Submission by the Canadian Marketing Association to the Special Committee to Review the BC Personal Information Protection Act

July 30, 2021

Executive Summary

The Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Special Committee reviewing British Columbia's Personal Information and Protection Act (PIPA).

The CMA is the voice of the marketing profession in Canada, representing more than 400 corporate, not-for-profit, public, and post-secondary member organizations.

We strongly urge British Columbia to proceed with amendments to PIPA **only after the federal government proceeds with the next iteration of privacy law reform**. It is critical for British Columbia to align with the federal government's approach to privacy law so that organizations across the country have consistent regulation, and consumers have strong protection.

We appreciate the Government of British Columbia's commitment to protecting privacy, while supporting the responsible use of data to fuel economic growth. Any updates to PIPA must reflect:

- The critical importance of data, including personal information, to the digital economy and post-pandemic economic recovery,
- Evolving consumer privacy expectations, which indicate consumer appreciation of the value of responsible data use and sharing, and:
- The ability for small and medium-sized businesses (SMEs) – the backbone of the economy – to leverage consumer data to compete and grow.

The CMA has seven recommendations to better protect the privacy of individual British Columbians, while ensuring that any new requirements do not pose an unnecessary burden on businesses or inhibit the growth and prosperity of British Columbia's innovation ecosystem.

1. **Align with federal privacy law** to prevent disruptions for organizations and consumers, and complications for trade and investment.

2. **Preserve PIPA's strengths as flexible, principles-based and proportionate to the privacy objectives to be achieved**, permitting the law to be nimble in the face of rapidly evolving technologies, business models and consumer expectations.

3. **Introduce mandatory data breach reporting requirements** in line with other jurisdictions to help individuals become aware of, and take steps to mitigate, the potential risks involved with the improper disclosure of their personal information.

4. **Ensure PIPA's consent framework is meaningful for consumers and practical for organizations.** PIPA's approach must avoid the over-emphasis on express consent, and the rigid, rules-based requirements for requesting valid consent (and for relying on exceptions to consent) found in Bill C-11. A legitimate interests exception to consent should be explored.

5. **Consider the practical consequences of a new right to deletion**, and include sufficient exceptions to the right that balance it with other important social and economic objectives.

6. **Enhance meaningful protections around automated decision systems**, including through new openness and transparency requirements, without restricting the beneficial use of these systems for consumers and organizations through unduly harsh restrictions.

7. **Preserve the ability for organizations to leverage de-identified and pseudonymized information for the benefit of consumers and businesses** by excluding truly de-identified information that is, by definition, not personal information, from the scope of the law.

The CMA looks forward to continued discussions with the Government of British Columbia on these important topics.

Introduction and Context

The Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Special Committee reviewing British Columbia's Personal Information and Protection Act (PIPA). In light of recent developments, including the federal government's introduction of Bill C-11, this submission supplements our August 2020 submission to the Special Committee.

The CMA is the voice of the marketing profession in Canada, representing more than 400 corporate, not-for-profit, public, and post-secondary member organizations. We are committed to helping marketers and their organizations maintain high standards of conduct and transparency through our mandatory Canadian Marketing Code of Ethics & Standards, and our training and professional development opportunities, including the Chartered Marketer (CM) designation program. We offer extensive resources on privacy law and best practice, including a Guide on Transparency for Consumers. Our online Consumer Centre helps consumers can understand their privacy rights and obligations. We regularly handle marketing-related privacy enquiries and requests for information from both marketers and consumers.

The CMA's BC Marketing Forum supports members across British Columbia by giving them a stronger voice and amplifying local marketing best practices, programs and thought leadership. Marketing – the link between organizations and their consumers – is a key driver of British Columbia's economic growth and recovery. Marketing stimulates consumer demand, supports business expansion, and generates substantial direct and indirect employment for British Columbians across all key sectors and industries.

British Columbia's marketers highly value their relationships with consumers. The loyalty and trust of customers is the foundation for business success, and most organizations work hard to protect and respect the privacy interests of the individuals they serve.

