CMA Feedback to Special Committee Reviewing British Columbia's Personal Information and Protection Act (PIPA)

August 14, 2020

Executive Summary

As the voice of the marketing profession, the Canadian Marketing Association (CMA) is pleased to provide feedback to the Special Committee reviewing British Columbia's Personal Information and Protection Act (PIPA).

In our modern digital economy, consumers increasingly expect organizations to deliver the intuitive products and services they want and need. PIPA, now and into the future, is based on a balance between embracing the enormous social and economic benefits of data use for British Columbians while protecting their privacy.

As the Special Committee considers proposing modifications to PIPA, the CMA is pleased to provide the following recommendations to help ensure this important balance:

1. **Preserve PIPA's strengths as a balanced, principles-based and technologically neutral law:** It is important that PIPA remain flexible in the face of rapidly evolving technologies, business models and consumer privacy expectations. It is not in the best interests of consumers and organizations to adopt aspects of international frameworks like the GDPR without assessing each aspect based on its merit in the British Columbia context.

2. **Introduce mandatory data breach reporting requirements in line with other jurisdictions in Canada:** 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.

3. **Strengthen and leverage the current enforcement model, given that existing tools have resulted in a high level of voluntary compliance to date.** In particular:
    A. **Improve the current model of fining through the Supreme Court of British Columbia:** Organizations are more cautious and less likely to consult in a cooperative way with a regulator that has the direct power to impose monetary penalties against them. Any new offences should be carefully considered for prosecution by the Court, not the OIPC, making best use of existing provisions and infrastructure.
    B. **Implement procedural safeguards for audits and investigations:** Additional procedural safeguards should be put in place to ensure audits and investigations are undertaken only when there are reasonable grounds to suggest that there is a contravention of PIPA. To ensure resources are focussed efficiently, the OIPC should only issue orders when an investigation has been initiated by a complaint.

4. **Focus consent on situations that are not reasonably expected, and where individuals have a meaningful choice:**
    A. **Encourage greater transparency:** Meaningful consent requires transparency. Organizations should be required to provide individuals with enough information to make informed decisions. Disclosure requirements should be proportionate and not unnecessarily prescriptive.
    B. **Include an exemption to consent in the Act for legitimate purposes:** PIPA should not require express consent in situations where it is not meaningful or appropriate, such as in the case of personal information being used by organizations for identified legitimate purposes that would meet reasonable expectations.

C. **Add a definition in the Act for de-identified information, and a framework for its continued use without consent:** Given the critical importance of de-identification to security safeguarding efforts and to innovation more broadly, and in order to remove any legal uncertainty, the Act should clarify that consent is not required to de-identify data, or for its collection, use and disclosure, as long as de-identification standards are met.
D. **Maintain current requirements for transfers to third parties for processing:** Current openness and accountability requirements are sufficiently strong in the context of transfers for processing. That said, further clarity is required in the Act regarding the obligations of service providers processing personal information on behalf of clients, including those located abroad.

5. **Ensure an efficient co-regulatory model for privacy:** Privacy is everyone's responsibility. Voluntary codes, certifications and other standards (such as the Canadian Marketing Code of Ethics and Standards) play an important role in supplementing privacy legislation. More specifically, the Government of British Columbia should:
   A. **Encourage self-regulated standards and codes:** Self-regulated standards and codes should be referenced in the Act as tools that can help organizations ensure compliance with PIPA and help demonstrate accountability in the event of an investigation by the OIPC.
   B. **Incentivize formally recognized certifications and codes**: There should be an allowance in the Act for the formal recognition of some certifications and codes by the Government of British Columbia and/or the OIPC, with oversight from select third-party accrediting bodies approved by the Government of British Columbia.

6. **Further assess the impacts of a right to data portability, and pursue a cautionary approach:** The right to data portability creates serious new privacy risks, and its wider impacts on British Columbia's unique economy are not well-understood. Data portability should only be achieved through a phased-in approach that allows for the implementation of sector-specific frameworks developed in consultation with industry.
   A. **Limit the scope of portable data:** Sector frameworks can provide clarity on the scope of data appropriate for the objective of data portability, including limited data related to commercial transactions.
   B. **Protect against fraud and ensure fair accountability:** Strong authentication should be in place, and organizations mandated to port data should have limited liability.

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).

The CMA is the voice of the marketing profession, representing more than 400 corporate, not-for-profit, public, and post-secondary members. We are committed to helping organizations maintain high standards of conduct and transparency through our mandatory Canadian Marketing Code of Ethics & Standards , and our privacy and data protection resources for marketers and consumers. As the recognized longstanding leader in marketing self-regulation, we strive to ensure an environment where consumers are protected and businesses can thrive.

