

Submission to the Commission d'accès à l'information on the Guidelines on Criteria for Valid Consent

June 27, 2023

Introduction

The Canadian Marketing Association (CMA) greatly appreciates the opportunity to provide feedback to the Commission d'accès à l'information (CAI) on its draft guidelines on criteria for valid consent. Given the momentous changes to Quebec's private sector privacy law, it is critically important for the CAI to consult with industry to ensure that its guidance is practical and effective.

Modern economies are predicated on the exchange of personal information. Where individuals provide personal information to an organization in connection with the purchase of goods or services, they reasonably expect the organization to use the information to serve them better. Consumers are demanding much greater speed and quality of information so that they can identify and access services provided by companies and make informed purchase decisions. Responsible use of data to personalize experiences is key to providing value to consumers, and to delivering on their increasingly sophisticated expectations in a fast-paced world. Recent research indicates that 43% of Canadian consumers agree that data exchange with business is essential to the running of modern society—rising significantly from 35% who agreed with this statement in 2018.¹

The loyalty and trust of customers is the foundation for business success. Most organizations in Quebec recognize that having strong privacy and data protection practices give businesses a competitive advantage. They work hard to protect and respect the privacy interests of the individuals they serve.

Privacy law must strengthen consumer privacy protections for consumers while ensuring organizations can innovate with data and serve consumers well. A risk-based and context-specific approach to the interpretation of privacy law is critical to ensure that the law can withstand rapidly evolving technologies, business models and consumer expectations for years to come.

Overall assessment of the draft guidelines

We appreciate the significant efforts by the CAI to develop these detailed guidelines, and to provide realworld examples for organizations. However, as outlined below, some of the CAI's interpretations depart significantly from the language in Law 25, create unintended consequences for consumers and organizations, or fail to acknowledge the practical challenges of obtaining consent in a complex data environment thereby exacerbating issues like consent fatigue.

Several examples within the guidelines explicitly deem activities as either compliant or non-compliant. This will result in organizations avoiding certain activities without sufficient contextual analysis. It is critical that the examples (and the guidelines) reflect what is required by the law versus an optional best practice. Where the guidance suggests such aspirational measures, they should be clearly labelled as best practices, rather than legal requirements.

The guidelines are long (36 pages) and businesses, particularly small and medium-sized enterprises (SMEs) with limited access to legal advice, are looking for concise and simple guidance on how to apply Law 25 to their business. Individuals without legal training should be able to readily understand how the basic legal requirements apply in practice. We commend the CAI for including the diagram on page 13 as a helpful visual tool, and suggest additional practical tools for organizations, such as a summary checklist, flowchart, or birds eye overview of basic "must have" legal requirements.

¹ <u>Global Data Privacy: What the Consumer Really Thinks</u>, GDMA, 2022.



The CMA urges the CAI to amend the guidelines in the <u>seven key areas outlined below</u>. In all cases, we urge the CAI to make best efforts to align its guidelines with other Canadian jurisdictions to support consumer understanding, ensure businesses can operate seamlessly across borders, and create a foundation for a wide availability of goods, services and investment in Quebec.

Request for reasonable enforcement timeline

We request that the CAI publicly indicate that the <u>guidelines will not be enforced for 18 months</u> from the time they are released, given significant uncertainty around certain provisions, and given organizations require the necessary time to implement the changes, including preparing systems and training staff.

Organizations have diligently been preparing for the law's coming into force. However, some areas of the law, particularly section 8.1, have resulted in significant uncertainty and fundamental disagreements in legal interpretation. Organizations will not have sufficient clarity regarding some aspects of the law until the CAI's official guidelines are released. This is expected to occur in October – a month after the provisions come into force.

Organizations will need sufficient time to implement changes to compliance plans, business processes, staff training and IT systems. In particular, operationalizing section 8.1 will require substantial changes to internal and external policies and procedures, consumer-facing interfaces, and contractual arrangements with service providers. In light of the insurmountable operational difficulties, some organizations and services providers have signaled their intention to cease operations and service to Quebec if there is not a reasonable implementation period.

Many SMEs do not have the resources to tool up quickly to comply with this provision, while large enterprises with numerous and complex applications, systems and processes will need sufficient time to reprogram and redevelop them, and to train hundreds or thousands of personnel.