The purpose of PIPA is: "to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes **both** the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

We appreciate the Government of British Columbia's commitment to protecting privacy, while supporting the smart use of data to fuel economic growth.

It is critical for British Columbia to align with the federal government's approach to privacy law so that organizations across the country have consistent regulation, and consumers have strong protection. We strongly urge British Columbia to proceed with amendments to PIPA only after the federal government proceeds with the next iteration of privacy law reform.

It is important that any updates to PIPA pursued by the Special Committee reflect the following:

- **The critical importance of data to the digital economy:** British Columbians have never been more reliant on the digital economy. It improves our personal lives and well-being. At work, it supports our ability to innovate, build businesses and remain competitive.

  When used responsibly and in a privacy preserving manner, the analysis and use of personal information is critical to our digital economy, and can be highly beneficial to consumers, organizations, government and society.

Data is, and will continue to be, a driving force for innovation across all industries. It is estimated that Canadian investment in data has grown more than 400 percent in the last 15 years, and that data-related assets in Canada were worth $217 billion in 2018—equivalent to more than two-thirds the value of the country's crude oil reserves. What's more, we are relying on our data-driven industries to play a central role in driving post-pandemic economic recovery.

Privacy regulation that supports the increasing focus on data as a vehicle to drive innovation, efficiencies and productivity will help ensure a strong economic future for British Columbians for years to come.

- **Evolving consumer privacy expectations:** The ability for organizations to collect, use and disclose personal information is key to providing value to consumers. At the same time, consumers increasingly expect organizations to deliver the intuitive products and services they want and need.
    - In a recent survey by Ipsos Canada, 50% of consumers indicated a desire to see internet advertising that is relevant and targeted to them, despite having concerns about the security of their personal information.
    - A 2018 research study Data Privacy – What the Canadian consumer really thinks found that a strong majority of Canadian consumers (76%) are willing to share personal data in order to receive benefits, as long as the data is properly protected.
    - According to a recent survey from Kantar, more than 80% of consumers are concerned about the unauthorized access of their personal information, while only 35% are concerned about receiving unwanted ads. Although 77% of Canadians are concerned about privacy and data protection, they are significantly more concerned about criminal activity than by attempts by the private sector to serve them in a more targeted and personalized way.

Technological advancements have provided organizations across British Columbia with the agility to offer relevant, useful offerings to consumers who want them.

User data-driven systems, including recommendation engines, customer service chatbots and marketing geared towards consumer preferences, are important and beneficial tools and services for consumers, and for organizations striving to better serve their customers. For example, nearly all industries (retail, banking, insurance, travel, grocery etc.) now offer recommendation engines to assist consumers with their digital choices. Many consumers have grown accustomed to receiving these recommendations, as they often save time and money, and help to ensure consumers have everything they require to utilize the products and services they are purchasing.

Similarly, many companies run advanced customer pricing analytics/loyalty analytics to offer consumers discounted prices based on historic shopping behaviour. This helps consumers save money and helps companies build better relationships with consumers by providing them with opportunities to save.

British Columbia's public policy approach must acknowledge evolving consumer interests and expectations, and recognize the enormous economic and social benefits of the data economy for individuals.

- **The ability for small and medium-sized businesses (SMEs) to flourish and sustain our economy:** A recent survey of over 1,000 Canadian SMEs, the State of Small and Medium Businesses in 2021, shows the critical importance of consumer data to SMEs. The ability to leverage consumer data to communicate regularly and in a personalized manner with customers was cited as the primary way SMEs built enough consumer trust and loyalty to weather the

pandemic. Their ability to access and apply consumer data was also cited as their top ongoing strategy to continue to compete against large online competitors.

As British Columbia navigates the road to post-pandemic recovery, it is critical that any proposal to update privacy regulation focus on protecting consumers against bad actors and egregious offences, as opposed to creating an undue administrative burden for responsible companies, including the SMEs that are the backbone of our economy.