British Columbia'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.

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."

As the Special Committee considers proposing modifications to PIPA, the CMA is pleased to provide the following recommendations to help ensure this important balance:

Recommendations

1. Preserve PIPA's strengths as a balanced, principles-based and technologically neutral law

In our modern digital economy, consumers increasingly expect organizations to deliver the intuitive products and services they want and need. In a recent survey[1] 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. Similarly, a 2018 research study[2], *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.

Many consumers, including younger generations, have adopted a more pragmatic attitude towards their data and realize that data exchange is increasingly fundamental to accessing many of the beneficial services they use and interact with daily. A 2019 research study[3] showed that even when people are

[1] Ipsos, 2019: Canadian Digital Marketing Pulse Survey
[2] Foresight Factory, 2018: Data Privacy Study: What the Canadian Consumer Really Thinks
[3] Barth et al., 2019: Putting the Privacy Paradox to the Test

technically proficient and well-aware of privacy risks, they will consistently choose functionality and relevance.

The ability of organizations to collect, use and disclose personal information is key to providing value to consumers, and to ensuring British Columbia's innovation and competitiveness. It is important that PIPA remain flexible in the face of rapidly evolving technologies, business models and consumer privacy expectations.

While some aspects of PIPA are due for an update, we must recognize that this law has many strengths that have stood the test of time. It is built on solid principles that provide flexibility for specific applications, and its framework is understandable and achievable for non-specialists. Many features of PIPA and other principles-based Canadian laws are regarded to provide materially better privacy outcomes for individuals than newer and more prescriptive laws in other jurisdictions. This includes the EU's GDPR which in many respects remains unproven, and has created a staggering regulatory burden for government and business.

We appreciate that PIPA is being reformed with a view to ensuring reasonable interoperability with privacy frameworks in other jurisdictions. 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 Special Committee 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.

A reformed law must preserve PIPA's strengths as principles-based, technology neutral and not overly prescriptive. The nuances – the respect for context, individuals' expectations and overall emphasis on reasonableness, must remain.

We also encourage the Special Committee to ensure reasonable alignment with the Government of Canada's efforts underway to reform the Personal Information Protection and Electronic Documents Act (PIPEDA), as significant differences between the two laws will lead to further regulatory complexity.

2. 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.

The CMA supports the introduction of mandatory data breach reporting requirements, in line with the requirements under PIPEDA and other provincial privacy laws. 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

3. Strengthen and leverage the current enforcement model

Most Canadian organizations want to protect the trust and privacy interests of the consumers they serve**.** We support enhanced enforcement measures to crack down on bad actors. This can be achieved by strengthening and leveraging the current enforcement model.

The OIPC already has several tools at its disposal to ensure compliance with PIPA, including initiating investigations and audits, educating organizations and individuals about the law, commenting on the

privacy implications of proposed initiatives of organizations, and importantly, investigating and mediating complaints.

One of the most important roles of the OIPC is to investigate and attempt to resolve complaints, make findings, and issue recommendations. The OIPC may initiate investigations, audits and inquiries upon receiving a complaint. It also has the power to issue legally binding orders, giving it more power than its federal counterpart, the Office of the Privacy Commissioner of Canada (OPC).

The OIPC has seen a high level of voluntary compliance from organizations to date. It receives approximately 200 complaints from individuals on an annual basis, and resolves most complaints through mediation. Only a small percentage proceed to inquiry where an adjudicator makes a finding regarding the application of PIPA and issues an order requiring an organization to address the complaint and meet its obligations under PIPA.

The current model permits the OIPC to protect and promote the privacy rights of individuals through positive and proactive engagement with industry associations and organizations seeking guidance on compliance and emerging privacy issues. Organizations are more cautious and less likely to consult in a cooperative way with a regulator that has the direct power to impose monetary penalties against them.

There is also an inevitable degree of uncertainty when applying privacy principles to new technologies. A flexible and collaborative model is required to create conditions under which the OIPC and organizations can work together to find the right solutions.

Through PIPA, the OIPC can constructively engage with businesses to address privacy issues. If voluntary co-operation is not forthcoming, the OIPC may hold a formal inquiry if a complaint does not settle. It can compel testimony, order the production of evidence, enter premises, and if needed, issue and publish binding orders. Ultimately, the Supreme Court of British Columbia can order fines of up to $10,000 for individuals and $100,000 for organizations. Individuals also have a statutory right of action under PIPA and a right to engage in a class action under the Class Proceedings Act. To date, the OIPC has not utilized its ability to refer a matter to the Court for prosecution.