Detailed feedback

1. Mandatory express consent for identification, tracking and profiling

Recommendation: We strongly submit that section 13 of the guidelines (relating to section 8.1 of the act) should be removed and instead be the subject of separate guidelines – to be developed in consultation with the CMA and other industry stakeholders – that are specific to the collection of personal information through identification, location and profiling technologies. The basis of this recommendation is that section 8.1 of the act does not directly relate to the subject of these guidelines, the nature and scope of identification, tracking and profiling technologies is varied and nuanced, and there is a critical need for the CAI to consult with the online advertising industry on the interpretation and operationalization of this section in order to avoid unintended consequences for consumers and organizations.

If the CAI is unwilling to create separate guidelines, it is critical that the express consent requirement in section 8.1 of the law be applied so as to focus on situations that are outside the reasonable expectations of individuals and/or that carry a material risk of harm. In this case, the request for an 18-month delay of active enforcement becomes critical.

Section 31b of the draft guidelines indicates that technologies that identify, track or profile individuals must be turned off by default, amounting to an express (opt-in) consent requirement for organizations that collect personal information through any of these technologies.

This approach goes far beyond interpreting the law, which is written as an extension of the transparency obligation in section 8. The wording of section 8.1 speaks only of an obligation to inform individuals of the



means available to activate these functions, without explicitly stating that these means must in fact exist or that the functions themselves must be disabled by default. Section 8.1 is entirely distinct from section 9.1, which imposes default privacy settings only on the offering to the public of a "technological product or service having privacy settings", not on the use of profiling and tracking technology more generally.

We fully support greater transparency. However, the CAI's extreme interpretation of this provision would require express consent for any collection of personal information through the use of technology, in all cases and contexts. In addition to going beyond the explicit requirements of the statute, this blunt express consent requirement fails to take a risk-based approach and will have unintended consequences for consumers, organizations and the digital economy upon which they rely.

There is no basis for restricting this type of activity unless there is clear risk of harm. The days of collecting personal information via pen and paper are long gone. Technology is how companies collect data to serve their customers. The application of section 8.1 of the law to **all** technologies is extremely broad and unworkable.

All technologies that 'identify' or 'locate' people would cover a huge range of routine and non-harmful activities. For example, it is common practice for websites to infer location in order to direct users to the appropriate site for their country, reflecting the correct pricing, currency and product availability. A website may collect IP addresses in order to avoid serving copyright-protected content to user residents in a jurisdiction for which the website provider does not hold the rights to make that content available.

Retailers often use inferred location data to display the store nearest to a user and its hours and contact details, as well as sales or flyers applicable to that location. Call centre operators use area codes, from which location can be inferred, to route calls to an appropriate call centre.

In many cases, a tracking or profiling feature is the core purpose of the app or other technology, making an express consent requirement unnecessary and creating pointless consumer burdens. For example, a ride-sharing app can't function without accessing location; a fitness tracking app can't function without tracking user activity and performance.

Of course, in other cases, express consent would be reasonably required, such as where a feature would optimize, rather than be critical to, the delivery of the overall service. For example, location tracking may not be required to use a dating website or app but the company could give users the option to turn on location tracking to enhance an individual's experience by showing other users nearby.

National or international companies would have to collect some form of personal information (such as an IP address) to know whether they are even dealing with an individual in Quebec in order to comply not only with Law 25 but also with other regulations, including Quebec's language laws. If companies need express consent to determine where individuals are located, the requirement seems absurd. Users visiting websites would have to be presented with a landing page to consent to inferring location before proceeding. What language would the page be in? What wording would be required to meet the requirements of the local jurisdiction if the company was not aware of the jurisdiction?

The definition of profiling is also extremely broad. In the marketing sector, profiling is used to give consumers the types of meaningful and intuitive experiences that they expect from organizations today (in contrast to the older practice of mass generic spamming), including through the use of third-party analytic tools and software, such as cookies, pixels and beacons. For example, organizations may create a profile in order to suggest more relevant products and services based on an individual's preferences or interests, or to offer discounted pricing for products and services based on an individual's inferred interests, reliability, behaviour or location.



A recent survey found that 50% of consumers want to see internet advertising that is relevant and targeted to them.² Further research found that people ultimately want experiences that feel valuable to them as individuals. Overall, consumers are more comfortable sharing their data when they understand how they benefit from such sharing. With regards to online advertising, the study found that people's attitudes towards online privacy shift based on the perceived value of an ad. People find ads valuable when they are tailored to their interests, lead to time or cost savings, and are brought to their attention at the right moment.

