CANADIAN MARKETING ASSOCIATION
CMA

145 Wellington Street West, Suite 203, Toronto, Ontario, M5J 1H8
416.391.2362 ● theCMA.ca

Submission to the Office of the Privacy Commissioner of Canada by the Canadian Marketing Association on the Exploratory Consultation for a Children's Privacy Code

August 2025

Introduction

The Canadian Marketing Association (CMA) is the voice of marketing in Canada, bringing professionals together to share insights, champion shared interests, and shape the future of the industry. We represent virtually all of Canada's major business sectors, and all marketing disciplines, channels and technologies. Our Consumer Centre helps Canadians better understand their rights and obligations.

We appreciate the opportunity to provide this submission in response to the Office of the Privacy Commissioner of Canada's (OPC) exploratory consultation regarding the development of a children's privacy code ("an OPC Code").

The CMA unequivocally supports the protection of children. For decades, we have been the leader in setting standards for marketing to young people, through the Canadian Marketing Code of Ethics & Standards (the "CMA Code"). The CMA Code included standards in this area as far back as the 1990s, and we enhanced these in 1998 with new standards that took effect the following year. Our 1998 amendments were adopted by the International Federation of Direct Marketing Associations, setting a global standard. In 2023, we enhanced the CMA Code once again by incorporating principles from the UK Children's Code. And we were one of the most active associations advocating for adoption of the Consumer Privacy Protection Act in Bill C-27.

Most Canadian organizations recognize that having strong privacy and data protection practices provides a business with a competitive advantage, also helping to bolster customer retention. More than 92% of Canadian businesses consider the protection of customers' personal information to be important to their business. CMA member organizations work hard to protect and respect the privacy interests of the individuals they serve, providing appropriate security safeguards and protecting customers' personal information.

This submission sets out the CMA's position in response to the OPC's exploratory consultation questions, offering a risk based, practical framework that protects young Canadians in a manner that upholds key privacy principles, such as data minimization and proportionality. Throughout our response, we refer to individuals under 13 as 'children', and those from age 13 to the age of majority in their province as 'teens'. 'Young people' or 'minors' refers to everyone under the age of majority (i.e., children and teens). Crucially, in the current economic environment, it is vital that any new code avoids imposing undue regulatory burdens that could stifle innovation and create barriers to participation for both businesses and young people.

Our submission is informed by our expertise in marketing, with a focus on the practical application of an OPC Code to these activities.

Application of a Children's Privacy Code

Consultation Questions:
1. Should a children's privacy code apply differently to sites exclusively directed at children and those directed at a broad audience that includes children? Which factors should be considered when determining the likelihood of children accessing a service? How can this assessment be done in a privacy-protective manner?
2. Should a children's privacy code only apply when certain risks or harms are possible due to access to or use of the site - and if so, which ones?
3. How should a "significant number of children" be defined? Should this threshold be adjusted or removed?

CMA Response:

Many organizations do not know whether a particular customer is a minor, nor do they need to know or have a strong privacy rationale to treat the data differently.

For example:

- A telco has no way of knowing whether any of the phones purchased by an adult as part of a family plan will be used by minors or, which family member will be using which phone, and the company has no way of distinguishing minors' data versus other data. Location data is required to connect a wireless device to the nearest cell tower and deliver service, but the provider will not know if that location data belongs to a minor.
- A mapping app gathers location to provide accurate navigation information, but it does not know if that location data is gathered from minors.
- A sports team's website provides player and team stats, player biographies, team schedules, video highlights and online stores. This content is intended to drive fan loyalty and promote the team and is intended for a general audience (rather than specifically targeting minors).
- A teenager researches guitars on a music store's website before making a purchase with their savings, or buys a gift for their parent from a major retailer. There are thousands of similar services and websites that collect and use innocuous, non-sensitive data. These service providers have no need or interest in knowing which of their visitors or users may be minors. In these cases, no changes to data handling or privacy practices are warranted solely because some users or website visitors may be minors.

A regulatory framework that fails to distinguish between these low-risk activities and high-risk data processing would be a blunt instrument, imposing significant operational and financial burdens on organizations, particularly the small and medium-sized enterprises (SMEs) that are the backbone of the Canadian economy. Forcing all service providers and websites to implement age-assurance mechanisms would compel them to collect age or age-related information from all users, which is counter to the foundational privacy principle of data minimization. Such a mandate would represent a cure far worse than the disease, transforming millions of innocuous interactions into transactions where personal data must be collected, processed, and stored, thereby creating new and unnecessary privacy risks for all users, including young people.

