

# Submission by the Canadian Marketing Association on the Exploratory Consultation on Age Assurance By the Office of the Privacy Commissioner

September 2024



#### Introduction

The Canadian Marketing Association (CMA) is the voice of the marketing profession, representing corporate, public and not-for-profit organizations across Canada. We help marketers and their organizations maintain high standards of conduct and transparency through our Canadian Marketing Code of Ethics & Standards, our extensive resources on laws and best practices, and our training and professional development programs, including the Chartered Marketer (CM) professional designation. Through our Code and compliance materials, we have been a leader in setting standards for marketing to children and youth for decades.

We appreciate the opportunity presented by the Office of the Privacy Commissioner of Canada (OPC) to provide comments on the OPC document: Privacy and age assurance – Exploratory Consultation.

The CMA has long recognized that marketing to children and teenagers imposes a special responsibility on marketers, recognizing that not all marketing techniques are appropriate for them. An entire chapter of the CMA's <u>Canadian Marketing Code of Ethics & Standards</u> addresses special considerations for communicating with children and teenagers. The Code recognizes that with respect to the processing of their personal information, children have very different needs and capabilities than teenagers, who may bear many of the responsibilities and enjoy many of the privileges of adults.

We support reasonable and appropriate measures to protect young people online. The focus of our submission is on safeguarding young people's data in the context of its collection and use for commercial activities while also recognizing the legitimate needs of young people to access information online and engage in legitimate communications with organizations.

#### Insights and recommendations

The consultation paper seeks additional context to inform the OPC in its future work to champion children's privacy rights. In response, we offer the following insights and recommendations:

## **Data minimization**

Data minimization is a fundamental principle in privacy law that requires organizations to collect, use and retain only necessary and relevant information to achieve a legitimate purpose.

There are significant risks associated with collecting or assessing age and birth date, since breaches of these systems can lead to identity theft, fraud and other malicious activities. The less information an organization has about purchasers' age or birth year, the more purchasers (whether children or adults) are protected from a variety of online harms.

Applying the data minimization principle to protecting children in this context suggests that the child's age should be collected or inferred only when it is directly relevant to the product, use or service that is being provided or offered.

Many organizations, or types of organizations, have no knowledge about 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:

• When an individual visits an online local clothing boutique to purchase sunglasses, it is not important for the business owner to know whether the purchaser is 15 or 50.



- When an individual is searching for information on most topics, it should not be necessary for the search
  platform to estimate or verify the person's age. For example, it is not necessary or relevant for the
  search platform to know whether the individual researching a historic event, or an environmental cause
  is a student working on a school assignment or a professor teaching a history or environmental studies
  lesson.
- Professional sports teams maintain websites with player bios, team stats and schedules, video
  highlights, and online stores. They often collect browsing information (through cookies and related
  analytics technologies) and allow fans to sign up for additional content and promotional material through
  email. They collect and use fairly innocuous, non-sensitive data to promote their brand, and have no
  need or interest in knowing the age of their visitors or addresses. Nor is there any public policy rationale
  for treating any personal information of fans who happen to be minors differently from adult fans.
- Many types of organizations do not deal with or interact with young people including business-tobusiness services, and educational platforms and resources designed for use in schools.
- It would be a paradox for an anonymous web browser, the purpose of which is to allow users to access
  the internet without revealing their IP address or location, to use age assurance technologies on their
  users.

We submit that OPC guidance in this area should focus on:

- organizations whose business is focused on minors,
- organizations who know, or should be deemed to know, that they are processing the personal information of minors, such as in the case of a toy manufacturer, and
- organizations who offer products or services intended for adults only.

Focusing guidance on these types of organizations would be consistent with the approach taken by the Children's Online Privacy Protection Act in the US,<sup>1</sup> as well as by privacy laws in California<sup>2</sup> and the EU,<sup>3</sup> and would avoid targeting organizations that may only incidentally and unknowingly process the data of minors.

If guidance applies to organizations who are not directing their communications to minors, then many organizations will feel compelled to take steps to verify the age of **all** customers/users for no other reason than to confirm whether they are minors. They would also feel compelled to retain the data order to demonstrate compliance in the event of a complaint or investigation by the OPC. This would increase unauthorized access and disclosure risks for both the affected individuals and the organization.

1

<sup>&</sup>lt;sup>1</sup> See <u>Children's Online Privacy Protection Rule, 16 CFR Part 312</u>. 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.

<sup>&</sup>lt;sup>2</sup> The <u>California Consumer Privacy Act of 2018, California Civil Code § 1798.120</u>, 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.

<sup>&</sup>lt;sup>3</sup> Article 8 of the <u>General Data Protection Regulation (Regulation (EU) 2016/679)</u> 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.



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. The personal information required to verify age (e.g., government-issued ID with birthdate) is among the most sensitive information about an individual. It carries the greatest adverse risk in the event of a breach and is most sought after by criminals.

The necessity to collect and retain such sensitive personal information would impact the customer experience and create additional 'friction' to engagement. It would also introduce substantial – and potentially unworkable – business costs and complexity, without a strong privacy rationale or apparent enhancement of privacy protection for the minors that may incidentally use the service.

Some businesses might find it necessary to end services and offerings for customers who do not provide birthdates or ID, and this could inadvertently exclude seniors and vulnerable populations from access to important products and service.

In extreme cases, where the business complexity, implementation costs and potential regulatory risk outweigh any perceived benefit of providing products and services to consumers that happen to be minors, some businesses may decide not to service minors. Given that minors could be old as 18 in some provinces – as well as the philosophy that seems to be gaining traction of setting the age-gate at 21 to provide a buffer given that age assurance technologies are not completely accurate – this could have a particularly negative impact on the offerings available for young adults, as well as mature minors, who otherwise have many of the rights and obligations of adults.