Customers increasingly expect organizations to take steps to prevent issues before they arise; knowing when, where, and how to get in touch; and to proactively reach out where necessary. This calibre of consumer experience requires an understanding of customers through well-developed profiles. At a basic level, it could be a restaurant wanting to use an automated tool to record a customer's favorite wine to offer it to them on their next visit.

Even under the GDPR, profiling is only restricted through an individual's right to opt out of solely automated decisions that produce legal or similarly significant effects. As outlined by Axel Voss (a Member of the European Parliament and one of the original drafters of the GDPR), the lack of context continues to be a shortcoming of the GRPR, as he notes "...a lack of distinction between automated processing, including profiling, which is expected by individuals and which contributes to more effective services to individuals and more relevant content, and profiling which creates harm, such as political manipulation, or a commercial lock up effect for which specific safeguards should be put in place."³

Consent is only one lever to ensure privacy protection. It is important that consent is not so over-used that it becomes illusory. The broad express requirement will result in an onslaught of pop-ups, with most consumers opting out⁴ in the name of perceived risk reduction, even in cases where there is no meaningful risk to them – and where there may even be substantial advantage to them. The requirement will also exacerbate the widespread consent fatigue consumers are already experiencing, making them even less likely to carefully review notices and make informed privacy decisions. By opting out without reviewing and considering the consent notice, consumers will be inadvertently denying themselves information that could be of value to them.

Significant research in the EU has indicated that excessive privacy notices offload too much responsibility on the consumer without a proven increase in privacy understanding and awareness. For example, 72% of consumers indicate that they feel annoyed about the number of times they must accept cookies to access content. Many organizations, in a bid to avoid stiff penalties, resort to asking their customers for consent multiple times, across multiple different touchpoints.⁵ This is why the UK Government's 2023 data privacy reforms include an expanded range of exceptions to consent for cookies to reduce the onslaught of cookie consent banners. (Law 25 specifically excludes browser cookies from section 9.1, which requires the highest level of confidentiality by default. However, browser cookies are not excluded under section 8.1, which is confusing for organizations.)

The Digital Advertising Alliance of Canada (DAAC) has been collaborating with governments and stakeholders across the country to deliver a self-regulatory program that provides transparency and choice for consumers in the context of interest-based advertising. The program is designed with an understanding of the complex nature of global data flows in the online advertising space, and with the goal of empowering consumers without overwhelming them.

The digital advertising ecosystem is just one of many complex data ecosystems that provide tremendous value to individuals and are core to Quebec's prosperity and global competitiveness. We urge the CAI to

² <u>Canada's Digital Marketing Pulse</u>, Ipsos, 2019.

³ Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021.

⁴ We can estimate that this will be the case based on the implementation of App Tracking Transparency by Apple in the Spring of 2021, which resulted in the rate of consent to tracking and tracing plateauing at around 25%.

⁵ Consent Fatigue, The Data Privacy Group, 2022.



collaborate with the CMA and other key industry associations to deepen its understanding of complex data ecosystems in different sectors, and to rely on self-regulatory initiatives underway. The CMA would be pleased to organize a meeting between the CAI and other digital advertising stakeholders to discuss the practicalities of operationalizing privacy requirements in this space.

Without accounting for context and risk, the express consent requirement is completely unworkable for organizations and needlessly burdensome for consumers, without providing meaningful additional privacy protection. Faced with such a broad requirement, we fully expect some companies to stop servicing individuals in Quebec altogether, rather than cope with the operational difficulties and likely low consent rates. We have already seen this occur in the EU, with some of the law's impractical requirements leading to a reduced availability of goods and services for EU consumers, without a corresponding proven privacy benefit.⁶

We support greater transparency for all situations where an organization collects personal information using technology that identifies, locates or profiles an individual. This adequately fulfills the requirement in the text of the law, which is to inform an individual of the use of such technology and the means available (if any) to activate it. It is also appropriate to the privacy risk of routine and non-harmful collections of personal information through these technologies. We also strongly support options that allow consumers to turn off or opt out of tracking technologies when they are not reasonably necessary for the provision of the service in question.

Informing can take place through various means and organizations can take a multi-layered approach, as appropriate and reasonable (e.g., general information in a privacy policy, terms and conditions, website, FAQs, and more specific information on forms or in other direct communications like a "just in time" notice or pop up). Notification should always be reasonably prominent, and organizations should be clear with customers about which functions are activated by default (i.e., "By downloading this app, you will be profiled, which means..."). In addition to being clear with customers about which functions are activated by default, organizations should be clear about the choices individuals have to expressly opt in to features in accordance with their preferences.