Furthermore, in addition to a right to privacy, the United Nations Convention on the Rights of the Child (UNCRC) calls for children under 18 to have the right of access to information from diverse sources that promotes their well-being. Overly broad rules that discourage general-

audience sites from providing content would inadvertently create barriers to this right. For these reasons, the focus of an OPC Code should be squarely on websites and activities that present a material risk of harm, not simply on the age of the user without considering the context. The true risk lies not in a minor visiting a website to check hockey scores but in specific, identifiable harms, such as exposing children to sites with age-inappropriate content, or age-targeted advertising or the unnecessary collection of sensitive information on services directed at children.

An effective, modern, and proportionate OPC Code must be a risk-based, tiered framework that applies to:

- Organizations whose business is directed at minors,
- Organizations that know, or should reasonably know, that they are processing minors' personal information (e.g., toy manufacturers, children's educational platforms), and
- Organizations that offer products or services intended for adults only.

It is also critical that an OPC Code clarify the distinction between the *purpose* of age collection versus the act of collection itself. In many sectors, verifying a user's age is not a discretionary choice but a foundational requirement for legal compliance, safety, or core service delivery. In these contexts, the collection of age is not the high-risk activity an OPC Code should be designed to prevent, but rather an integral component of providing a service lawfully and responsibly.

For example:

- An airline has both a regulatory obligation to verify a passenger's identity and a duty of care to provide special support to an unaccompanied minor.
- Financial and insurance sectors rely on age information to deliver services and manage risk. Banks require a date of birth to open an account, property and casualty insurers must know the age of a driver, and life insurers need to identify the status of beneficiaries.

Once an organization’s tier has been identified, a final assessment of material risk should be undertaken. This assessment must recognize that the necessary collection of age (or other information that may be considered sensitive) for legal, safety, or core service delivery purposes must be evaluated in context. If the purpose of the collection is paramount and necessary for these legitimate reasons, it should not be treated as the same type of high-risk activity that an OPC Code is meant to prohibit. Where no material risk of harm is present, an OPC Code should not apply. This ensures that obligations and standards set by the OPC are targeted, proportionate, and avoid placing undue burdens on organizations that only incidentally process the data of minors.

Regulators should encourage the adoption of centralized and privacy-protective methods for age assurance. For example, encouraging the adoption of app store age collection and parental approval before a minor downloads an application.

This risk-based approach aligns with established international best practices, including the approach taken by the Children's Online Privacy Protection Act (COPPA) in the US and modern privacy laws in California and the EU, ensuring Canada's framework is both effective and harmonized.

Finally, an OPC Code should allow for different treatment of mature minors, who bear many of the responsibilities and enjoy many of the privileges of adulthood. This approach aligns with the approach taken by the Children's Online Privacy Protection Act in the US,[1] as well as by privacy laws in California[2] and the EU,[3] and would avoid targeting organizations that may only incidentally and unknowingly process the data of minors.
We recommend developing clear, practical examples to help organizations determine when they fall under the scope of an OPC Code.

We would also appreciate clarification on the consultation paper's reference to "sites or services." We would like to confirm that the scope of an OPC Code would be to focus on online services delivered by a website or an app.

Enabling the Exercise of Children's Privacy Rights

Consultation Question:
1.What measures should be put in place to ensure that a child has the capacity to provide consent? When should consent be sought from parents/guardians instead of a child? How can organizations confirm the relationship of the parent/guardian to a child?
2.How should an organization present information to children of different developmental age ranges to ensure that they reasonably understand how their information is being collected, used or disclosed and can meaningfully consent to practices?
3.What are examples of "simple" means by which organizations could allow children and or parents/guardians to easily access, correct, or withdraw consent for the use of the child's personal information? How might organizations address withdrawing consent which they, or their parents/guardians, have previously provided?

CMA Response:

We recommend that an OPC Code include relevant features from the CMA Code, which recognizes that marketing to children and teenagers imposes a special responsibility on marketers. In December 2023, we substantially revised the provisions related to young people in the CMA Code, as described in the introduction to this submission, to better align with the UK Children's Code.

The CMA Code defines children as being under the age of 13, and teens as being 13 to the age of majority in their province.

