barriers to trade and foreign investment in Quebec.

Privacy reform initiatives underway across the country must be consistent to ensure that businesses can operate seamlessly across international and provincial borders, in addition to enabling Quebec to remain an attractive destination for direct foreign investment. If these approaches are not aligned, it will create unnecessary complexity and barriers for businesses, disrupting the services and innovative technologies consumers want and need. There must be a mechanism for alignment between the federal, provincial and territorial governments in order to prevent the damaging fragmentation of privacy frameworks, including the negative impacts of interprovincial trade barriers.

In particular, it is critical for the National Assembly to ensure reasonable alignment with anticipated reforms to the federal Personal Information Protection and Electronic Documents Act (PIPEDA), as significant differences between the two laws will cause complexity for businesses, consumers and government.

Quebec's privacy law should be compatible with jurisdictions that have a similar, principles-based approach to privacy. It is more important than ever for the law to be nimble in the face of rapidly evolving technologies and business models, allowing organizations to determine the most effective way to meet their common obligations. The nuances – the respect for context, individuals' expectations and overall emphasis on reasonableness, should remain.

Many features of existing Canadian privacy laws, although due for a thoughtful upgrade, have stood the test of time, providing privacy protection without unnecessary regulatory burden. Newer and more prescriptive laws in other jurisdictions, including the GDPR, remain unproven in many respects, and have created a staggering regulatory burden for both government and business. A privacy framework should not be so onerous that it cannot be effectively implemented and is not well understood by non-specialists.

With regards to GDPR adequacy status, reducing friction in data transfers is a worthwhile objective. However, in considering the adoption of certain aspects of GDPR, we urge the National Assembly to evaluate each based on its merit in the Quebec context, with the goal being compatible privacy outcomes as opposed to compatible legislative requirements. If Canadian privacy frameworks are more aligned, it would support a positive decision on GDPR adequacy status that would apply more comprehensively across Canada's jurisdictions, making it easier for Quebec businesses to trade and compete.

3. Requirements for cross-border data transfers must include proven, workable alternatives to adequacy

In today's interconnected world, the efficient and reliable outsourcing of data processing operations outside of Quebec is crucial to the functioning of Quebec's businesses and their ability to serve consumers well.

Bill 64 proposes considerable restrictions on organizations seeking to share information with third parties located outside of Quebec, complicating conditions for business efficiency, growth and trade.

Under this provision, Quebec companies can transfer personal information only to those "States" whose legal frameworks have privacy protections equivalent to Quebec's, as part of a comprehensive privacy impact assessment. This provision is concerning in several significant respects:

- The requirement for equivalency would create significant difficulties for Quebec companies, particularly SMEs, as they compete in the global economy. Companies will face undue complexity, delays and costs as they carry out individual assessments for every jurisdiction to which they may transfer personal information. The concerns raised following the recent "Shrems II" decision in Europe, mandating that every cross-border data transfer be assessed on a case-by-case basis, underscore the impracticality of this approach.

- Quebec-based organizations, including multinationals, may decide to scale back or alter their operations to the detriment of Quebec's economy, healthy competition and consumer choice.At present, the Bill does not clarify whether a "State" would include other provinces, which would create even more complexity for Quebec businesses, as well as the consumers they serve across Canada.

- The ongoing determination and review of the adequacy status of other jurisdictions will require significant attention and resources by the provincial government, as we have seen under the EU's GDPR.

- The adequacy requirement risks violating the provisions in important trade agreements with regards to cross-border data flows, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Canada-United States-Mexico Agreement (CUSMA). The absence of an alternative to equivalency could be interpreted as unduly restricting the movement of data for a business purpose contrary to CPTPP Article 14.11 and CUSMA Article 19.11. The equivalency requirement may also be a de facto requirement for companies to maintain computing facilities within Quebec as a condition of doing business and may violate Article 14.13 and 19.12 of the CPTPP and CUSMA, respectively.

We urge the government not to maintain the adequacy requirement. If the adequacy requirement is retained despite the obstacles it creates, there must be alternative mechanisms in place for the transfer of personal information to jurisdictions that are not deemed equivalent. As we have learned from the experience of other jurisdictions, there are well-established and legally enforceable alternative mechanisms available.

The GDPR, for example, is far more flexible and provides for various lawful bases other than adequacy for data transfers to other States, including for contractual necessity, or if standard contractual clauses, codes of conduct, or binding corporate rules are in place.

