Response to the Government of Ontario's Consultation on Strengthening Privacy Protections in Ontario

October 2020

Executive Summary

As the voice of Canada's marketing profession, the Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Government of Ontario's consultation on strengthening privacy protections in Ontario.

We strongly urge Ontario to continue to rely on the federal Personal Information Protection and Electronic Documents Act (PIPEDA) for privacy protection, with new provincial legislation focusing on addressing sectors and activities that a reformed federal law will not cover.

As the backbone of economic growth and stability for Canada, Ontario's business sector needs clear and consistent privacy regulation to support innovation, trade and competitiveness, and to avoid service disruptions and confusion for consumers. The creation of a new private sector privacy framework for Ontario would create significant additional costs for government, as well as regulatory complexity for organizations as they adjust to a new law, with presumably one set of rules applying to Ontario organizations engaging in intraprovincial activities and another for those engaging in interprovincial and international activities.

Provincial legislation should be considered only after a reformed PIPEDA is announced, focusing on enhancing privacy protections for Ontarians where the sector or subject matter is not covered by the proposed changes to PIPEDA.

Feedback on Discussion Paper: To the extent that the Government of Ontario moves forward with private sector privacy legislation – ideally limited in scope as described above, and given the importance of the questions raised in the discussion paper on private sector privacy reform, we are pleased to submit the following comments:

1. **Alignment with other Canadian privacy frameworks is critical to prevent disruptions for organizations and consumers, and complications for trade and investment**. There must be a mechanism for alignment between the federal, provincial and territorial governments in order to prevent the damaging fragmentation of privacy frameworks, and its impact on the data-based integrated industries that operate across provinces, the country and internationally.
2. **Any new privacy law must be principles-based and proportionate to the privacy objectives to be achieved,** providing flexibility in the face of rapidly evolving technologies, business models and consumer privacy expectations.
3. **Transparency requirements must be flexible, supporting transparency that is useful to individuals with requirements that are proportionate and sensitive to the context.** It is important that requirements are not too prescriptive, allowing organizations to determine how best to communicate with individuals in an understandable way.
4. **The type of consent required must be based on an assessment of relevant factors, and exemptions to consent should be implemented.** Organizations must be empowered to choose the type of consent appropriate (express or implied), depending on the sensitivity of the information and the reasonable expectations of the individual, both of which will depend on context. The government should also explore an exemption to consent for "legitimate purposes", enabling organizations to justify their legitimate purposes and identify them to individuals.
5. **The right to data portability must be delayed until its wider impacts are understood.** Data portability creates serious new risks related to fraud, privacy and security, and it should only be achieved through a phased-in approach that allows for the implementation of sector-specific frameworks.
6. **Enforcement measures must incentivize compliance without having a chilling impact on business and investment in Ontario.** The most effective lever for compliance is a proactive and collaborative relationship between the IPC and industry. The IPC's enforcement response should

follow a staged approach in order to give well-intentioned companies an opportunity to rectify the issues at hand.

7. **Standards for de-identified and anonymized information must be established to support a framework for its continued use without consent:** Privacy law should permit the collection, use and disclosure of de-identified information without consent for all reasonable purposes, as long as certain standards are developed and met.
8. **More analysis is required on the benefit of data trusts for privacy-protective data sharing.** The government should consult with stakeholders interested in the collective use of de-identified data for specific purposes. Industries and sectors should contribute to the development of standards appropriate and proportionate to the personal information involved and the reasonable expectations of individuals.
9. **Privacy codes and certifications must be leveraged 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 encourage self-regulated certifications and codes as tools for privacy compliance and accountability, and should further incentivize their use by selecting some for formal recognition.

The CMA looks forward to continued conversations with the Government of Ontario on these important topics.

Introduction and Context

The Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Government of Ontario's consultation on strengthening privacy protections in Ontario.

The CMA is the voice of the marketing profession in Canada, representing more than 400 corporate, not-for-profit, public, and post-secondary members, many of whom are headquartered in Ontario. 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 businesses can thrive and consumers are protected.

Ontario'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.

We appreciate the Government of Ontario's dual goal of protecting the personal information of individual Ontarians, while ensuring that any new privacy protections do not pose an unnecessary burden on businesses or inhibit the growth and prosperity of Ontario's innovation ecosystem.