An Ernst and Young Global Information Security Survey conducted in 2020 showed that Canadian companies are lagging behind their global peers when it comes to adequate protection against cyber threats. Efforts to support the cybersecurity maturity of organizations should be prioritized, as they help to protect against the data breaches that pose the biggest threat to the privacy of consumers. Cybersecurity breaches have a disproportionate impact on SMEs. In 2020, the average cost of a data breach on a Canadian company was $4.5M, and Canadian businesses reported spending a total of $7B directly on measures to prevent, detect and recover from cyber security incidents.

With 99% of British Columbia's businesses falling into the small to mid-sized category, it is critical for these companies to focus on security measures, rather than on new privacy requirements that create a significant administrative burden without an equally strong privacy protection rationale. For many SMEs, these barriers could prove debilitating in terms of the capital required, and limitations on the ability to automate and optimize. Furthermore, SMEs lack ready access to legal advice and representation to navigate the complexities of restrictive legislation, making it more difficult for them to use data to innovate and compete against large competitors with significantly more resources.

Many of the voices calling for stringent privacy reform aim to protect against flagrant and malicious misuse of consumer data, no doubt responding to the more extreme cases of misuse that have occurred in recent times. We do not in any way condone these abuses. Indeed, it is important that the law focus on preventing malicious misuse of data rather than creating hard barriers to reasonable uses of data that have become essential aspects of business in a digital age.

Recommendations

The CMA has seven recommendations to better protect the privacy of individual British Columbians, while ensuring that any new requirements do not pose an unnecessary burden on businesses or inhibit the growth and prosperity of British Columbia's innovation ecosystem.

1. Align with federal privacy law to prevent disruptions for organizations and consumers, and complications for trade and investment

There must be significant alignment between PIPA and federal privacy law, which is scheduled for reform, in order to prevent the damaging fragmentation of privacy frameworks, and negative impacts on the data-based integrated industries that operate across provinces, the country and internationally.

If approaches between the provinces and federal government are not aligned, the resulting patchwork of privacy legislation will create undue complexity for organizations, cause confusion for consumers, complicate conditions for trade, and reduce British Columbia's attractiveness as a business destination. It will also create crippling demands on SMEs and opportunities for malicious actors seeking to exploit differences in data protection.

The federal government's Bill C-11, with amendments in a few key areas, proposed an effective approach to private sector privacy law. Importantly, it would preserve Canada's principles-based, technology and sector-neutral approach to privacy, helping to ensure flexibility in the face of rapidly evolving technologies, business models and consumer privacy expectations. It also would provide consumers with added privacy protections and controls, including new rights to have more meaningful control over their data and new requirements for companies to be more transparent about their use of personal information – backed by strong penalties and enforcement.

The CMA has provided significant feedback to the federal government on the strengths and challenges of Bill C-11. The recommendations in this submission are guided by the need to ensure interoperability with the federal approach.

It is critical for British Columbia – and all provinces – to align with the federal government's approach to privacy law so that organizations across the country have consistent regulation, and consumers have strong protections.

2. Preserve PIPA's strengths as flexible, principles-based and proportionate to the privacy objectives to be achieved

In today's digital economy, it is important for the law to be nimble in the face of rapidly evolving technologies, business models and consumer expectations, without the need to repeatedly introduce legislative amendments to keep up with the times.

While some aspects of PIPA are due for a thoughtful update, we must recognize that this law has many strengths. It is based on sound principles that are flexible enough to account for context, and it can be thoughtfully applied to all technologies and business models. This is especially important to ensure compliance is not unduly onerous for SMEs, allowing them to determine the most effective way to meet their common obligations given operational realities and context-specific risks.

Privacy law must continue to be flexible enough to impose measures proportionate to the privacy interests involved and the individual's reasonable expectation of privacy in the circumstances. It must have a clear purpose clause ensuring that the law be interpreted in a proportionate and reasonable manner based on the circumstances.

Many features of PIPA and other existing Canadian privacy laws 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, have created a staggering regulatory burden for both government and business, and have had negative and costly impacts on the economy and trade.