Should the express consent requirement remain in this version of the guidelines (i.e., on valid consent and not separate upcoming guidelines), the guidelines should require organizations to take greater steps for potentially harmful activities by making a contextual assessment to determine whether express consent is appropriate in the circumstances.

Organizations should take the following factors into account in making their assessment:

- The reasonable expectations of individuals. For example:
 - An individual downloads a coffee shop's app. The coffee shop tracks the customer's location to determine when a visitor enters a competitor's store so they can send them a tailored offer or coupon. Location tracking when an app is not being actively used would be outside the reasonable expectations of an individual, and express consent would be reasonable.
- The sensitivity of the information involved. Identification, location and profiling should require opt-in for any activity that might be associated with or reveal information that is medical, biometric or otherwise intimate in nature, or the context of its use or disclosure gives rise to a high reasonable expectation of privacy (as per section 31a of the guidelines). For example:
 - An individual who is a member of a community group on a social media platform is served an ad for a health or "or otherwise intimate"-related product based on posts made within the group, or the friends of the user. Given this profiling is associated with information that carries a high reasonable expectation of privacy, express consent would be reasonable.

⁶ Privacy Law Pitfalls: Lessons learned from the European Union, Canadian Marketing Association, 2022.



- Express consent would be required when using a fingerprint or facial image, or tracking a person's heart rate, or if there is any collection of information related to ethnic origin, political opinions, religious or philosophical beliefs, state of health or sex life or sexual orientation.
- The risk of harm to the individual. For example:
 - Given the risk of real safety issues, express consent would be reasonably required for precise location tracking in the context of certain social media applications, such as dating apps.

It is critical that the guidelines better define what is meant by 'profile', 'identify' and 'locate, and – in collaboration with industry stakeholders – narrow the scope of technology that the requirement would apply to. For example, 'locate' should be defined as an attempt to determine the geographic location of a natural person with reasonable accuracy and precision, such as identifying longitude/latitude coordinates, or within an accuracy of a few meters. 'Locate' should not include inferring that a user is situated in a particular country or municipal area, which may be inferred through IP address/Internet Service Provider. The scope of profiling technologies that the requirement applies to should also be clarified, as the current interpretation covers much more than perceived risks related to certain apps and social networks, which appeared to be the original focus of section 8.1.

2. Express consent and consent fatigue

Recommendation: To ensure meaningful consent, we urge the CAI to indicate that express consent may be the preferred form of consent in many cases; not to encourage organizations to seek express consent whenever possible (section 30 of the guidelines). Law 25 does not require express consent "whenever possible" and encouraging organizations to collect express consent in this way would significantly exacerbate consent fatigue. Furthermore, the examples to reduce consent fatigue in section 33 of the guidelines should be replaced with more effective best practices.

Section 30 of the guidelines indicates that an organization should seek express consent whenever possible. This priority to express consent does not exist in the statute, and this is not a reasonable interpretation of the law. The act requires lawful authority, which can be obtained in different ways, for example by satisfying the conditions of presumed, implied or express consent. Once you satisfy the conditions, the collection, use or disclosure of personal information is lawful.

This is in alignment with other privacy frameworks across Canada. Given serious concerns about consent fatigue, it is critical that organizations have the operational choice of choosing the type of consent appropriate in the circumstances. Encouraging organizations to default to express consent is not only impractical but also undermines the utility of express consent, which could be rendered meaningless if it is used too often and not reserved for sensitive information or unexpected uses. Moreover, routinely requesting express consent would negatively affect the customer experience, and could also create confusion for individuals by suggesting they need not consent to personal information processing that is necessary to provide the product or service.

In section 33 of the guidelines, the CAI has explicitly recognized consent fatigue as an issue. However, the examples presented as solutions to address it, including breaking the rhythm through a math question or a waiting period, will only cause more frustration and weariness for consumers, causing them to disengage from the process. It is important to treat the underlying cause, which is information overload due to a high frequency and volume of requests, and not the symptom. It is not about paying attention, but a general capacity to take on the information and actions being requested. Furthermore, the suggestion of a waiting period or countdown could be seen as pressuring a consumer to consent, which is at odds with the concept of "free" consent. Ultimately, the best defence against consent fatigue is to ensure that express consent is required only with respect to purposes outside the reasonable expectation



of individuals, or that could give rise to material harm. The examples in the guidelines should reflect wellresearched best practices, such as those in the Office of the Privacy Commissioner of Canada's guidance on meaningful consent.