The CMA Code provides a practical and proportionate model that requires marketers to take the age and capacity of minors into account. All communications and online services directed to young people, including legal terms, must be concise, prominent and in clear language appropriate to the age of the young person. This tiered approach protects children effectively

[1] See Children's Online Privacy Protection Rule, 16 CFR Part 312. COPPA applies only to operators of websites and online services that are directed to children, or that have actual knowledge that they are collecting or maintaining the personal information of a child.
[2] The California Consumer Privacy Act of 2018, California Civil Code § 1798.120, requires consent for the sale of the personal information of consumers under 16 years of age (including parental consent, for children under the age of 13). These restrictions apply only on business with actual knowledge that they sell the personal information of consumers under the age of 16, or that wilfully disregard the age of a consumer.
[3] Article 8 of the General Data Protection Regulation (Regulation (EU) 2016/679) requires parental consent for the processing of the personal information of a minor under 16 years of age, with respect to the offering of information society services directly to a child.

without stifling their ability to participate in the digital world or creating unworkable compliance hurdles for organizations.

Provisions in the CMA Code include:

- Marketers should assess and mitigate risks to young people from data processing, and they must not use young people's personal information in ways that could be detrimental to their well-being, or that go against industry codes, regulatory prohibitions or guidance.
- Any consent framework must consider risk of harm as a key determining factor. The CMA Code allows marketers to communicate with teenagers based on the type of information and the teenager's age. Specifically, for children under 13 years of age, any collection, use or disclosure of personal information requires opt-in consent from a parent or guardian.
- For ages 13-15, the teen can consent to providing their contact information. However, parental consent is required for any other information, as well as for the disclosure of contact information to third parties.
- Teens aged 16 or older can consent to the collection, use, and disclosure of their personal information.
- Parents or guardians maintain the authority to withdraw consent that they previously granted to minors under 18 years of age, including those who are 16 and above.

The CMA Code also stipulates that marketers must adhere to the following requirements regarding the collection, use, and disclosure of the personal information of children and teenagers unless they can demonstrate a compelling reason to do otherwise that considers the best interests of the child or teenager.

1. They must collect and retain only the minimum amount of personal information needed to provide the product or service.
2. Geolocation options must be off by default
    - When location tracking is active, a prominent notification must be provided.
    - Options that make location visible to others must revert to 'off' at the end of each session.
3. Profiling should be 'off' by default and should only be used where marketers have appropriate measures in place to protect the child or teen from any harmful effects.
4. Marketers must not use techniques to lead or encourage young people to provide unnecessary personal information or weaken or turn off their privacy protections.
5. Connected toys or devices must comply with this Code.

Designing to Address Privacy Impacts and the Best Interests of the Child

Consultation Questions
1. How can consideration for the best interests of the child be integrated into the design and PIA processes? How can the best interests of the child be best assessed?
2. What potential impacts, including harms specific to children, should be considered in a PIA?
3. How should organizations actively involve children, their parents/guardians, teachers or child advocates in the PIA process?

CMA Response:

Considering the best interests of children should be part of Privacy by Design processes and Privacy Impact Assessments.

A meaningful way to assess considerations around the best interests of the child would be to establish a risk classification system through which websites could be classified as General Audience, Age Appropriate, or Restricted. During their Privacy by Design processes and development of their Privacy Impact Assessments, organizations should classify their products/campaigns into one of these categories, as outlined below.

- **Restricted:** Organizations that sell adult products would need to take reasonable and meaningful steps to limit the ability of minors to access the products. These steps should be aligned with broader privacy principles such as minimal data collection and secure age-checking verification to mitigate unnecessary privacy risks. This approach would be consistent with the UK's Age-Appropriate Design Code, and the US's Children's Online Privacy Protection Act (COPPA).

- **Age Appropriate:** Products/campaigns directed at minors, and companies that know, or should reasonably know, that they are processing minors' personal information, would be in the age-appropriate category. They would need to ensure all marketing communications are age appropriate, as described in the CMA Code and an OPC Code, and that the data used for profiling or ad -targeting algorithms for users classified as minors undergo risk assessments.

- **General Audience:** Companies in this category would not have to follow any special measures. For example, a music store might be visited by a young person who loves guitars and wants to save money until he can buy one. Since the website will not know that the child is a minor, he might be served some ads for musical instruments. However, this does not constitute a material risk of harm.

For websites and apps directed at children where there is a material risk of harm, we see merit in testing to ensure they understand how to navigate the site/app, including privacy and disclosure aspects. However, flexibility is needed to consider the size of a company. For example, a local toy store with a website would almost certainly not have the resources to undertake a formal child-centric consultation. An OPC Code should leave room for businesses to rely on consultations and guidance led by industry associations or other groups that inform approaches to design.