In considering the adoption of certain aspects of GDPR, we urge the government to evaluate each based on its merit in the British Columbia context, with the goal being compatible privacy outcomes as opposed to compatible legislative requirements.

3. Introduce mandatory data breach reporting requirements in line with other jurisdictions

At present, PIPA does not require an organization to notify the Office of the Information and Privacy Commissioner (OIPC) or affected members of the public when there has been a significant unauthorized disclosure of personal information.

We support the OIPC recommendation for the introduction of mandatory data breach reporting requirements, in line with the requirements proposed under Bill C-11. These requirements will help ensure individuals become aware of and can take steps to mitigate the risk of financial or other harm

caused by the improper disclosure of their personal information. It will also provide more opportunities for the OIPC to educate organizations on how to improve their privacy controls.

4. Ensure consent requirements and exceptions are meaningful for consumers and practical for organizations

Consent must be meaningful and focused on what matters most. The CMA provides significant guidance to the marketing community on how to ensure these principles are met.

British Columbia's consumers already suffer from "consent fatigue", causing them to be less likely to carefully review notices and make informed decisions. It is important to ensure that any reforms to PIPA do not exacerbate this problem.

The provisions proposed in Bill C-11 present a framework that would be more prescriptive than the GDPR, which offers an objective principles-based approach to consent and alternative legal bases for processing.

The bill's over-emphasis on express consent – coupled with its rigid, rules-based requirements for requesting valid consent and for relying on exceptions to consent – will be problematic for both consumers and organizations. Adopting Bill C-11's approach would result in a lack of interoperability with other consent regimes, which would cause organizations operating in British Columbia to re-consider their operations due to the additional compliance burdens associated with managing the law's unique consent requirements.

Aspects of Bill C-11's consent provisions that need to be adjusted are:

a. **Form of consent, and requirements for valid consent:** Under Bill C-11, express consent would be required for the collection, use, and disclosure of personal information unless the organization established that it is appropriate to rely on an individual's implied consent.

   This departs from PIPEDA's current balanced approach, which encourages organizations to make a contextual analysis of whether to seek express or implied consent, based on the reasonable expectations of the individual and sensitivity of the information. It also stands in contrast to the GDPR's approach, which balances a requirement for express consent with alternative bases for processing. Both approaches recognize that explicit consent is not always appropriate, effective, or meaningful for consumers.

   The CMA recommends against the prescriptive rules for requesting valid consent under Bill C-11 in favour of the more balanced approach under PIPEDA. This includes indicating that express consent "should" rather than "must" be obtained, and that consent is valid only if "it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."

   In addition to the overemphasis on express consent, Bill C-11 proposes even more rigid and prescriptive requirements for valid consent, mandating organizations to provide information to individuals in five specific areas. This will result in consumers being faced with more repetitive and lengthy requests for consent.

   Disclosure requirements that are too prescriptive will not result in better consumer understanding. Given the wide variety of business models and data uses, organizations need the flexibility to determine how best to communicate with individuals in an understandable way, considering the context, target audience and actual risks. The CMA recommends organizations be permitted more flexibility to satisfy the validity requirement proposed in Bill C-11 using different methods.

We also caution against the language of the refusal to deal provision. Like PIPA, Bill C-11 indicates that an organization must not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service.

Bill C-11's more rigid consent framework (described above) makes this significantly more impractical. It is uncertain whether common and beneficial uses of information by organizations can continue to be conditions of using a product or service, such as personalizing experiences or making recommendations (where these experiences or recommendations are part of the product or service). PIPA should adopt PIPEDA's more flexible standard of beyond the "explicitly specified and legitimate purposes."

b. **Exceptions to consent:** The exceptions to consent contained in Bill C-11 are unduly narrow and only cover specific circumstances. Even under the GDPR, the additional legal bases for processing (e.g., for legitimate interests) offer more flexibility.