A. **Improve the current model of fining through the Court:** A model through which administrative monetary penalties (AMPs) are issued by the OIPC would further undermine the collaborative model described above. Any new offences should be carefully considered for prosecution by the Court, not the OIPC, making best use of existing provisions and infrastructure. There could be consideration of a greater range of offences for the Court to prosecute. If more general non-compliance issues are included in the list of offences, they should be limited to more egregious cases with intent and gross negligence, such as in the case of intentionally insufficient safeguards or deliberate re-identification**.**

   Government should take a cautionary approach when considering extending the current fine amount, which serves as a real deterrent to individuals and organizations. Fines levied on a “per impacted individual” basis or on a “% of global revenues” basis could lead to a significant aggregate dollar amount out of touch with the actual impact of the offence. The Courts must have 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. We must also recognize the impact of additional deterrents outside of PIPA, including through private claims in tort and contract law.

B. **Implement procedural safeguards for audits and investigations:** Whether a complaint is received or not, the OIPC may initiate investigations and audits to ensure compliance with PIPA if there are reasonable grounds to believe that an organization is not in compliance.

   Additional procedural safeguards should be in place to ensure there is appropriate notice and a clear indication of the focus of audits and investigations, and to ensure all are undertaken based

on the current standard of reasonable grounds that there is a contravention of PIPA. Any proposal to expand grounds for investigation should include expanded grounds for not investigating, or for discontinuing the investigation of complaints, such as if an organization is in adherence to a formally recognized code or certification (see section below).

The Special Committee should not consider an allowance in the Act for the OIPC to issue an order where an investigation has been initiated without a complaint. This level of power would further threaten the positive and constructive engagement needed between the OIPC and organizations, the majority of whom are working hard to do the right thing.

The OIPC's enforcement response should always be triggered at the conclusion of an investigation, and should follow a staged approach, issuing warnings before orders in order to give well-intentioned companies an opportunity to rectify the issues at hand. Severe enforcement tools should be used only when lesser tools have been ineffective or the potential harm is too great. In all cases, there must be an appeal process.

4. Focus consent on situations that are not reasonably expected, and where individuals have a meaningful choice

We welcome the opportunity that this review provides to tweak PIPA's consent model to better serve consumers. As business models evolve in step with technological advancement, including big data analytics and IoT, it is more important than ever for organizations to ensure that they are obtaining meaningful consent.

A strength of the current consent model 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 the context and the reasonable expectations of the individual. And although we have learned not to place too much emphasis on consent alone, it is a central underpinning of PIPA that, paired with other obligations, helps empower individuals.

A. Encourage greater transparency

Meaningful consent cannot be achieved without transparency. By being open and transparent, organizations breathe life into the consent requirement, enabling individuals to make more informed choices about their personal information. The CMA Guide to Transparency for Consumers helps organizations provide clear, user-friendly information to consumers about how their personal information is collected, used and shared.

Organizations should be required to provide individuals with the information they need to make informed decisions, including on the intended use of the information and the nature of third parties with whom information will be shared. However, disclosure requirements that are too prescriptive, such as requiring organizations to include specific and standardized information or language in their privacy notices, 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, taking into account the context, target audience and actual risks.

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

The Act should not have a specific definition of, and protections for, "sensitive information"**.** Under PIPA, a contextual analysis is required prior to making a determination about sensitivity of data, as well as a determination of the scope of harm. These determinations must be based on the facts of the circumstances, so organizations avoid broad statements of acceptable or unacceptable use in their privacy policies or notices. While certain types of data, such as financial or health information, may at first glance seem to be sensitive, this data could be used in a way that could make it not as sensitive as initially envisioned. In the same way, fairly routine personal information could be sensitive in certain contexts.

B. Consider an exemption to consent for legitimate purposes

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

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. This is an important consideration as British Columbia considers a reasonable degree of interoperability with the GDPR, a law which includes other bases of processing besides consent such as "legitimate business interests" and "performance of a contract" – uses that today are covered through various forms of consent and exemptions to consent in PIPA.

PIPA should not require express consent in situations where it is not meaningful or appropriate, such as in the case of personal information being used by organizations for identified legitimate purposes that would meet reasonable expectations.

PIPA already allows for personal information to be used without consent in specific circumstances defined under section 12 (1). We recommend an exemption be added for situations in which personal information is used for legitimate purposes**,** as long as these purposes are:

- **Demonstrably consistent** with the requirement under PIPA under subsection 4 (1) that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances), and;
- **Explicitly specified** before the information is used. Organizations relying on this exemption must be transparent about their legitimate purposes by outlining them in a privacy policy or other method that is readily available to individuals.

