



THE CANADIAN  
BAR ASSOCIATION  
L'ASSOCIATION DU  
BARREAU CANADIEN

## **Privacy and Age Assurance – Exploratory Consultation**

**CANADIAN BAR ASSOCIATION  
PRIVACY AND ACCESS TO INFORMATION LAW AND CHILD AND YOUTH LAW SECTIONS**

**October 2024**

## **PREFACE**

The Canadian Bar Association is a national association representing 40,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Privacy and Access to Information Law and Child and Youth Law Sections, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Privacy and Access to Information Law Section.

## TABLE OF CONTENTS

### Privacy and Age Assurance – Exploratory Consultation

<b>I.</b>	<b>INTRODUCTION .....</b>	<b>1</b>
<b>II.</b>	<b>CBA COMMENTS TO OPC .....</b>	<b>1</b>
	A. Key points from consultation .....	1
	B. OPC preliminary positions .....	4
	C. Key terms .....	7
<b>III.</b>	<b>CONCLUSION .....</b>	<b>8</b>



# Privacy and Age Assurance – Exploratory Consultation

## I. INTRODUCTION

The Canadian Bar Association (CBA) is a national association of over 40,000 lawyers, law students, notaries and academics with a mandate to seek improvements in the law and the administration of justice. The CBA is made up of a broad membership with diverse views. This response includes comments from the CBA Privacy and Access as well as the Children and Youth Sections (CBA Sections). The CBA appreciates that the OPC has issued its Joint Statement on A Common International Approach to Age Assurance. We acknowledge this work and provide these comments in response to the original questions to the extent they continue to be helpful.

## II. CBA COMMENTS TO OPC

### A. Key points from consultation

1. Many jurisdictions, including Canada, have introduced or adopted legislation intended to increase the safety of young people in online spaces. This could mean, for example, that young people's access to certain content must be restricted or that their personal information must not be collected, used or disclosed in ways or for purposes set out in the legislation. This leads to the question – how can an online service determine whether a user is a young person, and thus subject to these restrictions?

CBA Sections comment:

- a. These two types of restrictions (access to content vs content provider's use of user PI) should be treated separately in privacy regulation and design, as well as legislation and enforcement. Mandatory age assurance raises different privacy and children's rights considerations than the optional use of such technology by organizations. As described below, facilitating the exercise minors' rights and freedoms must not be conflated with the responsibility of organizations to protect their personal information. Organizations have a heightened responsibility when seeking consent and handling the personal information of minors and other vulnerable communities for optional purposes. Meanwhile, the OPC can serve an important role in helping legislators avoid imposing mandatory personal information handling regimes on organizations that infringe on minors' privacy rights, freedom of expression and other fundamental freedoms that hinge on respect for privacy.

2. In some cases, the use of age assurance is mandated by law or regulation; in others, it is adopted by organizations as part of their overall compliance strategy.

CBA Sections comment:

- a. Mandatory and optional scenarios should be treated separately, but OPC has a role to play in both.
  - b. We note that in September 2024, UK's Information Commissioner's Office posted the Joint Statement on a Common International Approach to Age Assurance, signed by international partners, including the OPC. The CBA appreciates that it sets out 11 principles meant as a guide for industry in developing these systems. Broadly speaking, these principles are consistent with PIPEDA and they are infused with child rights considerations, including best interests of the child. The CBA envisions that industry will be encouraged to implement these principles, while more specific policy is developed.
3. This [age assurance] technique can also have impacts on privacy and other fundamental rights.

CBA Sections' Comment:

- a. The Privacy and Access Section is of the view that governments and the OPC must recognize that privacy is a core element in facilitating other fundamental rights (e.g. freedom of expression). The OPC is right to focus on this as its mandate is to protect privacy rights of all Canadian residents and especially those in vulnerable communities who may be disproportionately impacted by age assurance technologies that remove or reduce anonymity in internet access. The OPC plays a crucial role in reminding legislators that reducing privacy protections can limit access by equity-seeking communities to other fundamental rights. To that end, the CBA stresses that point 7 in the OPC's Joint Statement, regarding the right to safely access information online, is essential and not be overlooked while seeking to protect children from harmful online content.
  - b. The Children and Youth Section is of the view that governments and the OPC must consider all interests at play. Age assurance can have a positive impact on, or facilitate, the best interests of children and protect their right to life, liberty and security. Effective age assurance can help safeguard children from preventable harms such as online luring, sextortion and exposure to child sexual abuse and other criminal material. In accordance with the rights of the child under the United Nation's Convention on the Rights of the Child ("UNCRC"), this should be an important consideration for the OPC.
4. The goal of this consultation is to prompt meaningful discussion of this topic, and to increase our understanding of the benefits, concerns, and existing research or writing associated with age assurance.

CBA Sections' comment:

- a. The Privacy and Access Section says that intentional efforts should be made to seek comments from particularly vulnerable communities, including children, disability, Indigenous and 2SLGBTQ communities.
- b. Since age assurance is a matter that directly affects children, they have a right to be consulted under the UNCRC.
- c. The Children and Youth Section members says that there should be efforts to seek input from those supporting the well-being and safety of children, such as school counsellors, therapists, and helplines. These professionals have valuable information about the harms children and youth encounter online and the resultant impacts.
- d. Some members in the Privacy and Access Section express concern that the current political climate may allow certain moral codes to be imposed by individuals working within school institutions, overriding the right to freedom of expression. A balancing of interests is needed in these situations.
- e. The Children and Youth Section recommends reading the upcoming research paper in the International Journal of Child Rights on Child Rights and Online Age Assurance Systems, authored by Sonia Livingstone (London School of Economics and Political Science), Abhilash Nair (University of Exeter), Mariya Stoilova (London School of Economics and Political Science), Simone van der Hof (Leiden University) and Cansu Caglar (Aston University). The paper highlights the promise and the challenges of developing age assurance methods that keep children safe online in keeping with various rights. It synthesizes insights from three distinct methods:
  - A study of laws and regulations relevant to age assurance applicable to online content, and the gambling and sale of alcohol and tobacco online in the EU and UK;
  - A review of methods in the EU for obtaining parental consent while maintaining children's rights and
  - A rapid review of the evidence on age assurance and parental control tools from the perspective of children and families (using Preferred Reporting Items for Systematic Review and Meta-Analysis Protocol (PRISMA-P) guidelines to search five major multidisciplinary and subject-specific databases, identifying 1,656 results of which 61 remained for analysis after screening against the review criteria).

The authors suggest that age assurance, together with privacy and safety-by-design, can provide children with age-appropriate digital opportunities and protections. They also suggest that a range of child rights approaches can be useful, including robust evaluations, child consultation and participatory design. More generally, the OPC should also consider General Comment No. 25 on children's rights in relation to the digital environment, issued by the UN Committee on the Rights of the Child in 2021, and the

2021 Report of the Special Rapporteur on the right to privacy regarding Artificial Intelligence and privacy, and children’s privacy.

- f) The Children and Youth Section recommends, based on the above-noted upcoming review and Mukherjee et al.’s Child Rights Impact Assessment: A Tool to Realise Children’s Rights in the Digital Environment, that the OPC consider including child rights impact assessment (CRIA) in legal age assurance requirements for digital services. In July 2023, Justice Canada launched a CRIA tool and e-learning course that, while primarily aimed at federal officials, can also be used by other governmental or non-governmental organizations, or by others seeking to assess the impact of initiatives on children’s rights. The Child and Youth Law Section notes that child rights approaches are currently not well understood by digital provides and internet governance policymakers in Canada.
- g) The Privacy and Access Section recognizes that privacy impact assessments are important tools in a privacy tool kit and that a child focused impact assessment could be effective. However, they recommend that the OPC consider the potential regulatory burden. Requirements should be proportional to the level of risk. Some members argue that the OPC’s statement of principles strikes an appropriate balance:

“Providers should assess and document the severity of the potential data protection risks to users, and particularly children, from the age assurance method(s) implemented.”

## **B. OPC preliminary positions**

- 5. It is possible to design and use age assurance in a privacy-protective manner. However, this does not mean that the use of age assurance will be necessary to the same extent in all circumstances.