We strongly urge Ontario to continue to rely on the federal Personal Information Protection and Electronic Documents Act (PIPEDA) for privacy protection, with new provincial legislation serving to address sectors and activities a reformed federal law won't cover.

Currently, the collection, use and disclosure of personal information in the course of commercial activities across Ontario is governed by the federal Personal Information Protection and Electronic Documents Act (PIPEDA), which is being reformed. There is great merit in maintaining this approach, helping to ensure a single overarching privacy framework to the extent possible.

The creation of a new private sector privacy framework for Ontario would create significant additional costs for government, as well as regulatory complexity for organizations as they adjust to a new law, with presumably one set of rules applying to Ontario organizations engaging in intraprovincial activities and another for those engaging in interprovincial and international activities.

Consistent and coherent privacy regulation across the country provides certainty for consumers, organizations and government. It is also the most cost-effective regulatory approach, particularly given the current demands of the pandemic on the provincial budget.

We understand that there are some limitations on PIPEDA's application to certain sectors and activities in Ontario, including employees in provincially regulated sectors, political parties and the non-commercial activities of non-profits and charities.

Once PIPEDA is reformed, a provincial framework should only address privacy protections for Ontarians where the sector or subject matter will not be covered federally. This will prevent the creation of a costly and duplicative overarching privacy framework for Ontario.

Feedback on Discussion Paper

As noted above, private sector privacy legislation enacted by the Government of Ontario must be limited in scope as described above. However, given the importance of the questions raised in Government's discussion paper on private sector privacy reform, we are pleased to submit the following comments.

1. Alignment with other Canadian privacy frameworks is critical to prevent disruptions for organizations and consumers, and complications for trade and investment

There must be a mechanism for alignment between the federal, provincial and territorial governments in order to prevent the damaging fragmentation of privacy frameworks, and the negative impacts this would have 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 and consumers, complicate conditions for trade, and reduce Ontario's attractiveness as a business destination.

2. Any new privacy law must be flexible, principles-based and proportionate to the privacy objectives to be achieved

The ability of organizations to collect, use and disclose personal information is key to providing value to consumers, and to ensuring Ontario's innovation and competitiveness.

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. Consumers are expecting and demanding that contact with businesses is relevant, timely and of value to them. The smart use of data is central to the delivery of that promise. Without sufficient tailoring of marketing and servicing efforts, issues arise related to inefficiency, spamming and more.

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.

Privacy law should be based on sound principles that are flexible enough to account for context, and 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.

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. It should include a clear purpose

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

clause ensuring that the law be interpreted in a proportionate and reasonable manner based on the circumstances.

Ontario's approach should be compatible with jurisdictions that have a similar, principles-based approach to privacy. 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 new privacy framework should not be so onerous that it cannot be effectively implemented and is not well understood by non-specialists.

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

3. Transparency requirements must be flexible, supporting transparency that is useful to individuals with requirements that are proportionate and sensitive to the context

Increased transparency by organizations builds trust and enables consumers to make more informed choices about their personal information.

The CMA has long been a proponent of transparency. 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.

The CMA supports the requirement for organizations to provide clear information using plain language about the use of personal information: to state what personal information is collected, how it is collected, how it is used, and with which third parties the information will be shared.

To assist individuals in better understanding how decisions are made about them, we also support a 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 it does not require organizations to reveal any confidential or proprietary commercial information, algorithms or procedures.

It is important that requirements are not too prescriptive (e.g. through a requirement for specific and standardized language in privacy notices). Given the great 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.

4. The type of consent required must be based on an assessment of relevant factors, and exemptions to consent should be implemented

An overreliance on express consent in all instances contributes to "consent fatigue", causing individuals to be less likely to carefully review privacy notices, make informed decisions, and exercise choices. This 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. This will often result 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.

The discussion paper proposes a requirement for express consent for any collection, use or disclosure of personal information, unless an exception to consent has been established for a specific circumstance.

This leaves out the important role of implied consent. A longstanding strength of Canadian privacy frameworks is that organizations have the operational choice of whether to seek express or implied 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).