The Act should allow, if necessary, 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. This approach works within the current PIPA framework, providing additional flexibility together with additional accountability, and regulation-making power if needed.

If a definition is needed for "legitimate purposes", it should cover the following areas as a minimum:

- The process of de-identifying personal information for an organization's own use (see Section 4B below).
- Transfers of personal information to a third party for the purposes of processing on behalf of the organization (see Section 4C below).
- Any legitimate purposes included in a formally recognized code or certification (see Section 5B below).

The processing of personal information for legitimate purposes can already be done using implicit consent. This should continue to be the case for the most obvious uses, for example, those necessary to deliver the products and services that a consumer requests.

The reason for introducing an exemption to consent for legitimate purposes is to provide greater certainty for business, but to also ensure a greater level of accountability. Organizations could rely on the exemption in less obvious but equally non-harmful uses, such as big data analytics. Because organizations would be relying on an exemption to consent, they would have to be able to demonstrate that the legitimate purpose in question is demonstrably consistent with s. 4(1), thereby introducing a greater level of accountability.

This would prevent organizations from trying to rely on this exemption as a “catch all”. It would place responsibility on organizations to justify their processing and outline it clearly in their privacy policies and through the performance of internal assessments. That is how an organization “demonstrates” that it is consistent. In effect, it requires an assessment based on the specific context and circumstances to demonstrate that processing is appropriate and reasonable.

C. Add a definition of de-identified information to the Act, and a framework for its continued use without consent

Data de-identification provides a significant opportunity for organizations to protect individual privacy, while permitting the smart use of data. The CMA supports adding a definition of de-identified information to the Act.

Given the critical importance of de-identification to security safeguarding efforts and to innovation more broadly, and in order to remove any legal uncertainty, the Act should clarify that consent is not required to de-identify data, or for its collection, use and disclosure, as long as de-identification standards are met.

At present, the meaning and methodology of de-identification varies across organizations. 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. Consistent with the reasonable safeguards principle, the standard of de-identification and ongoing monitoring should fit the purpose/activity. The context and data-use activity is more relevant than the type of data.

The Act should acknowledge these standards, and should include benchmarks for technical and administrative procedures and monitoring, as well as proper risk assessments and protocols. Accountability chains are important to guard against the technical risk of reidentification. 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.

Robust de-identification, in and of itself, poses no risk of harm and has no negative impact on the individual to whom the personal information originally related. Not only is this a useful

safeguarding technique, but de-identification is also one of the most privacy-protective mechanisms available for organizations to engage in data analytics and innovation in the digital economy.

As technology evolves, the requirements for robust de-identification must also evolve to keep up with the times. This may mean an 'evergreen' approach to OIPC guidance, and other formalized standards around deidentification. These standards should be developed in consultation with industry, and could result in a formal certification involving a third-party accreditor approved by the Government of British Columbia (see section 5 below).

D. Maintain current requirements for transfers to third parties for processing

We recommend the government preserve the current model, which does not require additional consent for third-party transfers, and provides adequate privacy protection in the context of third-party data flows, including across borders.

Any requirement for additional consent would contribute to consumer consent fatigue, disruptions in service for consumers, significant operational consequences for organizations relying on third-party data processing (including non-profits and others providing critical services to British Columbians), and a lack of interoperability with other privacy frameworks. Given the nature of data flows, consent is not the most effective form of responsible data governance and it offers no meaningful additional privacy protection. In many cases, consent would be illusory as the requirement would not mean individuals have any choice at all but to walk away. A customer who is very interested in a product or service is not likely to make that choice. In fact, it works against our common goal of obtaining meaningful consent to the benefit of consumers.

Current openness and accountability requirements, including providing notice and using contractual or other means to provide a comparable level of privacy protection when data is transferred, are sufficiently strong in the context of transfers for processing. A future law need not require demonstrable accountability by giving a public authority, such as the OIPC, additional powers to approve standard contractual clauses before they are implemented and, once they are adopted, proactively review their implementation. Issues should be reviewed only upon complaint to the OIPC. The proposed drafting of such clauses, similar to the GDPR's standard contractual clauses, would depart from PIPA's balanced approach.