Given the nature of data flows, current contractual obligations between organizations are an effective form of responsible data governance. If standardized contractual clauses are considered, they must allow for some flexibility to account for the varying nature and scope of the organizations and activities involved.

Finally, the Act must clarify when its provisions have extra-territorial effect. It should clearly state that its provisions apply within the province of Quebec and only apply to entities or activities outside of Quebec where there is a "real and substantial connection" to the jurisdiction, similar to the requirement under PIPEDA.

We recommend the following changes to the Act:

> *17. Before communicating personal information outside Québec, a person carrying on an enterprise must conduct an assessment of privacy-related factors ~~must~~, in particular: ~~take into account~~*
> *(1) the sensitivity of the information;*
> *(2) the purposes for which it is to be used; and*
> *(3) the protection measures that would apply to it, including contractual measures.; ~~and~~*

~~(4) the legal framework applicable in the State in which the information would be communicated, including the legal framework's degree of equivalency with the personal information protection principles applicable in Québec~~.

The information may be communicated if the assessment establishes that it would receive a comparable level of protection through legislative, contractual or other measures ~~equivalent~~ to that afforded under this Act. ~~The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment.~~

The same applies where the person carrying on an enterprise entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on its behalf.

This section does not apply to a communication of information under subparagraph 7 of the first paragraph of section 18.

~~17.1. The Minister shall publish in the Gazette officielle du Québec a list of States whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Québec.~~

4. Accountability for outsourcing should be placed on the principal organization

We support Bill 64's framework for sharing personal information with service providers in the context of outsourcing relationships. It represents best practice by not requiring additional consent.

To ensure a clear and consistent accountability chain, it is important that the Act clarify that the principal organization (i.e. "a person carrying out an enterprise") is solely responsible for ensuring compliance with privacy law, while the role of the service provider (i.e. "a person or body carrying out a mandate or performing a contract of enterprise or for services") is to follow the requirements set out by the principal organization.

Service providers have a responsibility for protecting personal information adequately, and these responsibilities are generally defined in the contract. Since the principal organization is the ultimate decision-maker when hiring a provider to provide a service, it makes senses that the principal organization remains solely responsible for complying with the Act.

We recommend the following change to the Act:

> *18.3(3) For the purpose of this Act, a person or body carrying out a mandate or performing a contract of enterprise or for services on behalf of a person carrying out an enterprise is not deemed to be a person carrying out an enterprise.*

5. The type of consent required must be based on an assessment of relevant factors, reserving express consent for when it is truly meaningful

An overreliance on express consent has contributed to "consent fatigue" for consumers, causing individuals to be less likely to carefully review privacy notices, make informed decisions and exercise choices. It is ill-suited to the realities of commercial enterprises, to the increasingly connected world in which consumers live and to evolving consumer expectations.

Requesting express consent, tracking consent and keeping records of consent for reasonable and standard data uses is overly burdensome for businesses, without a corresponding privacy protection benefit, and often results in poor customer experience.

It is imperative that the requirement for express consent be reserved for the things that matter most; for situations that may not reasonably be expected, and where individuals have a meaningful choice.

Bill 64 introduces several improvements to the consent model. The marketing community strongly supports the proposed exceptions to the consent requirement for:

- transferring personal information to an agent for processing,
- secondary uses and enterprise analytics where the use is consistent with the original consent,
- when the use is clearly in the individual's best interest, and
- in the case of a business transaction.

We also support the exclusion of business contact information from the definition of personal information that will trigger the consent obligation.

However, the current language around consent in Bill 64 is unclear. The Bill appears to require consent in almost all circumstances where personal information is used or transferred to a third party as a result of ss. 12 and 13. Consent must be express when it involves sensitive personal information, which seems to imply that another form of consent may be acceptable in some circumstances involving non-sensitive information.

The Bill states that consent must be clear, free, informed, "given for specific purposes and must be requested for each such purpose", in clear and simple language and "separately from any other information provided to the person concerned". These requirements are disproportionate in many circumstances, and inconsistent with the important role played by implied consent. Furthermore, it is unclear whether "separately from any other information provided to the person concerned" means outside the scope of a privacy policy.

Bill 64 does not currently refer to the concepts of express and implied consent, in contrast to other privacy laws across Canada, which authorize implied consent under certain circumstances. The proposal to separate consent for each purpose from other terms significantly departs from other privacy regimes. The Act should be amended to recognize the importance of implied consent, and should clarify that implied consent is sufficient where it is reasonable in the circumstances.