Commented [SC1]: The changes here were proposed by a member who is not on the Committee.

Ensuring Child-Appropriate Transparency Practices

Consultation Questions:
1. What information should an organization provide in a privacy notice about their handling of children's personal information?
2. How can information be tailored to different age ranges and capacities to ensure that children and/or their parents/guardian make informed decisions about privacy? Are there tools or approaches that can be used to support this? What are potential challenges and solutions to doing this effectively?

3. How and when should information be presented strictly to parents/guardians (or trusted adults)? How should information be presented when directed at both parents/guardians (or trusted adults) and children?
4. What resources could be provided to parents/guardians (or trusted adults) to help them explain the privacy implications of services or products to children?

CMA Response:

The CMA Code and other CMA guidance materials call for clear, age-appropriate transparency, grounded in privacy by design and applied whenever an organization knows (or should reasonably know) it is engaging with minors. The 2024 Sweep Report points to LEGO's age-appropriate and child-friendly videos as an example of best practice for clear, visual, and comprehensible information geared to children.

Similar best practices are seen in platforms such as PBS Kids, which uses simple language and intuitive design, directly addressing the ICO's Age-Appropriate Design Code and GDPR's emphasis on transparency for children. Additionally, Toca Boca's approach to children's privacy is a prime example of data minimization in practice. By intentionally designing their digital apps to function without collecting personal data, they successfully meet the rigorous requirements of an FTC-approved COPPA Safe Harbor program. Specifically, their membership in the PRIVO Kids Privacy Assured program provides third-party certification that their privacy practices are compliant with the Children's Online Privacy Protection Act.

While these are excellent examples of best practices for child-friendly design, developing and maintaining such approaches is extremely costly and even debilitating, particularly for small and medium-sized enterprises (SMEs) In a challenging economic climate, imposing such significant financial burdens risks stifling innovation and reducing the competitiveness of Canadian businesses, with costs ultimately passed on to consumers. Recognizing these realities is important to ensure best practices remain accessible and achievable across organizations of all sizes.

Under the CMA Code, which applies up to the age of majority in each province, organizations must provide accessible explanations of data processing that are tailored to the medium and the audience so that it is user friendly and user appropriate. This approach directly aligns with PIPEDA's consent and data minimization rules. To operationalize these principles, disclosures should be tailored through child-centric design, such as simplified pop-ups, interactive summaries, bright colors, and child-friendly language. Sites could include prominent, inviting buttons to click: one for children and another for parents to explain how they can help their children navigate online. (e.g., models like LEGO's, highlighted by the OPC Sweep Report for its age-appropriate privacy policy sections and child-friendly videos), or just-in-time prompts. Additionally, there are or should be limitations on the collection and retention of information of individuals under the age of 18.

The Sweep Report found that privacy policies in Canada are longer than in other jurisdictions. This is an unavoidable consequence of a framework where consent is the only grounds for processing, which requires exhaustive disclosure for every activity at a level that is not required in other jurisdictions. This has led to the well-documented phenomenon of 'consent fatigue,' where consumers, including parents, are so overwhelmed by lengthy and complex notices that they click 'agree' without meaningful engagement, undermining the very purpose of the consent process. The CMA's Guide to Transparency for Consumers suggests better means to inform consumers, such as using a layered approach, and providing just-in-time information.

For sites/apps where there is a material risk of harm, organizations can follow approaches to promote awareness of privacy decisions and safe practices, such as having a “For Kids” button and a “For Parents” button. The section for parents can explain what is in the kids’ statement and provide advice on how they can help their kids navigate.

Critically, organizations must minimize data collection and retention of minors’ personal data to what is reasonably necessary to provide the service. Sensitive data should be strictly limited except where it is required to deliver the service (such as using location data to connect a wireless device to the nearest cell tower).

Teenagers increasingly rely on digital services to access information that is critical to their development. This includes education, mental health resources, financial literacy, and career opportunities. Access to such content should not be unduly hampered or subject to overly burdensome requirements for mature minors, provided that robust safeguards are in place to protect against harmful data practices. This balanced approach aligns with teens’ evolving autonomy while maintaining appropriate privacy protections.

For marketing contests geared to children, marketers must collect only the amount of personal information required to determine the winner(s) and to contact the parents/guardians of the winner(s). All communications should be directed solely to winners’ parents/guardians, with no direct contact with the winners. No personal information should be used for any other purpose beyond the contest winners and contacting their parents/guardians. Determining the contest winner(s) and contacting their parent or guardian, and the organization must not retain the personal information following the conclusion of the contest.