Indeed, the exceptions are too prescriptive to accommodate many common activities that a reasonable person would expect a business to undertake. The exceptions to consent for business activities must be broadened to recognize additional common practices for businesses with respect to R&D activities that may use personal information (e.g., to allow businesses to better understand their customers, their preferences, and the way they use products and services). This will support consumer understanding by allowing privacy policies to focus on more unexpected uses.

Consumers would be well protected under this approach because any collection, use or disclosure of personal information (even if valid consent is obtained or an exception is used) must be only for purposes that a reasonable person would consider appropriate in the circumstances. For more than 20 years, this "reasonable person test" has been an overarching requirement helping to protect against the abuse of consent provisions. This will continue to be the case.

We strongly recommend that the Special Committee consider incorporating a legitimate interests exception to consent, which is categorically different than the exceptions to consent found in Bill C-11. The exception is practical enough to apply to any type of processing for any reasonable purpose, and unlike the Bill C-11 approach, it is not limited to "collection" and "use".

It also creates greater accountability for organizations as there is built-in safeguards. Further, it will enhance interoperability with leading privacy laws elsewhere, including, for example, the GDPR and Singapore's data protection law, both of which have built in strong safeguards.

The GDPR incorporates a three-part test that considers if there is a legitimate interest behind the processing, if the processing necessary for that purpose, and if the legitimate interest overridden by the individual's interests, rights or freedoms.

Singapore has supplemented the GDPR approach with explicit requirements for conducting an impact assessment and informing individuals of reliance on legitimate interests. This provides additional guardrails. The Special Committee should consider a similar approach for PIPA.

5. Consider the practical consequences of a new right to deletion

We agree that personal information is not held by organizations for longer than necessary, and that consumers have sufficient control in that regard. At the same time, adding a new right for individuals to request that their personal information be deleted by an organization creates several complexities.

PIPA already requires an organization to destroy personal information, or render it unidentifiable, "as soon as it is reasonable to assume that…the purpose for which that personal information was collected is no longer being served by" its retention, and that retention is not necessary for legal or business purposes.

By contrast, Bill C-11 gives individuals the express positive right to require an organization to, as soon as feasible, "dispose of personal information that it has collected from the individual". This new right offers little additional privacy protection to consumers given the protection that is offered through regular retention limitations and disposal obligations. Privacy law already limits the scope of personal information that can be collected, the purposes for collection, the requirement for consent, the ability to withdraw consent, and places limits on the retention of personal information. These obligations give individuals sufficient control over their personal information, and the ability to trigger the cessation of collection, use, disclosure and ultimate disposal in appropriate circumstances.

The proposed right could create a false expectation with consumers that the responsibility is on them to ensure their data is deleted, causing them confusion, and potentially creating a false sense of additional privacy protection.

Recent data breaches concerning overheld information indicate that some organizations are retaining personal information for longer periods than necessary. An effective remedy for this already exists through PIPA's provision that prohibits an organization from retaining personal information longer than necessary. Indeed, under Bill C-11, organizations in violation of this requirement could face still monetary penalties. This is a much stronger remedy than the right to disposal, which only impacts individuals who make a request, and targets not just overheld information, but also information that should be held for valid reasons.

The broad scope of the right and the requirement to carry out disposal as soon as feasible would create practical challenges and costs without a proportionate privacy benefit. It is difficult and disruptive to dispose of personal information on request, before the retention period has expired, without corrupting records and disrupting processing of other data.

An additional obligation for organizations to inform their services providers of the disposal request, and to confirm the disposal, would complicate things further. While this obligation can be set out in contracts with service providers, its implementation faces significant practical barriers. Many services providers, including providers of most cloud-based services, do not have access to the data that they process on behalf of their customers and, as a result, are unable to provide confirmation of disposal.

The provision would impair the ability of organizations to retain personal information for reasonable and legitimate business purposes. However, should the Special Committee consider implementing it, it is critical that the right be subject to additional exceptions that balance disposal with other important social and economic objectives and practical considerations.

This includes if the organization requires the information for legal or business purposes (to the extent that is appropriate in the circumstances), to comply with other requirements under privacy law, or with respect to an existing legal proceeding, inquiry or investigation (or one that could be initiated within an applicable statutory limitation period).