A longstanding strength of Canadian privacy frameworks is that organizations have the operational choice of whether to seek express or implicit consent. This ensures the appropriate form of consent is dependant on an assessment of the sensitivity of the information and the reasonable expectations of the individual, both of which will depend on context.

In general, express consent (e.g. opt-in) should be used for a collection, use or disclosure that generally involves sensitive information, is outside the reasonable expectations of the individual, or creates a meaningful risk of significant harm. Implied consent (e.g. opt-out) should be used for a collection, use or disclosure which generally involves non-sensitive information and straightforward purpose(s).

We urge Quebec to adopt the same framework for implied consent that the federal government and other provinces rely on, as outlined in the Office of the Privacy Commissioner of Canada's Guidelines for Obtaining Meaningful Consent.

We recommend the following changes to the Act:

> *14. When explicit consent is appropriate under this Act, such consent must be clear, free and informed ~~and be given for specific purposes~~. It must be requested ~~for each such purpose,~~ in clear and simple language ~~and separately from any other information provided to the person concerned~~. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested.*
>
> *The consent of a minor under 14 years of age is given by the person having parental authority.*
> .
> *The consent of a minor 14 years of age or over is given by the minor or by the person having parental authority.*
>
> ~~*Consent is valid only for the time necessary to achieve the purposes for which it was requested. Consent not given in accordance with this Act is without effect.*~~

The National Assembly should also incorporate additional alternatives to express consent (e.g. an exemption to consent for "legitimate purposes"). Express consent should not be required in situations where it is not meaningful or appropriate, such as in the case of personal information being used by organizations for legitimate purposes that take into account the reasonable expectations of the individual under the circumstances.

Organizations relying on this exemption must be transparent about their legitimate purposes, explicitly specifying them in advance and outlining them in a privacy policy or other method that is readily available to individuals.

The Act could allow for the formation of Regulations to specify allowable legitimate purposes or classes of legitimate purposes and to specify what information needs to be explicitly specified by organizations before the information is used.

It is reasonable to expect organizations relying on this exemption to justify their legitimate purposes and outline them clearly in their privacy policies and through the performance of internal assessments. The assessment would need to be based on the specific context and circumstances to demonstrate that processing is appropriate and reasonable.

6. Enforcement measures must be reviewed and reduced to incentivize compliance without having a chilling impact on business and investment in Quebec

The vast majority of Quebec organizations want to protect the privacy of their customers. They do not want to damage their reputations and jeopardize consumer trust by misusing or mistreating personal information. We support enhanced enforcement measures to provide effective recourse for individuals and to crack down on bad actors. However, it is critical that these measures not have a chilling effect on businesses and their ability to serve consumers well.

Bill 64 proposes new enforcement measures that are disproportionate to the privacy goals to be achieved and lack sufficient procedural safeguards. Penalties must provide sufficient incentive to deter businesses that might not otherwise comply, and must also be designed to avoid a costly and litigious environment, when reduced penalties could be just as effective.

If unduly strict enforcement measures are put in place, some organizations will find it necessary to assess the risks, costs and benefits of continuing to do business in Quebec. The measures in Bill 64

must be modified to ensure a reasonable approach to enforcement, with a level of liability that incentivizes compliance while fostering a collaborative and trusting privacy landscape.

The use of a percentage of worldwide turnover to calculate possible fines[2] is not advisable, and if this approach is set in place, it is important to reduce the maximum amount to a more reasonable and proportionate level. The proposed range for fines and AMPs would lead to fines out of touch with the actual impact of most offences, and is not likely to be able to appropriately reflect the circumstances of each case. It would make companies more reluctant to enter or remain in the Quebec market, particularly if Quebec accounts for only a small portion of their overall business, for fear of being fined as a percentage of worldwide turnover.

There must be specific factors to consider when applying fines, using a proportionate approach that considers the nature of the violation and the size and data processing activities of the organization that committed the violation. Fines should be focussed on the most egregious cases with intent and gross negligence. If the current range for AMPs is maintained, rigorous procedural safeguards must be put in place to ensure fairness.

The Bill proposes a new private right of action. This would create conditions that promote potentially opportunistic class actions, in addition to increased exposure by organizations to privacy-related claims, including claims for punitive damages. It imposes a strict level of liability for privacy that is unprecedented, creating a disproportionate burden on businesses.