Further clarity is required in the Act regarding the obligations of service providers processing personal information on behalf of clients. The AggregateIQ decision by the OIPC and OPC diverges from the common working assumption that British Columbian companies that collect, use and disclose personal information on behalf of clients are subject to the laws that govern their clients' activities. The recent decision creates an obligation on British Columbian processors to ascertain whether data controllers obtained valid consent under PIPA even when those controllers are located outside of Canada and dealing with the information of non-Canadians (and in this case, used a legitimate grounds for processing besides consent under the GDPR). Such an obligation would create significant barriers for businesses to compete at home and abroad. There is no express legal basis for this decision under the current law, and clarification under a reformed law is critical.

5. Ensure an effective co-regulatory model for privacy

All sectors have a role to play to protect the privacy of British Columbians. 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.

Standards could be either self-regulated or formally recognized by government, as outlined below. 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.

A. Encourage self-regulated standards and codes

Self-regulated standards and codes should be referenced in the Act as tools that can help organizations ensure compliance with PIPA and help demonstrate accountability in the event of an investigation by the OIPC. 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 & Standards is a comprehensive code that establishes and promotes high standards for the conduct of marketing in Canada 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 OIPC should investigate and audit only where complaints arise that haven't been resolved internally, or where there isn't an adequate internal complaints process in place. When an organization cannot demonstrate compliance, it would risk falling under general compliance rules enforced by the OIPC.

B. Incentivize formally recognized certifications and codes

The Act should further incentivize the use of certifications and codes as tools for privacy compliance and accountability through an allowance in the Act for the formal recognition of some certifications and codes by the Government of British Columbia and/or the OIPC, with oversight from select third-party accrediting bodies approved by the Government of British Columbia.

The Act should 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 should be informed by adequate consultation and could 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 could be considered to meet the requirements for a set time period (e.g., three years), after which its adherence could be renewed if the conditions and requirements are still met. Collaboration should occur between the provincial and federal governments in this regard. The Standards Council of Canada has a thorough development and review process for accreditation standards; its role should be leveraged and maximized.

The OIPC 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 OIPC investigation, or Court prosecution. The OIPC 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 OIPC where an organization's compliance is revoked for non-compliance.

6. Further assess the impacts of a right to data portability, and pursue a cautionary approach

As the Special Committee examines the merits of certain aspects of GDPR in the British Columbia context, including conferring a new individual right to data portability, we encourage caution.

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 are not well-understood, and more research must be done to understand its effects.

To ensure that this new right does not create unintended consequences that hamper British Columbia's economic well-being, other bodies, such as the federal Competition Bureau, should have a significant role in the research and development of this concept in a Canadian context. This is more than a privacy issue, and the corresponding reform of other statutes, including at the federal level, may be necessary.

For the right to data portability to be effective, it must be meaningful for consumers and not overly burdensome or costly for organizations (and by extension, consumers). If the right to data portability is ultimately pursued, it would require 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 required.

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 OIPC should be involved in the enforcement of such frameworks, with the OIPC overseeing issues related only to privacy compliance.

Other important considerations include:

A. Limit the scope of portable data

Providing data directly to an individual is an extension of the current right to access under PIPA, 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. For organization-to-organization transfers, 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, about a third party (e.g. an individual's contact list), or not considered personal information. This includes derived data (insights, observed data) and de-identified data. Some of the exempted data would continue to be subject to the normal access request process, such as, for example, call notes and complaints. Sector frameworks could 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 would be 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 should 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. Regulatory frameworks will need to be reviewed on a periodic basis to reflect technological and other advancements. As advancements occur, the scope of ported data could evolve accordingly.

Consideration should be given to ensuring that these rules do not create barriers for SMEs, working against the original intent of greater competition.

B. Protect against fraud and ensure fair accountability

When organizations are obligated to respond to individuals' requests for their own data, strong authentication must be in place to guard against fraudulent requests. Organization-to-organization mobility must be conditional on the request being made by the individual (and not just the third-party organization), and on there being an adequate sector-specific regulatory framework in place. Bulk requests from third parties must be prohibited. In particular, the Act should ensure organizations cannot automate requests, or attempt to bury consent for the sharing or obtaining of ported information in contracts.

The introduction of the right to data portability will attract third-party providers that must be properly assessed, especially if they operate internationally and can potentially evade OIPC enforcement. Parties receiving ported information must be accountable to consumers, and should be prepared to adequately protect their personal information.

An exclusion of liability must be in place when an organization is mandated to port data to a third party that it wouldn't choose to port to. The responsibilities of the originating organization must be limited to confirming that the request is from the individual (i.e. not fraudulent) and the safe transfer of 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. Additionally, organizations transferring ported data should not be responsible for educating recipients on their responsibilities.

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 in Canada. We serve more than 400 corporate, not-for-profit, public and post-secondary members, including Canada's most prestigious brands. 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.