Response by the Centre for Information Policy Leadership to OPC's Exploratory Consultation on Privacy and Age Assurance

Submitted September 10, 2024

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Exploratory Consultation on Privacy and Age Assurance by the Office of the Privacy Commissioner of Canada (OPC).[2]

CIPL supports the OPC's effort to prompt meaningful discussion on this topic in order to understand the benefits and challenges associated with age assurance. In our 2022 white paper on children's data privacy,[3] CIPL identified age assurance as one of the key issues relating to children's data and online engagement. We subsequently held a roundtable on age assurance and age verification tools in 2023,[4] and in 2024, together with WeProtect Global Alliance,[5] we launched a multistakeholder dialogue to further drive the discussion.[6] We incorporate by reference the white paper and takeaways produced as a result of our research and meetings, and we invite the OPC to participate in our future discussions.[7]

---

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-age/expl_gd_age/.

[3] CIPL Policy Paper - *International Issues and Compliance Challenges*, Oct. 2022, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-_international_issues___compliance_challenges__21_oct_2022_.pdf.

[4] Key Takeaways from CIPL Roundtable on Age Assurance and Age Verification Tools, March 16, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/takeaways_from_cipl_roundtable_on_age_assurance_and_age_verification_tools__16_march_2023_.pdf.

[5] The WeProtect Global Alliance is an independent organization—registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK—that brings together over 300 members from governments, the private sector, civil society and intergovernmental organizations to develop policies and solutions to protect children from sexual exploitation and abuse online. See https://www.weprotect.org/about-us/who-we-are/.

[6] A Multi-Stakeholder Dialogue on Age Assurance: Key Takeaways, May 15, 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf. A Multi-Stakeholder Dialogue on Age Assurance: Law and Regulation, July 11, 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_key_takeaways_age_assurance_law_and_regulation.pdf.

[7] CIPL has extended an invitation to the OPC to join an event to be held September 25, 2024, in San Francisco, California.

OPC Preliminary Positions

1. **"Privacy-Protective"**

   OPC Position: "In general … we take the position that 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."

CIPL agrees with the OPC's preliminary position that use of age assurance measures and technologies can be done in a privacy-protective manner. However, to address this issue, we will first need to develop a common understanding of what "privacy-protective" means in practice.

For example, a prohibition on the ***retention*** of identifying information could be regarded as "privacy-protective" in relation to data in the possession of an entity. Indeed, many U.S. state laws requiring the use of age assurance measures to prohibit minors from accessing pornographic material online also prohibit online publishers from retaining any identifying information collected for purposes of ensuring that website visitors are over 18.[8] Ongoing legal challenges to such laws argue (among other things) that a prohibition on *retention* fails to cover ***transmission***,[9] including to the government, thereby raising individuals' concerns of "state monitoring" of "what kind of websites they visit."[10] Given such concerns, it would be helpful for the OPC to provide guidance on "privacy-protective" features, capabilities, and guardrails for organizations to consider when deploying appropriate age assurance tools. The OPC should also offer guidance as to how organizations can implement privacy-enhancing technologies (PETs) in this context and incentivize their development and adoption where feasible and appropriate.

2. **High Risk and Best Interests**

   OPC Position: "[T]he use of age-assurance systems … [s]hould be restricted to situations that pose a high risk to the best interests of young people …."

CIPL agrees that the deployment of age assurance should follow a **risk-based approach**, but any risk assessment must be context-specific. Whether age assurance systems should be restricted to situations that pose only **high risk** will depend on the context of a given situation, as there may be lower (but not "low") risk situations that would still warrant the use of age assurance tools. Indeed, "hard" age verification could be limited to high-risk situations, but age assurance could be appropriate in lower risk situations, for instance monitoring whether there are users in a lower age range accessing higher age range content. Other mitigation measures will also have an impact on whether age assurance remains potentially necessary.

There is no one-size-fits-all approach to age assurance. The utility and suitability of different age verification or assurance methodologies will depend on the risk context of the underlying service(s), or how and on what type of device the service is likely accessed. Moreover, services providing layered

---

[8] See, for example, Tex. Civ. Prac. & Rem. Code § 129b.002(b): "A commercial entity that performs the age verification required by Subsection (a) or a third party that performs the age verification required by Subsection (a) may not retain any identifying information of the individual."

[9] See *Free State Coalition v. Paxton*, Petition for a Writ of Certiorari (filed April 12, 2024; granted July 2, 2024). U.S. Supreme Court Docket No. 23-1122, available at https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/23-1122.html.

[10] *Id.*, Petition for a Writ of Certiorari, p. 9.

functionalities might require layered age assurance (i.e., age assurance requested at different access points) and/or the use of multiple methodologies at different stages.

As the OPC notes in its Exploratory Consultation, there is a growing body of work that examines the relationship between privacy and age assurance, or that proposes principles to ensure appropriate use of the technology. But it is important to note that age assurance cannot be viewed solely from a privacy perspective; safety considerations in particular must also be taken into account. While CIPL is not recommending the OPC to look at issues beyond its remit, the OPC must understand that organizations using age assurance tools must look beyond privacy concerns, especially when conducting risk assessments. While the OPC's Exploratory Consultation highlights useful guidance released by several data protection authorities in Europe,[11] there is no consensus on a **taxonomy of risks** or factors to consider when conducting an appropriate risk assessment.