Being Privacy Protective by Default

Consultation Questions:

1. *What measures could organizations employ to ensure that children’s personal information is only retained for as long as is necessary (for example, having messages automatically “expire” after a shorter period of time)? Are there specific factors that should be considered when setting a retention or disposal policy for children’s information?*
2. *Are there any specific practices that should be avoided because of the difficulty in obtaining meaningful consent from a child or because it would constitute an inappropriate data practice?*
3. *Are there any scenarios where it would be in the best interests of the child to have less restrictive default settings?*

CMA Response:

For children, a practice that should be avoided is targeted advertising. This is generally already the case. The OPC has already established “no go zones” under Section 5.3 of PIPEDA. Under this Section, an organization can only process personal information if a reasonable person would consider it appropriate in the circumstances.

Scenarios where it would be in the best interests of the child to have less restrictive default settings would apply mainly in the case of mature minors. Mature minors use the internet for many legitimate purposes. They are expected to access websites to complete homework assignments. They apply for post-secondary education and for summer jobs. They search online for birthday gifts for family and friends. They do online banking. We need them to become informed and savvy digital citizens, and to know how to safely navigate technologies. How to

differentiate between legitimate ads and offers, and those with dark design patterns or from unreliable sources. These are skills developed over time as they spend time online.

These examples underscore the developing autonomy of older adolescents and the practical necessity for these individuals to manage certain personal data. In Quebec, Law 25 acknowledges that minors aged 14 or older can give their own consent to the collection of personal information. The OPC considers children under the age of 13 to be unable to meaningfully consent, which implies different privacy measures than for adults or for young people older than 13.

Avoid deceptive practices

Consultation Questions

1. *Beyond the practices set out in Section 5 (Being privacy protective by default) and approaches referenced above, how can products or services be designed to encourage children to adopt privacy protective behaviours?*
2. *What practices should be encouraged to mitigate potential harmful behaviours, and/or help children make informed decisions about their personal information?*

CMA Response:

Helping minors make informed decisions about their personal information requires empowering them to navigate online spaces securely and share consciously and deliberately. Education is key. As outlined in the OPC's 2024–2027 Strategic Plan, one of its core objectives is to champion children's privacy rights by "engaging youth for informed education and outreach". It's essential to protect children from risks while maximizing the benefits and opportunities of the digital environment. These types of practices align with the principles advocated by leading privacy authorities, including the OECD's Recommendation of the Council on Children in the Digital Environment and the UK Information Commissioner's Office (ICO)'s Age-Appropriate Design Code.

If the OPC sees a role for consumer education, they could partner with organizations like the CMA to develop initiatives that empower children with the knowledge and skills to understand the implications of sharing their data and to make informed choices when it is appropriate to do so.

Limiting disclosure of children's information

Consultation Questions

1. *What type of technical (or other) measures could be used to prevent the unauthorized use of children's information?*
2. *Should children receive notifications when their information is being shared? Are there scenarios where this is more critical?*
3. *Are there certain types of personal information that should never be disclosed? Are there certain purposes for which a child's personal information should never be disclosed?*

CMA Response:

The CMA Code states that organizations must ensure that children's personal information is not shared or disclosed without explicit, opt-in parental or guardian consent. This requirement applies to all marketing communications directed to children and is intended to respect the authority of parents and the privacy rights of minors.

Restrictions applied too broadly could impede an organization's ability to deliver its services. For example:

- An airline may need to securely share a child passenger's information with a partner carrier to ensure the transfer of the minor and their luggage to a connecting flight.
- Members of a wireless family plan might choose to turn on their phones during vacation in an area where service partners are delivering services.
- The secure exchange of personal data is required to fulfill the requested service.

General Questions and Next Steps

Consultation Questions

1. *What role do you see the OPC playing in ensuring that the best interests of the child are upheld?*
2. *Are there other privacy considerations that should be taken into account in the establishment of a children's privacy code?*
3. *Are there areas/industries where the OPC should provide sector or industry-specific guidance for the handling of children's personal information?*
4. *What challenges or solutions do you foresee in applying a children's privacy code?*

CMA Response:

OPC Mandate

An OPC Code should remain firmly within the Commission's core mandate of privacy protection and avoid extending into adjacent regulatory domains such as online harms, human rights, deceptive practices or content moderation. Expanding the scope of privacy regulation into these areas would create unnecessary, and potentially conflicting, regulatory overlap with existing federal and provincial frameworks. This could undermine the clarity and effectiveness that businesses and families need to ensure compliance. A focused approach that leverages the OPC's established expertise in privacy matters while respecting the jurisdictional boundaries of other regulatory bodies will ultimately deliver more coherent, enforceable, and effective protection for children's personal information.