CBA Sections’ comment:

- a. The Privacy and Access Section says it may be possible to design and implement age assurance technologies that are less privacy-invasive than others. However, there is limited evidence that scalable technologies exist that are truly privacy protective, meaning that a careful balancing of necessity, harm-reduction, invasiveness and impact on other rights is still required.
- b. The Children and Youth Section refer the OPC to the Livingstone research paper mentioned above.
- c. As the OPC notes, the Privacy and Access Section says that limiting the collection of personal information to what is necessary for the identified purpose should be central to any analysis of implementing such technologies. When assessing the appropriateness of data collection, the impact on individual and community privacy and other rights should be carefully weighed against the potential benefits to children and youth associated with these measures.
- d. Similarly, the Children and Youth Section says the collection of young peoples’ personal information for access to services should be assessed in light of the impact on their privacy and the purposes of collection. Organizations should ensure they implement the appropriate form of (1) notice (in the case of mandatory age



assurance) and (2) consent (in the case of optional age assurance) based on the context and type of personal information being handled. Consideration should also be given to the ability of young people of varying ages and people with disabilities affecting their capacity to give meaningful consent in the design of notice and consent mechanisms.

6. In our preliminary opinion, 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 and adult users of the online service.

CBA Sections' comment:

- a. The Privacy and Access Section says that while legislators must consider the risks to youth when deciding whether and when to mandate age assurance systems, organizations that voluntarily choose to implement them must also take this into account when collecting personal information. The OPC should be firm in its oversight role, focusing on the privacy impact and invasiveness of personal information and the direct identification of users, whether such systems are mandated or adopted voluntarily.
- b. We refer to our comment above regarding the potentially disproportionate impact of both mandatory and optional age assurance on equity-seeking communities, including children, and intentional efforts should be made to consult with these communities.
- c. The Children and Youth Section emphasizes that all parties involved must be informed about and consider the risks to youth, including legislators deciding whether and when to mandate age assurance systems, organizations voluntarily implementing them, and the OPC in its oversight role. The OPC should assess the privacy impact when such systems are mandated or voluntarily adopted. It is incumbent upon the OPC to strike the right balance, recognizing that under the UNCRC the best interests of children are a State obligation and that all rights are inclusive, indivisible and interdependent. Regard should also be had to the Children's Rights and Business Principles developed by the UN Global Compact, UNICEF and Save the Children. The Principles define the scope of corporate responsibility towards children, calling on companies to respect children's rights through their core business actions, but also through policy commitments, due diligence and remediation measures.

7. Moreover, legislation or regulations requiring the use of age-assurance systems to restrict young people's access to content:

Should be proportionate to the risk and have taken into account potential alternative means of restricting access to content such as education, device-level parental controls, or individual or household-level Internet filtering technologies.

## CBA Sections' comment:

- a. The Privacy and Access Section states this is a critical point. Even where age declarations without proof are easy to circumvent, they serve an important awareness and education function in some contexts. They can achieve the same objectives as age assurance systems without collecting personal information. The OPC has a significant role to play in assisting governments, community groups and businesses enhance education for parents, caregivers, educators and young people. The OPC should also engage in dialogues about whether potentially harmful content is a risk solely to young people or to the public at large.
  - b. Further, the OPC should consider the long history of Canadian common law, legislation and social development, which shows that objectively determining what content is harmful to youth or other groups is extremely difficult and subject to political agendas of the time. These agendas may not align with Charter rights or the best interest of children and youth as well as their rights to freedom of expression and to access information and material from a diversity of sources. Political and regulatory dialogues about the pros and cons of access to various types of content and age-related considerations must remain neutral and rights-focused. As an example, the OPC should be concerned about the impact on privacy and other rights if age assurance legislation were to restrict a child's access to content about varying gender expressions and sexual orientations (or related health care and social services) simply because a government deemed it not age appropriate. Such restrictions would require a different rights analysis.
8. As well, the use of age assurance to limit the exposure of young people to data practices that might negatively influence their behaviour or cause them harm:

Should require that an organization demonstrates the necessity of applying those practices by default.