Moreover, while age assurance is a tool to keep children safe online, it also has an exclusionary element by keeping children away from certain online content. Age assurance tools must therefore carefully consider the **best interests of the child** as enshrined in the UN Convention on the Rights of the Child,[12] which Canada has ratified. The UN's Committee on the Rights of Child General Comment No. 25[13] provides guidance on the considerations to be taken into account in the digital environment, including the rights of children "to seek, receive and impart information, to be protected from harm and to have their views given due weight."[14] Different maturity levels must be considered, since the best interests of a 5-year-old will not necessarily be the same as that for a 14-year-old in a given context. While interpretations of "best interests" can vary widely from culture to culture, family to family, and child to child, from a policymaking perspective, the "best interests" standard should be applied with consideration of what is generally applicable at a given stage of development.

It would be helpful for the OPC to clarify that risk assessments must be **context-specific** and that any risk assessment should consider both the **likelihood** and **severity** of a risk of harm as well as the benefits to the child (as part of the consideration of best interests).

3. Privacy Rights

OPC Position: "[T]he use of age-assurance systems ... [m]ust consider impacts on the privacy rights of both young persons and adult users of the online service."

---

[11] Agencia Española de Protección de Datos (AEPD) – Decalogue of Principles – Age verification and protection of minors from inappropriate content, (December 2023), available at https://www.aepd.es/guides/decalogue-principles-age-verification-minors-protection.pdf; Commission nationale de l'informatique et des libertés (CNIL), Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy, (August 2021), available at https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy; Online age verification: balancing privacy and the protection of minors, (September 2022), available at https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors; UK Information Commissioner's Office, Age Assurance for the Children's Code, available at https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/.

[12] Convention on the Rights of the Child, available at https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child. Canada ratified the Convention in 1991.

[13] General comment No. 25 (2021) on children's rights in relation to the digital environment, available at https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

[14] *Id.*, paragraph 13.

CIPL agrees that age assurance systems should consider impacts on the privacy rights of both young persons and adult users.

With regard to adult users, CIPL supports the use of age verification measures for situations comparable to those where adults must provide or are accustomed to providing proof-of-age in brick-and-mortar interactions. That said, the type of verification used in the online context will depend on the risks at issue and the harms sought to be mitigated. Again, the use of privacy-enhancing technologies (PETs) should be encouraged where feasible and appropriate.

4. Proportionality

> *OPC Position: "Legislation or regulations requiring the use of age-assurance systems to restrict young people's access to content ... [s]hould 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."*

CIPL agrees that the use of age assurance systems should be proportionate to the level of risk. For example, choosing a hard age verification method where the estimation of an age range would suffice could result in the disproportionate collection of personal data. Indeed, disproportionate collection of personal data (from age verification or even from precise age inference requirements) could hinder or potentially break pseudonymous and anonymous experiences, which are pro-privacy. Identifying the most appropriate method means balancing its effectiveness with privacy protections. It must be context-specific to the risk(s) being addressed.

Moreover, the OPC should recognize that risks can change over time as services develop and new threats or benefits emerge in the online environment. This means that risk assessments must be systematic and repeatable. CIPL has been on the forefront of promoting organizational accountability, and the iterative process of reassessing risks is a fundamental feature of CIPL's Accountability Framework.[15]

CIPL also agrees that laws and regulations incorporating age assurance obligations to create safe spaces for children cannot rely on age assurance alone. It is not a panacea. Keeping children safe online and protecting their privacy and other rights will require a combination of measures to ensure compliance with various data protection and other legal requirements and regulatory guidance, such as privacy and safety by design and default, appropriate user-centric transparency, content moderation and personalization of content, parental consent for certain ages and family-specific controls, and age-appropriate services (or child-friendly spaces within services).

5. Choosing an Appropriate Method

> *OPC Position: "[T]he use of age assurance to limit the exposure of young people to data practices that might negatively influence their behaviour or cause them harm … [s]hould 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."*

---

[15] See CIPL Organizational Accountability Project, available at https://www.informationpolicycentre.com/organizational-accountability.html.

When it comes to choosing a particular method or combination of solutions, CIPL believes that companies should be able to demonstrate why a particular method or combination of solutions is effective and in the best interests of children, given the context of their service. Organizations should be ready to provide evidence of risk mitigation and efficacy. Moreover, as noted above, regardless of the method(s) chosen, CIPL supports the use of other measures in conjunction with age assurance to keep children safe online and protect their rights.

Given the rapid pace of development of available technologies, the OPC should consider creating a safe harbour or a limitation of liability for companies that have adopted specific measures pursuant to a proper risk assessment.

6. Data Minimization

OPC Position: "[A]ge assurance systems … [s]hould be designed to minimize the identifiability of users and the ability to link users across services ….