The law should not require organizations to dispose of personal information:

- that privacy law would otherwise permit the organization to retain (e.g., records of bad debt or poor payment history, which would be relevant to a subsequent transaction with the individual);
- that privacy law permits the organization to collect, use or disclose without knowledge or consent (e.g., personal information processed to prevent fraud); and

- that is required to give effect to a withdrawal of consent by the individual and permit the organization to continue to comply with laws respecting adherence to such requests (e.g., to comply with CASL or Unsolicited Telecommunications Rules).

Even under the GDPR, the right to erasure applies only where the legal basis on which the processing was conducted no longer exists (and there are five bases for processing in addition to consent). It is also balanced with a series of exceptions (such as when processing is necessary for freedom of expression, archiving purposes or other compelling legitimate grounds).

Looking at Bill C-11, the only exception that would permit the continued retention of personal information for legitimate business purposes (as opposed to in response to legal requirements) would be for an organization to spell out in its customer contracts the organization's legal right to retain all data subject to its retention policy, even after a disposal request. This would lead to lengthier, more detailed consumer agreements, working against the policy objective of focussing privacy policies on unexpected areas where a consumer has a meaningful choice.

6. Enhance protections around automated decision systems without unduly restricting the beneficial use of these systems for consumers and organizations

We support greater accountability around the use of automated decision systems (ADS), as well as enhanced efforts to ensure consumers are aware of how ADS may impact them.

It is important that new requirements not be unduly restrictive, as this could impact British Columbia's position in the global innovation ecosystem, as well as the availability of innovative goods and services for consumers by discouraging organizations from developing and leveraging automated or partially automated systems.

New transparency requirements around the use of ADS will go a long way to protect consumers. However, harsher restrictions on the use of such technology would put organizations in British Columbia at a competitive disadvantage with respect to their counterparts in other jurisdictions, like the United States, that do not impose such restrictions. Furthermore, they will add unnecessary administrative burden for organizations – with the associated cost being passed along to consumers – without a compelling privacy protection benefit.

There are a growing number of helpful automated decisions being made about us each day, resulting in beneficial services for consumers. Examples include chatbots that provide consumers with relevant and personalized advice, or the use of AI in market research to deliver adaptive surveys to customers (as opposed to more rudimentary systems, under which every respondent would be asked every question regardless of how they answered earlier questions).

Alongside the tangible benefits to individuals, AI helps businesses in British Columbia improve accuracy and efficiency and reduce costs. For example, one of the CMA's media agency members is implementing an optimization tool that uses machine learning based on a decision tree to test, learn and optimize its offers in real time. Another CMA member in the not-for-profit sector has implemented a consumer voice initiative that uses natural language processing to transcribe voice to text, and better understand verbal queues. This greatly enhances the organization's ability to gain deeper and quicker insights into how individuals perceive their interactions with the organization, allowing it to adjust marketing and fundraising efforts accordingly.

We support Bill C-11's general openness and transparency requirements, which would result in greater consumer understanding and acceptance of ADS. However, to the extent that the Special Committee considers additional aspects of the framework for ADS proposed in Bill C-11, we suggest re-consideration

of both the definition of ADS and the right to explanation, both of which are broader than what is necessary for effective privacy protection.

Given the bill's transparency obligations, the overly broad definition of ADS will result in the provision of unnecessary information to consumers, and a significant administrative burden on organizations, with no material privacy protection benefit. The definition itself should be narrowed to only those decisions that materially assist or replace human decision-making, and the element of "judgement" should be removed.

The bill also proposes a new right to explanation that indicates that, on request by an individual (and regardless of whether there is any impact on the individual), an organization must provide an explanation of: (i) any prediction, recommendation or decision made using an automated decision system; and (ii) how the personal information used to make the prediction, recommendation or decision was obtained.