That is, organizations should be required to justify why a particular age assurance technique is a more appropriate option than, for example, assuming all users are young people and applying appropriate practices.

## CBA Sections' comment:

- a. The OPC should also play an important role in reminding governments, organizations and the public of the need for integrated solutions that safeguard all individuals from data practices that could negatively influence behaviour or cause harm. Individuals with disabilities, even if they have reached the age of majority, may still require heightened protections as a result of their ability or inability to provide consent. Similarly, some young people of the same age will have varying understandings of risks, options and their privacy rights depending on their family, community and social surroundings.
9. Finally, age-assurance systems:
- Should be designed to minimize the identifiability of users and the ability to link users across services;

CBA Sections' comment:

- a. The Privacy and Access Section says this will be a challenging balance at both the federal and cross-jurisdictional levels. Will age verification be required every time an individual wishes to access restricted content or services, resulting in repeated collections of personal information? Or will confirmation of previous age verification be stored on a device or site? How do these approaches align with Quebec and other regions' regulations of the use of profiling and identification technologies? If neither is a good privacy option, it may indicate that the objectives of age verification do not outweigh the invasiveness of the privacy impact. Interoperability and privacy impact assessments should be central considerations.
- b. Should not permit information collected for age-assurance purposes to be used for other purposes;

CBA Sections' comment:

- a. The Privacy and Access Section says that law enforcement authorities in domestic and foreign jurisdictions may have lawful access to such personal information collected by organizations for age-assurance purposes. Similarly, even with such regulations this data could be vulnerable to unauthorized access and disclosure through privacy breaches and cyber-attacks. Depending on the context of the content, organization or political environment, this could have significant impacts on individuals (e.g. exposing sexual orientation, gender identity, reproductive health care or other sensitive personal information about individuals who could face significant legal, social, educational and family consequences from such breach).
- b. This should factor into whether, and which, such systems should be used at all; and the focus should not be entirely on what organizations may choose to do with the personal information.

### **C. Key terms**

10. Age estimation: The individual's age is estimated based on an analysis of biometrics or behaviours, generally performed by an artificial intelligence system.

CBA Sections' comment:

- a. The Privacy and Access Section says: the OPC is no doubt mindful, and cautious about age-assurances technologies that engage AI systems to assess eligibility for services, given that bill C-27/AIDA is still pending in Parliament and Canadian organizations are operating in an AI regulatory vacuum. The OPC has an important role to play in educating legislators, organizations and the business community about the dangers of implementing AI systems that can process highly sensitive personal information to deny individuals access to services and public content, particularly when the rules for doing so responsibly have not been finalized.
11. As such, by design an age estimation system will reject (or refer to an alternative assurance method) a number of individuals who are above the threshold age for the restriction, but below the buffer age.

CBA Sections' comment:

- a. The Privacy and Access Section says the OPC should be especially cautious about proposals to implement such systems, which could result in the double collection of sensitive personal information – first through biometric data (which comes along with known concerns of inequity in training and implementation) and then through identification, image or other verification methods if the individual does not pass the biometric method.
12. Age assurance can pose equity issues: In general, age verification methods will rely on the individual having access to an authenticated identity (a government-issued ID; an account with a trusted party, such as a bank; etc.). This may pose challenges for groups who do not have ready access to such identifiers, including younger teenagers (in situations where those over 13 are permitted access to content or a service), unhoused or unbanked individuals, or non-citizens. Age estimation techniques (such as facial analysis) have also faced issues with respect to inconsistent performance across skin tones and genders.

CBA Sections' comment:

- a. These are significant issues, and as mentioned above, efforts should be made to get input from these groups, children and advocacy organizations that work with them. The harms of denying vulnerable individuals and communities' access to content or services as a result should weigh heavily against the risks of harm to young people that such legislation or voluntary system seeks to avoid. As noted above, necessity should be a primary consideration. In many cases the objectives of the system will not outweigh the privacy, equity and other human rights impacts of implementing it.

### **III. CONCLUSION**

The CBA appreciates the opportunity to contribute to the OPC's work on age assurance and is eager to work with the OPC to share constructive feedback throughout the consultation process.