Bill 64 attaches liability unless the underlying event was impossible to foresee and impossible to avoid. There is no due diligence defence or other defence set out in the proposed regime. An organization could still incur liability if it acted reasonably and responsibly, provided notice of possible risks to the individual in advance and took all possible precautions to manage personal information in a compliant manner.

If the private right of action is ultimately pursued, it must be implemented only as a last resort, once it is clear that the use of fines and AMPs is not sufficient. In addition, it must allow for all reasonable defences at law, including the exercise of due diligence.

7. Reasonable transparency should be required around profiling and decisions based on solely automated processing

When an organization uses personal information to render a decision based exclusively on automated processing, Bill 64 proposes to grant individuals the right to be informed at or before a decision is made, including to be provided with information regarding the elements of personal information used, the reasons and principal factors leading to the decision and the right to have their information corrected. The organization would also be required to allow the person to submit observations for review of the decision.

To assist individuals in better understanding how decisions are made about them, we support a requirement for organizations to share summary information (in their privacy policies) with individuals about the use of automated decision-making, the factors involved in the decision, and where the decision is impactful. They must not be required to reveal any confidential or proprietary commercial information, algorithms or procedures.

[2] Bill 64 includes a penal regime with fines of up to $25,000,000 (or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year), doubling this for subsequent offences. The Bill also sets out administrative monetary penalties (AMPs) for a broad range of offences of up to $10,000,000 (or, if greater, 2% of worldwide turnover for the preceding fiscal year). In addition, the Bill proposes a private right of action with no-fault liability.

If concerned individuals submit observations to the organization for review, an organization must have the discretion to determine whether or not to ultimately change its decision. These decisions are highly nuanced, and a right to object to decisions based solely on automated processing would be highly problematic.

As drafted, the notice requirement is too broad, as it would be applicable in all circumstances involving decisions based on automated processing, regardless of materiality of the impact of the decision on the individual.

It is far from clear that all forms of automated decision-making are problematic or warrant a regulatory response. In fact, "automated decision-making" includes a range of legitimate activities, such as a website declining to serve copyright-protected content to a user resident in a jurisdiction where the website provider does not hold the rights to make that content available. As data becomes more complex, the use of automation is critical and beneficial. There are a growing number of helpful automated decisions being made each day, resulting in beneficial services for consumers, such as chatbots that provide consumers with relevant and personalized advice.

Individuals are demanding faster, easier and more intuitive services and automation is central to the delivery of this promise. There are cases where automated decision-making is linked to the actual provision of a service that a consumer may want or need. There must be an understanding that if a consumer objects to the automated decision-making, they would not be able to access the service altogether.

Bill 64 would also require organizations that collect personal information using technology that has the ability to identify, locate or profile an individual to inform the individual of such technology and the means available, if any, to deactivate such technology.

In the case of marketing, profiling is intended to provide an individual with a more relevant experience, such as if a product or service is offered based on an individual's previous preferences and habits. Many organizations create a profile or use automated decision-making in order to target their marketing efforts, including through the use of third-party analytic tools and software, such as cookies, pixels and beacons.

We caution against the GDPR model, which places restrictions on solely automated decisions that produce "legal **or** similarly significant effects,", as there is significant uncertainty by organizations in assessing "similarly significant effects," stifling innovation and resulting in industry confusion.

Transparency will be the most important factor. Organizations should be transparent in their privacy policies about their use of third-party analytic tools and software to track, identify and target individuals in order to serve them relevant advertising. Where possible, they should also refer individuals to the opt-out mechanism accessible through the service provider's platform.

8. The consent exception for de-identified information should be broadened, provided certain standards for de-identification are met

De-identification and anonymization are among the most effective privacy-protective mechanisms available for organizations to engage in data analytics and innovation in the digital economy.

Bill 64 states that personal information collected for one purpose may be used, without consent, for the secondary purposes of study or research or for the production of statistics, if the information is de-identified.

As the consent exemption applies only to use within the enterprise, the purposes of study, research and the production of statistics may be construed as enterprise or business analytics. This should be clarified in the Act.

Given the critical importance of de-identification to responsible innovation, and in order to remove any legal uncertainty, the Act should be amended to further permit the collection, use and disclosure of de-identified information without consent for all reasonable purposes, if certain standards are met.

To ensure a level playing field and provide clarity, it is important for organizations to have a set of common standards by which they can demonstrate whether they took all reasonable steps at the time to de-identify personal information and mitigate the risk of re-identification. The standard of de-identification and ongoing monitoring should fit the context, which is more relevant than the "type" of data.