In addition to ensuring organizations are empowered to make the best choice on the type of consent appropriate, the government should explore exemptions to consent, such as 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 identified legitimate purposes that take into account the reasonable expectations of the individual under the circumstances.

If an exemption to consent for "legitimate purposes" was implemented, organizations relying on this exemption must be required to 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 law 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.

Organizations relying on this exemption would perform internal assessments based on the specific context and circumstances to demonstrate that processing is appropriate and reasonable..

"Legitimate purposes" should cover the following areas at a minimum:

- The process of de-identifying or anonymizing data, or for its collection, use and disclosure by an organization, if certain de-identification and anonymization standards are met (see section 7 below).
- Transfers of personal information to a third party for the purposes of processing on behalf of the organization.
- Any legitimate purposes included in a formally recognized code or certification (see section 9 below).

The processing of personal information for legitimate purposes can already be done using implied consent. This should continue to be the case for the most obvious uses, such as 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 the requirement that an organization may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Finally, the discussion paper proposes that individuals should be permitted to revoke consent at any time. There must be an acknowledgment that some processing is integral to the provision of the goods or services that the consumers requests. For example, in the case of delivering cellular services, an individual cannot revoke consent for location tracking, because the service would no longer function if the cell towers could not identify the phone's location. If the collection, use, and disclosure of personal information is required to perform a contract, or retention of information is necessary for a regulatory or legal requirement, it must be clear that consumers cannot revoke consent.

5. The right to data portability must be delayed until its wider impacts are understood

The primary objective of data portability is to encourage competition in the marketplace. Although it may be 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 a data portability right in Ontario pending further study of its non-privacy impacts.

To ensure that this new right does not create unintended consequences that hamper Ontario'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 Ontario 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 practicalities and risks in each affected sector and could be implemented through regulation. These frameworks must consider important economic, technical, authentication, security and operational issues. Once these frameworks are set, organizations will have to make considerable IT investments and updates. There must be adequate time for implementation. A reasonable timeframe would be 2 years, as organizations have specific IT release windows and planning calendars are usually set a minimum of 12 months in advance.

   Other regulators beyond the Information and Privacy Commissioner of Ontario (IPC) should be involved in the enforcement of such frameworks, with the IPC overseeing issues related only to privacy compliance.

B. **Limits on the scope of ported data:** The current right to access under most privacy laws already goes a long way to support consumer control; individuals 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 portability must be done at the request of the individual, but the right to data portability 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 and certain data (e.g. transactions) created through interaction with products and services. It should exclude other types of data that may be proprietary, derived or not considered personal information (e.g. de-identified data).

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.

6. Enforcement measures must incentivize compliance without having a chilling impact on business and investment in Ontario

Reputable organizations want to protect the privacy of their customers. They do not want to jeopardize consumer trust by misusing or mistreating personal information.

Ontario's enforcement model must provide sufficient incentive to deter businesses that might not otherwise comply without having a chilling effect on businesses and their ability to serve consumers well.

A flexible and collaborative model is required to create conditions under which the IPC and organizations can work together to find appropriate solutions. This is particularly critical during the COVID-19 era, when organizations have been expected to digitize their business models faster than ever before.

Enforcement measures must be proportionate to the privacy goals to be achieved. We appreciate the government's acknowledgment that there are variety of tools that may be employed to help ensure compliance besides penalties.

We support an expanded mandate for the IPC to provide advice and guidance to organizations, particularly SMEs. Well-intentioned organizations would benefit from seeking non-binding, advance opinions and guidance to gain certainty and predictability, without fear of being subject to investigations or undue enforcement. The CMA would welcome the opportunity to engage in consultations to inform innovative strategies around education, research, guidance, and advisory services as well as regulatory sandboxes

Both the federal and provincial privacy commissioners have seen a high level of voluntary compliance from organizations to date, resolving most complaints through mediation. That said, we recognize the need for enforcement measures to crack down on bad actors if voluntary co-operation is not forthcoming.

Enabling the IPC to investigate complaints and issue binding orders and public reports about an organization's privacy practices will go a long way in ensuring compliance. However, 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.