This requirement, as drafted, would capture a broad range of routine, micro decisions, the majority of which have no significant impact on an individual or potential to harm them (such as a call centre using AI to support call routing, or a website declining to serve copyright-protected content to a user in a jurisdiction where the website provider does not hold the rights to make that content available).

The requirement would result in large amounts of innocuous information being provided to consumers, making it difficult for them to determine what is most important. The requirement would also create a potential burden for companies dealing with large volumes of requests (including potentially automated requests), without a corresponding benefit for individuals.

We urge the Special Committee to ensure that any new right to explanation focus only on the use of ADS that could have a significant impact on an individual, permitting them to engage if they feel they have been harmed. Furthermore, given the nature of data flows and automated decisions in practice, particularly with regards to machine learning, deep learning and neural nets, the explanation required by organizations should be "reasonable in the circumstances."

This approach could leave room for privacy commissioner guidance or industry best practices (codes or certifications) to support these requirements, including what explanation would be "reasonable under the circumstances".

With these adjustments, the approach proposed in Bill C-11 would be a reasonable and effective one to incorporate into PIPA.

We note that the OIPC has recommended an approach similar to Quebec's proposed Bill-64. This includes recommendations to have organizations "on request, disclose the reasons and criteria used", and to "receive objections from individuals to the use of automated processing by someone within the organization that has the authority to review and change the decision".

We support the requirement for organizations to share summary information with individuals about the use of automated decision-making, the factors involved and where the decision is impactful, as long as it does not require organizations to reveal any confidential or proprietary commercial information, algorithms or procedures. However, any right to object to decisions using "automated processing", even if it were solely automated processing, would be highly problematic.

A regulatory response should be remedial, prohibiting or restricting only those activities where there is clear evidence of harm. 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. 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.

If concerned individuals are permitted to submit observations to the organization for review, an organization must have the discretion to determine whether to ultimately change its decision.

Finally, we caution against another aspect of the approach in Quebec's Bill 64, which requires that organizations that collect personal information using technology that can identify, locate or profile an individual to inform the individual of such technology and the means available, if any, to deactivate such technology.

This proposal would impose new obligations on the marketing community's ability to provide consumers with relevant, tailored and useful advertising. 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 to target their marketing efforts, including using third-party analytic tools and software, such as cookies, pixels and beacons. This helps organizations provide consumers with the relevant products and services that they want or need. There is no basis for restricting this type of activity unless there is clear evidence of harm.
Under the GDPR, which places restrictions on solely automated decisions that produce "legal **or** similarly significant effects,", there is significant uncertainty by organizations in assessing "similarly significant effects," stifling innovation and resulting in industry confusion.

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

7. Preserve the ability for organizations to leverage de-identified and pseudonymized information for the benefit of consumers and businesses

De-identification and pseudonymization of personal information are longstanding techniques that are commonly used by organizations to fulfill data minimization requirements and principles. Particularly with respect to internal uses of data by an organization, these techniques are generally regarded as hallmarks of responsible data stewardship, allowing organizations to analyze and extract key insights from data sets while protecting individual privacy. In fact, these best practices have long been viewed as important privacy-protective mechanisms by Canadian privacy commissioners, including the OIPC, who have recommended their use when analysis and other processing does not require the use of individually identified data. If anything, privacy laws should encourage, rather than discourage such techniques.

The CMA supports some aspects of Bill C-11's treatment of de-identified and pseudonymized information. For example, we strongly believe that the simple act of de-identifying or pseudonymizing personal information is not, of itself, a use of personal information that requires individual consent. Like other non-substantive manipulations of data (e.g. truncation, encryption, creation of subsets of personal information from a larger sets), de-identifying or pseudonymizing personal information results in no detrimental impact on the individuals in question - in fact, many of these manipulations and techniques actually serve to enhance privacy protection. While the federal bill unfortunately used language that characterized de-

identification as a "use", it did go some way toward explicitly recognizing that the de-identification of personal information does not require consent, a concept that the CMA strongly supports.