The Act should acknowledge formal industry standards, and include benchmarks for technical and administrative procedures, monitoring, and risk assessments and protocols. The Act should clarify parameters of accountability around the onward transfers of de-identified data, and should emphasize the need for contractual provisions between organizations to be in place to address re-identification.

As technology evolves, the requirements for de-identification will need to evolve too. We propose that the government work with industry to develop these standards , which could result in a formal certification involving a third-party accreditor approved by the Government of Quebec (see recommendation 9 below).

9. Self-regulatory measures should be encouraged and incentivized to ensure regulatory efficiency

All sectors have a role to play to protect the privacy of Quebecers. A co-regulatory model in which government regulation and industry self-regulation work in tandem is important to ensure regulatory efficiency. There is no one-size-fits all approach to privacy compliance; much depends on each sector and the types of information being collected, used and shared. Now and into the future, codes, certifications and other standards will play an important role in supplementing privacy legislation.

All schemes should be voluntary, recognizing the varying degrees of data processing operations among organizations, and ensuring organizations with limited resources are not unduly impacted. Standards could be either self-regulated or formally recognized by government, as outlined below:

A. **Self-regulated standards and codes:** Self-regulated standards and codes should be referenced in the Act as tools that can help organizations ensure compliance, and help demonstrate accountability in the event of an investigation by the Commission d'accès à l'information du Québec. Industry should be encouraged to develop and follow these standards and codes.

   Industry and professional self-regulated codes of practice are practical and efficient tools to steer privacy compliance. For example, the Canadian Marketing Code of Ethics and Standards is a comprehensive code that establishes and promotes high standards for the conduct of marketing and strengthens marketers' knowledge of compliance requirements. Section J of the Code addresses the protection of personal privacy. The Code is reviewed and updated annually. Upon joining the CMA and upon membership renewal each year, all CMA members agree to comply with the Code.

   These instruments operate in a legal environment that includes consumer, competition, health and safety, labour and environmental legislation and regulations, and contract and tort law. For example, if an organization purported to be in compliance with a code but was not, it could be

subject to the Competition Act for misleading advertising. Failure to adhere also has a reputational impact.

The Commission d'accès à l'information du Quebec should investigate and audit only where complaints arise that have not been resolved internally, or where an adequate internal complaints process has not been established. When an organization could not demonstrate compliance, it would risk falling under general compliance rules enforced by the Commission.

B. **Formally recognized certifications and codes:** Quebec's privacy framework would be further enhanced if the Act allowed for the formally recognition some certifications and codes based on approval by the Government of Quebec or the Commission d'accès à l'information du Quebec, with oversight from select third-party accrediting bodies.

The Act must not prescribe a list of areas that warrant standards but rather a framework to allow existing bodies to develop schemes for approval in response to market needs. They could be in relation to certain provisions of the Act only or a broad assessment of privacy (for example for a sector or industry).

Borrowing from the UK model, proposals submitted for approval could identify the data processing operations covered, the categories of organizations that they apply to, and the privacy issues that they intend to address. Proposals must be informed by adequate consultation and be ranked against standard admissibility criteria. Once an organization is deemed to be in compliance with a certification or code by a third-party accreditor, it would be considered to meet the requirements for a set time period (e.g., three years), after which its adherence would need to be renewed. This approach should be developed through collaboration between the provincial and federal governments. The Standards Council of Canada has a thorough development and review process for accreditation standards; its role should be leveraged and maximized.

The Commission d'accès à l'information du Quebec could have a general obligation to consider adherence to formally recognized codes and certifications in making decisions about whether to investigate. Compliance should also be a factor in determining due diligence in the context of an investigation or fine. The Commission should not have authority to periodically review an organization's adherence to a scheme, and this would properly fall with the third-party accrediting body. The accrediting body could have a duty to report incidences to the Commission where an organization's compliance is revoked for non-compliance.

10. The right to data portability should be postponed until its wider impacts are understood

The proposed right to data portability would provide an explicit right for individuals to direct that their personal information be moved from one organization to another in a standardized digital format, where such a format exists.

The primary objective of data portability is two-pronged: to provide greater individual control over data and to encourage competition in the marketplace. Although data portability is intended to enhance consumer control and choice, it creates serious new risks for consumers with regards to cybersecurity, privacy and confidentiality. In addition, its wider impacts on the economy, innovation and competition are not well-understood. More research must be done to understand its effects.