Once an OPC Code is in place, the OPC has an obligation to educate all parties, including impacted organizations, children and parents.

Enforcement Capacity

The experience with GDPR implementation illustrates the risks of creating overly extensive and prescriptive regulatory frameworks that exceed enforcement capacity. European privacy regulators have struggled to investigate and address the full breadth of GDPR violations due to resource constraints, leading to selective enforcement that has created undeliverable expectations for consumers and imposed undue costs and uncertainty for organizations.

The European Union Agency for Fundamental Rights (FRA) and the European Data Protection Board (EDPB) have both published reports highlighting these types of challenges faced by Data Protection Authorities (DPAs). An FRA report specifically highlighted that a lack of resources could compromise the implementation of a DPA's mandate and its independence. The report also noted that a large majority of interviewees emphasized that insufficient financial and human resources pose a significant obstacle to DPAs in fully executing their duties required under the GDPR, as outlined in Article 52 and Recital 121.Canadian privacy regulators face similar resource limitations and have likewise had to triage certain types of investigations over others.

An overly comprehensive OPC Code would perpetuate this problematic dynamic, creating false expectations among parents and children that all privacy violations will be addressed while simultaneously creating economic uncertainty for businesses.

A more prudent approach would focus regulatory resources on areas where children face material harms. This would ensure that the Canadian economy is not overburdened with compliance costs for requirements that may not receive consistent regulatory attention, allowing businesses to focus their resources on genuine risks and productive innovation.

Interoperability

An OPC Code must ensure interoperability with provincial and international standards to avoid consumer confusion and reduce compliance friction for Canadian organizations operating globally

In closing

The CMA supports an OPC Code that prioritizes risk-based protections for minors while ensuring practical compliance for businesses. Under Article 17 of the UNCRC, children have the right to access information from various sources, particularly those that promote their well-being, which is especially critical for life issues such as mental health, financial literacy, and career opportunities. As children mature, their right to privacy grows, and this is essential for them to explore their identity and develop autonomy. General Comment No. 25 supports this principle by recognizing that privacy is essential for a child's evolving autonomy, allowing them to explore their identity and develop independence. Enabling them to access general audience sites freely is an important reflection of this.

The OPC, as the federal regulator responsible for developing and overseeing its Code, should ensure that young people are actively engaged throughout the development process so that their perspectives, lived experiences, and concerns are reflected in an OPC Code. By leveraging its networks and key audiences, the OPC can ensure that its Code is not only protective in nature, but also relevant and practical from the perspectives of those it is designed to safeguard.

Our submission outlines a risk-based, tiered framework that emphasizes obligations on organizations that offer restricted products, and organizations that know, or should reasonably know, that they are processing minors' personal information, while avoiding unnecessary burdens on products and services directed at general audience. Drawing on the CMA Code, we stress the need for clear and practical guidance on implementation, particularly in determining scope. This includes respecting the desire of teens to access information and products without age verification, while also ensuring valid consent and implementing age-appropriate privacy measures.

The CMA stands ready to assist the OPC in developing a code that is both practical for industry and protective for young Canadians.

To discuss our submission, contact:

Sara Clodman
Chief Public Affairs and Governance Officer
sclodman@thecma.ca

About the Canadian Marketing Association (CMA)

The CMA is Canada's largest marketing association and the voice of the marketing profession. We are the catalyst to help Canada's marketers thrive today, while building the marketing mindset and environment of tomorrow. We represent virtually all of Canada's major business sectors, and all marketing disciplines, channels, and technologies.

Our purpose is to champion marketing's powerful impact. We provide opportunities for our members from coast-to-coast to develop professionally, to contribute to marketing thought leadership, to build strong networks, to meet consumer needs and provide meaningful, trust-building relationships with their customers, and to strengthen the regulatory climate for business success.

Our Chartered Marketer (CM) designation signifies that recipients are highly qualified, with the skills they need to help businesses grow and up to date with best-in-class modern marketing practices, including those reflected in the Canadian Marketing Code of Ethics and Standards and our Consumer Centre helps Canadians better understand their rights and obligations.