While age assurance is part of digital safety by design, solutions must also come from a privacy by design approach. Data minimization, storage limitation, and data security must be balanced against the necessity to process data in line with the perceived risk. It is imperative that those responsible for safety, security and privacy within organizations cooperate to determine the appropriate balance.

That said, the OPC should recognize that solutions for age assurance involve different actors in the online ecosystem, viz., telecommunications providers, online platforms, device manufacturers, app stores, and individual apps. Proposals to streamline the process for the benefit of users include browsers, app stores, or device OS as opportunities to establish age at a central point of contact, thereby fostering interoperability. While this has the advantage of building on some already existing infrastructures, such an approach would need to carefully balance a number of challenging issues including privacy, security, competition concerns, costs and liability. Workable solutions will have to carefully address all these concerns.

Beyond interoperability, there may be situations where operators may wish to identify users across services, such as in the case of identifying child predators.

7. Purpose Limitation

OPC Position: "[A]ge assurance systems … [s]hould not permit information collected for age-assurance purposes to be used for other purposes ….

Generally speaking, CIPL would not support a blanket prohibition on the use of information for purposes other than age assurance, as certain contexts may warrant the use of such information for compatible or related purposes, such as for the protection of minors or for the improvement of the given age assurance methodology. While PIPEDA limits the use of personal information to the purposes identified at or before the time of collection,[16] Québec's Law 25 permits the use of personal information for another purpose "if it is used for purposes consistent with the purposes for which it was collected."[17] To the extent there may be conflicting standards within Canada, the OPC should, together with the Commission d'accès à l'information du Québec, clarify whether and to what extent

[16] Personal Information Protection and Electronic Documents Act, Schedule 1, Section 4.2

[17] Act respecting the protection of personal information in the private sector, Section 12.

those using and/or deploying age assurance technologies may use information for compatible or related purposes. Ideally, in CIPL's view, a **risk-based approach** would include a consideration of compatible or related purposes.

8. Industry Standards

OPC Position: "[A]ge assurance systems … [s]hould be designed in accordance with relevant industry standards and guidance from regulators (including the OPC) and be subject to effective oversight ….

CIPL notes that industry standards should be developed in a collaborative way, with the participation of all stakeholders (industry, policymakers, regulators, civil society) in a manner that leaves flexibility for change in this area of rapid technological development. Standards are needed to ensure a more ready and systematic adoption of appropriate tools and techniques, and ultimately to ensure greater protection for children and youths online. As mentioned in our introduction, CIPL has partnered with WeProtect to drive a multistakeholder dialogue on age assurance, which includes the development of standards, technology, and partnerships. CIPL would welcome the OPC's participation in these efforts.

Many organizations, especially the larger ones, have made serious investments and commitments to develop best practices for age verification and assurance. They are testing available age assurance methods and exploring new solutions, for instance through participatory design testing. As research and with it our understanding evolves, it is imperative that all stakeholders continue engaging and sharing in ongoing dialogue regarding expectations and progress. The OPC will need to ensure that its guidance on standards is future-proof and flexible enough to permit adoption of new and developing technologies.

Moreover, there will be a need for further developments of standards and certifications that are accepted throughout multiple jurisdictions and by multiple organisations. As laws and regulations across the globe are considering and sometimes requiring the use of age assurance or age verification measures, it is increasingly important to develop an interoperable set of regulatory standards. No government can satisfactorily address age assurance in isolation. Cooperation at the international level is essential to promote online experiences for children and young people that meet their best interests and accord with the rights and freedoms of all users.

As CIPL has noted in the context of data protection, global interoperability enables responsible provision of services across borders, broadens access, reduces compliance costs, increases legal certainty, and ensures consistent protection of the rights and interests of individuals.[18] Different jurisdictions will have their own priorities, legal traditions, and body of existing regulation, but they may be able to coalesce around core principles and approaches in considering age assurance. They can also take steps to codify interoperability through recognition and certification mechanisms.

9. Access Restrictions

OPC Position: "[A]ge assurance systems … [s]hould not require individuals to undergo an age assurance process to access non-restricted content.

---

[18] CIPL, "Ten Principles for a Revised US Privacy Framework," March 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_principles_for_a_revised_us_privacy_framework.pdf.

Any requirement to undergo an age assurance process for non-restricted content would be neither proportionate nor privacy-protective. With the adoption of a **risk-based approach**, age assurance systems would not be deployed in situations where the likelihood and severity of risk are minor.

10. CIPL Resources.

CIPL encourages the OPC to review our following papers:

- Protecting Children's Data Privacy, Policy Paper I - *International Issues and Compliance Challenges*, Oct. 2022, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-_international_issues___compliance_challenges__21_oct_2022_.pdf.
- *Key Takeaways from CIPL Roundtable on Age Assurance and Age Verification Tools*, March 16, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/takeaways_from_cipl_roundtable_on_age_assurance_and_age_verification_tools__16_march_2023_.pdf.
- *A Multi-Stakeholder Dialogue on Age Assurance: Key Takeaways*, May 15, 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf.
- *A Multi-Stakeholder Dialogue on Age Assurance: Law and Regulation*, July 11, 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_key_takeaways_age_assurance_law_and_regulation.pdf.