3. Granularity: separate consent for each purpose

<u>Recommendation</u>: The requirement for granularity in section 59 of the guidelines should permit the bundling of similar and logically related purposes as long as each purpose is clearly specified and the groupings are not unclear or misleading.

Section 59 of the draft guidelines indicates that consent must be granular and requested separately for each purpose. This is unworkable for organizations and will result in a very poor experience for individuals. Many companies, including those offering critical goods and services to individuals in Quebec, have multiple business lines and interactions with customers. For example, if the average telecom company were to request consent separately for each purpose, consumers would be presented with dozens of requests.

We agree that each purpose should be clearly specified, and that companies should transparently identify purposes in a granular format. However, it is impractical to expect organizations, customers and employees to work through such a cumbersome and repetitive consent process.

Organizations should be permitted to collect a single consent for multiple purposes if those purposes are related and if doing so is not misleading. For example, a company may choose to group purposes thematically (e.g., those critical to the delivery of the product or service requested, for fraud purposes, for analytics, for communications with the customer (personalized marketing), for consultation purposes and surveys etc.) Organizations should consider the best approach in the circumstances to enhance consumer understanding, focusing the requirement for granularity more on secondary purposes or on situations where individuals have a meaningful choice.

The creation of a patchwork of consents, with individuals consenting to some elements but not others, would create an unduly complex environment for both organizations and consumers, and fails to recognize that purposes are often interconnected. Examples 60.1 and 60.2 in the guidelines are too straightforward to show the true nuanced nature of how organizations operate; the fact that you consent to one does not impact whether you consent to the other.

4. Authentication of the data subject - parental consent

Recommendation: Section 25 of the guidelines should indicate that organizations should make best efforts to verify parental consent with a degree of certainty that is reasonable *in the circumstances.* Further, the requirement for such certainty should be focussed on those organizations that know, or are deemed to know, that they are processing the personal information of minors. This is consistent with the approach taken by the Children's Online Privacy Protection Act in the US, as well as privacy laws in California and the EU, and would avoid targeting organizations that may only incidentally and unknowingly process the data of minors.

The CMA supports the protection of minors' data, and has for many years been a leader in setting standards for marketing to children through our Canadian Marketing Code of Ethics & Standards. Section 25 of the CAI's guidelines indicates that when parental consent is required for a minor under 14, the organization should verify the status of the person giving consent "always with a reasonable degree of certainty". The requirement that there always be a reasonable degree of certainty could prove to be an impossibly strict bar for many organizations. In most online contexts, it is impossible to verify whether parental consent is genuine, or whether a minor under 14 is attesting and accessing a service



themselves, without the intrusive collection of government-issued identification, biometrics, and other sensitive information.

The proposed guidelines may unnecessarily lead to the routine collection and retention of sensitive personal information solely to satisfy the requirement for certainty that the organization is not dealing with minors. Moreover, organizations will be incentivized to retain this authentication information in order to prove compliance with the law, if challenged.

The personal information required to verify age can be among the most sensitive (e.g., governmentissued ID with birthdate). It carries the greatest adverse risk in the event of a breach, and is most soughtafter by criminals. In many cases, the risks associated with the collection and retention of such information would far outweigh the potential privacy risk to any minor that did access a service targeted to adults, or a more generalized population. In the absence of the CMA's proposed amendment, organizations that do not target minors, or whose businesses are not known to attract large numbers of minors, will be collecting and retaining additional personal information on all customers for no other reason than to confirm that they are not minors. Given the serious risks of harm associated with unauthorized access to such personal information, this may be a case where the cure is worse than the disease.

5. Failure to obtain valid consent as a confidentiality incident

<u>Recommendation</u>: Section 16 of the guidelines should be removed and addressed under separate guidelines on confidentiality incidents, which more appropriately deal with situations of loss and unauthorized use or disclosure.