A model through which administrative monetary penalties (AMPs) are issued by the IPC would undermine the collaborative model needed. Any new offences should be carefully considered for prosecution by the courts, not the IPC, making best use of existing provisions and infrastructure.

If the government decides to grant the IPC authority to impose AMPs, more thought must be given to the quantum of fines, given the real risk of fines having a chilling impact on Ontario's business and innovation climate. Fines levied on a "% of global revenues" basis would lead to fines out of touch with the actual impact of most offences, failing to take into account the circumstances of each case. For example, in cases where organizations that have taken all reasonable steps to protect personal data are targets of a malicious act that results in a breach, it is important to consider that the companies themselves are victims too.

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, and rigorous procedural safeguards must be put in place to ensure fairness.

If an unduly strict fining structure is put in place, some organizations will find it necessary to assess the risks, costs and benefits of continuing to do business in Ontario, particularly if it makes up a small part of their operations and they risk being fined a percentage of global revenues.

Investigations, audits and inquiries must be initiated only upon receiving a complaint. The IPC's enforcement response should 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 adequate appeal process.

Finally, there must be a provision to ensure that organizations subject to the law do not face "double jeopardy", facing penalization actions under both the federal privacy law and any new Ontario law. It is critical for privacy law to enshrine a requirement that privacy commissioners at both levels work together on joint investigations.

7. Standards for de-identified and anonymized information must be established to support a framework for its continued use without consent

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. It is important that a definition of de-identified information be included in privacy law, as well as a framework for its continued use without consent.

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

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 or anonymize personal information and mitigate the risk of re-identification. Standards 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 law 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.

There must also be alignment with standards being developed at the federal level and in other provinces. Differing requirements could cause significant issues for organizations leveraging certain data sets, such as de-identified data being used for geolocation-based insights across several jurisdictions.

As technology evolves, the requirements for robust de-identification and anonymization must also evolve to keep up with the times. This may mean an 'evergreen' approach to IPC guidance, and other formalized standards around deidentification and anonymization. These standards should be developed in consultation with industry, and could result in a formal certification involving a third-party accreditor (see section 9 below). The CMA would be pleased to lend its expertise to the development of standards.

8. More analysis is required on the benefit of data trusts for privacy-protective data sharing

We agree that data silos can hinder innovation, reducing the scope of insights available to benefit Ontarians. However, the concept of data trusts requires further analysis to ensure it represent the best model for data stewardship in the public interest.

Establishing guidelines, principles and standards for the use of these trusts will be important. It is important that government and industry work together to identify possible opportunities, and consider how both personal and deidentified personal information can be shared among different organizations to drive innovation for the public good, or for other common interests.

The government should consult with stakeholders interested in the collective use of de-identified data for specific purposes. Industries and sectors should contribute to the development of standards appropriate and proportionate to the personal information involved and the reasonable expectations of individuals.

In the marketing context, the gradual phasing out of third-party cookies has led to an interest in gaining consumer insights in a more privacy-protective and anonymized way. There is merit in exploring the possibility of combining de-identified data sets among organizations to inform marketing efforts, helping to reduce the use of third-party web tracking. In that sense, data trusts may provide an opportunity for the marketing community to explore more privacy protective ways of combining data to understand, reach and serve consumers. It would also help alleviate concerns that only a few large players have access to the majority of consumer insights, allowing smaller providers to share insights amongst each other.

9. Privacy codes and certifications must be leveraged to ensure regulatory efficiency

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

As the Government of Ontario considers new privacy legislation, it must consider a role for both self-regulated and formally recognized codes and certifications, 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. Self-regulated standards and codes: Self-regulated standards and codes should be referenced in privacy law as tools that can help organizations ensure compliance and demonstrate accountability in the event of an investigation by the IPC.

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 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. In addition, failure to adhere has a significant reputational impact, which can be damaging to customer trust and loyalty and can directly impact the bottom line.

B. Formally recognized certifications and codes: Privacy law should further incentivize compliance by allowing for the formal recognition of some certifications and codes based on approval by the Government of Ontario or the IPC, with oversight from select third-party accrediting bodies.

The law 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 law only or a broad assessment of privacy (for example for a sector or industry).

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 IPC 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 IPC 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 IPC where an organization's compliance is revoked for non-compliance.

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.