Some parties are understandably concerned with potential scenarios in which personal information may be processed using ineffective or inappropriate de-identification techniques, resulting in output data with respect to which a serious possibility of individual identification remains. However, the CMA would note that in such cases, as a matter of law, the output data would continue to be considered to be "personal information" under PIPA (or any of Canada's private sector privacy laws). Accordingly, any use or disclosure of such data would continue to be subject to all requirements of the Act, and would continue to be investigated and enforced as would any processing of personal information by an organization.

On a related point, we also support Bill C-11's conceptual recognition that assessing the efficacy and adequacy of any de-identification measures as to whether they remove a serious possibility of re-identification is necessarily a context-specific exercise, taking into account the sensitivity of the personal information in question, the proposed use and handling and the associated risk of re-identification. There is no one-size-fits-all approach to de-identification for privacy purposes. As technology evolves, standards for de-identification will need to evolve too. It would also be beneficial for organizations to have a set of common standards for reliable de-identification. There is significant opportunity for government to draw upon private sector work in this area.

Notwithstanding the CMA's general support for these features of Bill C-11, PIPA should not be amended to reflect the remainder of the approach to de-identified information proposed under Bill C-11. That approach would have a profound negative impact on the ability of organizations to innovate and serve customers well. It would impede important data-driven technologies and services (including solutions that rely on artificial intelligence and machine learning) and push the innovation they enable to other jurisdictions with less restrictive frameworks. It would also put British Columbia's privacy law at odds with even the GDPR and California's Consumer Privacy Act (CCPA), which explicitly do not apply to de-identified data.

As currently drafted, Bill C-11 would bring de-identified data within the scope of privacy legislation, essentially regulating the use of what is currently considered by Canadian law to be non-personal information. The definition of the term "de-identify" in Bill C-11 is so broad that it appears to place restrictions on any data that was ever derived from personal information – including even data like aggregate-level numeric statistics. Adopting a similar approach would be a significant departure from PIPA, which indicates that if information is not identifiable, it does not fall within the scope of the law.

Currently, Canadian privacy laws and many international privacy and data protection laws apply only to information about an identifiable individual. By definition, then, information that cannot reasonably be associated with an identifiable individual is not considered to be personal information and is therefore not subject to applicable privacy laws. PIPA must continue to exclude from its scope de-identified information, as the GDPR, CCPA, and each of Canada's private sector privacy laws currently do.

The definition of de-identified information should reflect the test articulated by Canadian courts – and applied by the OIPC - for determining when data may be considered to be personal information under Canada's private sector privacy laws (i.e. "…where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information" or "…an 'identifiable' individual is considered to be someone whom it is reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available)[1]".

[1] Gordon v. Canada (Health), 2008 FC 258.

It should be noted that pseudonymization and similar techniques that may result in output data that would still be considered to be "personal information" under applicable law can still be an effective mechanism to protect personal information while allowing organizations to perform data analysis on individual-level data that does not of itself identify any of the individuals involved. Pseudonymization is explicitly recognized by the GDPR as a privacy-enhancing measure that can reduce risks to individuals and help organizations meet their data protection obligations,[2] and the GDPR permits the processing of personal data for various research and statistical purposes without individual consent. The Special Committee should consider amending PIPA to do the same, thereby helping facilitate innovation and grow the digital economy while protecting privacy.

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 Canadian Marketing Association

The Canadian Marketing Association (CMA) strengthens marketers' significant impact on business in Canada. We provide opportunities for our members from coast to coast to develop professionally, to contribute to marketing thought leadership, to build strong networks across all economic sectors, and to shape positions advocated by the CMA to strengthen the regulatory climate for business success. Our Chartered Marketer (CM) designation signifies that recipients are highly qualified and up to date with best practices, as reflected in the Canadian Marketing Code of Ethics and Standards. Our Consumer Centre helps Canadians better understand their rights and obligations as consumers in a variety of areas, including how to protect their personal information, avoid being a victim of fraud, identify spam, reduce the amount of print mail they receive, opt out of online ads, and protect themselves from Covid-19 scams.

[2] GDPR, Recital 28.