# Treatment of young minors vs. mature minors

Guidance in this area should allow organizations to consider the needs and capabilities of **mature minors**, who may bear many of the responsibilities and enjoy many of the privileges of adults (such as applying online for post-secondary education and jobs, driving a vehicle, voting in elections, and being tried as an adult). Age verification should not be required in these situations.

It is particularly important to note that in seven provinces and territories, the age of majority is 19 years of age, meaning that individuals as old as 18 are still legally considered to be "minors". Guidance that permits organizations to consider "the needs and capabilities of minors" would use provincial ages of majority as a starting point, but there would be flexibility when dealing with mature minors, while still providing strong protections for younger children. This approach is in accord with laws in other jurisdictions that focus protections on younger children, 4 as well as with the Canadian Marketing Code of Ethics & Standards.

## Situations that pose a high risk of harm

The relevance of age shifts when the products or services being sold are intended for adults only. In these cases, the potential risk of harm of exposing children to the products and services may be greater than the harm that could result from the collection and storage of their age-related data.

In this context, we agree with the OPC's preliminary position that the use of age-assurance systems should be restricted to situations that pose a high risk to the best interests of young people and must consider impacts on the privacy rights of both young persons while ensuring the right to information of adult users of the online services.

<sup>&</sup>lt;sup>4</sup> For example, the Children's Online Privacy Protection Act in the US applies to operators of commercial websites and online services directed to children under 13 years of age, or knowingly collecting personal information from children under 13. The GDPR requires parental consent for the processing of the personal information of children under age 16 by an information society service provided directly to a child.



## Impact on small and medium-sized businesses

All businesses are negatively impacted when laws and regulations are overly restrictive. Overregulation of any kind risks stifling innovation and growth across the business spectrum potentially hampering Canada's economic success.

While larger corporations may have more resources available to mitigate the impact, the challenges can be particularly acute for SMEs, as they often operate on tighter margins and with limited staff. Biometric analysis, third-party verification systems and other advanced age assurance technologies are usually expensive to obtain, integrate and maintain.

For some SMEs, the only way to comply with mandatory requirements would be to retain vendors who could oversee the purchase, set-up and maintenance of a company's age assurance system, diverting funds intended for other programs or initiatives, which could hamper innovation, product development, and growth strategies. This would hinder their growth and sustainability in a highly competitive market.

Our recommendations throughout this paper aim to ensure that the policy objective of protecting minors is met in a manner that ensures that compliance does not become an obstacle to business operations and growth. A measured approach would achieve a competitive landscape where businesses of all sizes can thrive while still protecting young people from risks of significant harm.

## Assessment criteria

The guidance could identify criteria to help organizations assess the necessity of determining or estimating the age of online visitors/customers. Criteria might include:

- Necessity: Is age assurance necessary given the nature of the product or service being offered? This is
  particularly relevant when the business would not otherwise collect, or need to know, the person's age.
- Exposure: Is there a reasonable risk of significant harm (RROSH) to young people that would warrant having their age identified and protected?
- Effectiveness: Will the proposed age assurance method effectively mitigate the identified risks?
- Proportionality: Is the age assurance method proportional to the level of risk implicit in the collection and retention of age-related data?
- Privacy Impact: Does the age assurance method minimize data collection and protect user privacy?

These criteria could be used by organizations to develop a privacy impact assessment.

#### Use of age assurance to limit exposure

One of the OPC's preliminary positions is that organizations should be required by default, in all cases, to demonstrate why it is necessary to use a particular age assurance technique to protect young people from certain data practices, rather than choosing a data practice that is appropriate for people of all ages.

It is important to recognize that many organizations who are aware that they are processing the personal information of minors are already taking steps to protect them.



For example, on a video site, content recommendations for adults could be based on factors such as the person's watch history, search history, likes and dislikes – provided they have consented to data collection and personalization.

However, the same site would not likely retain this type of data from users who were identified as children. It would instead suggest curated content suitable for children, and recommendations based on a video being watched, rather than a user profile based on a history of viewed content. For example, a child watching an educational video about dinosaurs might see an ad for a local museum's dinosaur exhibit, but this ad is based on the video content, not the child's personal data.

## Margins of error in age estimation

All age assurance methods are imperfect and carry margins of error. There will always be a risk that a minor (especially a technically savvy mature minor) could access adult content by deliberately circumventing the system. At the same time, these technologies may deny adults rightful access because of technical errors or a lack of access to sufficient ID.

Acknowledging these shortcomings in available technologies means recognizing that companies making the best efforts to protect youth while balancing the privacy and access to information rights of all users cannot be held liable for cases that fall within those margins of error. Any liability imposed on organizations would inevitably support an overly cautious and restrictive approach to age assurance. This may result in content being overly blocked – including legal and appropriate content for adults.

#### **Education and Awareness**

It is important for young people to learn how to conduct themselves and protect themselves online, just as they need to learn to be financially responsible. We recommend that the OPC undertake an education and awareness program to promote online safety. Education can often be more effective and less intrusive than technical solutions. A campaign could be undertaken in collaboration with relevant organizations. The CMA would be pleased to participate in such an effort.

We look forward to further engagement on this important topic and would be happy to provide additional input as the OPC develops its guidance document.

For questions or comments regarding this submission, please contact:

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

Shreya Bali Senior Manager, Technology and Privacy Policy sbali@theCMA.ca