It is important to postpone the implementation of the data portability right proposed in Bill 64 pending further study of its non-privacy impacts. Industry sectors can play a pivotal role in identifying specific technical or competitive considerations.

To ensure that this new right does not create unintended consequences that hamper Quebec's economic well-being, other bodies, such as the federal Competition Bureau, should be invited to collaborate in a significant way in the research and development of this concept in a Quebec context. This is more than a privacy issue, and the corresponding reform of other statutes may be necessary.

If the right to data portability is ultimately pursued, it will require:

A. **A phased-in approach that allows for the development and implementation of sector-specific frameworks:** We have learned from the GDPR model, which creates a sweeping data portability right but provides little clarity on implementation, that a more practical approach is essential.

   Sector-specific frameworks would need to be developed in consultation with industry to reflect the current practicalities and risks in each affected industry, and could be implemented through regulation. These frameworks must consider important economic, technical, authentication, security and operational issues. Other regulators beyond the Commission d'accès à l'information du Quebec should be involved in the enforcement of such frameworks, with the Commission overseeing issues related only to privacy compliance.

B. **Limits on the scope of ported data:** Providing data directly to an individual is an extension of the current right to access under Quebec's privacy law, which in its current form goes a long way to support consumer control. Individuals already have a right to access the personal information that an organization holds about them, to challenge its accuracy and completeness, and to have that information amended as appropriate. Organization-to-organization transfers must be done at the request of the individual. The right to data portability must be considered separately from the right to access, and the scope of data should not necessarily include all that is afforded under a typical access request.

   Ported data must be limited to personal information provided by the individual. Other types of data should generally be excluded, such as data that may be proprietary or not considered personal information. We support the government's stated intent that the proposed data portability right not cover information that was created, derived, calculated or inferred from data provided by the individual.

   Sector frameworks have the capacity to provide clarity on the scope of data appropriate for the objective of data portability, including limited data related to commercial transactions. With respect to higher risk or more sensitive data, it is advisable to limit the data fields that can be ported and strengthen authentication requirements.

   To avoid unnecessary disruption to standard business practices, the right to data portability must not automatically place an onus on an organization to delete ported data. Organizations must be permitted to follow standard policies and procedures around retention.

   In terms of format, ported data must be limited to digital data in technology neutral formats, in other words, a standardized digital format, where such a format exists, and not physical records to which normal access rights may apply. The Act must allow for solutions to emerge in each sector, and to evolve over time. As advancements occur, the scope of ported data could evolve accordingly.

   These rules must not create undue barriers for SMEs, as this would undermine the original intent of greater competition.

C. **Measures to protect against data breaches and fraud, and to ensure fair accountability:** Appropriate data security and authentication requirements must be in place to prevent data breaches and guard against fraudulent requests (possibly linked to the sensitivity of the data).

Portability must be conditional on the request being made by the individual (and not just the third-party organization), and on having an adequate sector-specific framework in place. Bulk or automated requests from third parties must be prohibited, and consent for the sharing or obtaining of ported information should not be buried in contracts.

An exclusion of liability must be in place when an organization is mandated by a consumer to port data to a third party. The responsibilities of the originating organization must be limited to confirming that the request is from the individual (i.e. not fraudulent) and to safely transferring the data. The originating organization must not be held responsible if the recipient organization falls short of its safeguarding obligations and other requirements under a sector-specific framework, leading to misuse of the data. Finally, the law should set out the bases on which an organization can object to a request for data portability.

For questions or comments regarding this submission, please contact:

Sara Clodman
VP, Public Affairs and Thought Leadership
sclodman@theCMA.ca

Fiona Wilson
Director, Government Relations
fwilson@theCMA.ca

About the CMA

The CMA is the voice of the marketing profession, representing more than 50 corporate, not-for-profit, public, and post-secondary members across Quebec, and contributing to the professional excellence of Quebec marketers through our events and professional development programs. Our community includes creative, media, and PR agencies, research firms, management consulting firms, technology companies and other suppliers to the marketing community. We support activities related to thought-leadership, professional development, consumer protection, and commercial success. We act as the primary advocate for marketing with governments, regulators and other stakeholders. Our Chartered Marketer (CM) designation ensures that marketing professionals are highly qualified and up to date with best practices. We champion self-regulatory standards, including the mandatory Canadian Marketing Code of Ethics and Standards.