Section 16 of the guidelines indicates that the failure to obtain valid consent is a confidentiality incident, meaning that if an organization detects a problem related to the failure to obtain valid consent, it must comply with incident-related obligations (recordkeeping, assessment of risk or harm, notice etc.). We wholeheartedly agree that failure to obtain valid consent is a breach of the statute and subject to enforcement. However, this extension of obligations related to typical confidentiality incidents is highly unusual, and contrasts with how these incidents are viewed currently in Quebec, and across the country. The vast majority of confidentiality incidents are not a violation of consent. Furthermore, the vast majority of circumstances where there was a failure of consent would not give rise to a trigger for notification (significant injury).

It is unclear why this issue, which is related to data governance, is addressed here (under the guidelines for the criteria of valid consent), rather than under guidelines on confidentiality incidents.

6. Repeated requests for consent as a violation of free consent

<u>Recommendation</u>: Section 41b of the guidelines should be adjusted to permit organizations to reseek consent at appropriate intervals.

Section 41b of the guidelines indicates that consent can generally only be sought once for the same purpose (unless there has been a substantial change in the context to justify it). This is not a requirement in the act and in some cases, the requirement is completely impractical.

There are many cases where companies cannot track if an individual has already been asked for consent before, such as if an individual using a public computer to view an open-access website (where they do not identify themselves) opts out of cookie tracking. The requirement is also in tension with the requirement for organizations to minimize the amount of data collected, given one of the best ways to avoid asking for repeated consent is obtaining sufficient data.



Although we agree that barraging a consumer with frequent requests is unacceptable, it is reasonable and beneficial for organizations to provide people with additional options to adjust their preferences at appropriate intervals. Consumer preferences change over time, and consumers are often presented with requests for consent after the passage of an appropriate amount of time. For example, if you are a nonlogged in user that purchases a book on a website, you may be asked for consent to join the company's email list on subsequent visits when you purchase books. This would not violate the free nature of consent, as long as there is conspicuous notice and an ability to exercise your choice. Even the Supreme Court of Canada has indicated that asking the same question dozens of times to an accused that has asserted their right to remain silent does not oppose the Canadian Charter of Rights and Freedoms.⁷

Section 41b of the guidelines should borrow the phrase "appropriate intervals" from section 69 of the guidelines (which indicates that where an organization seeks consent for a very long time, it should pay particular attention to transparency on an ongoing basis, reminding individuals at appropriate intervals). With respect to section 69 of the guidelines, we note that informing individuals of the duration for which consent is valid is not a requirement of the law, and in some cases may not be necessary or appropriate. This is an example where the guidelines go beyond what is required in the law. It should therefore be identified as a best practice, rather than a requirement.

We further note that the examples in the guidelines frequently suggest pop-up windows as a means of obtaining consent. It is important to illustrate the many other ways that organizations can obtain consent, particularly given many consumers find them annoying and many privacy management browsers block pop-up windows.

7. Information required for deemed consent

<u>Recommendation</u>: In order to avoid confusion for organizations, the guidelines should better articulate what information is expressly required upfront for deemed consent to be valid.

The guidelines appear to require more disclosures to ground deemed consent than what the statute requires, including some information that need only be available upon request. From a practical perspective, it would be helpful for the guidelines to suggest which of these disclosures should be referenced in a privacy policy versus included as part of a layered approach. It is important for organizations to take a pragmatic approach to the layering of information. For example, it is reasonable that organizations rely on a privacy policy provided to the consumer when consent is requested for routine activities and a more directed, just-in-time notice could be triggered for things that are outside an individual's reasonable expectations.

It would also be helpful for the guidelines to clarify how organizations should track deemed consent, which is presumably tracked by keeping records of disclosure of purposes, and individual's subsequent provision of personal information.

⁷ R. v. Singh, [2007] 3 SCR 405.



For questions or comments regarding this submission, please contact:

Sara Clodman VP, Public Affairs and Thought Leadership sclodman@theCMA.ca Fiona Wilson Director, Public Policy & Chief Privacy Officer fwilson@theCMA.ca

About the Canadian Marketing Association

The CMA is the voice of marketing in Canada and our purpose is to champion marketing's powerful impact. We are the catalyst to help Canada's marketers thrive today, while building the marketing mindset and environment of tomorrow.

We provide opportunities for our members from coast to coast to develop professionally, to contribute to marketing thought leadership, to build strong networks, and to strengthen the regulatory climate for business success. Our Chartered Marketer (CM) designation signifies that recipients are highly qualified and up to date with best practices, as reflected in the Canadian Marketing Code of Ethics and Standards. 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. For more information, visit thecma.ca.