September 9, 2024

Office of the Privacy Commissioner of Canada
30 Victoria St.
Gatineau, QC K1A 1H3

RE: Age assurance exploratory consultation - call for comments

To Whom It May Concern:

The Future of Privacy Forum (FPF) is pleased to submit comments to the Office of the Privacy Commissioner of Canada (OPC) regarding their age assurance exploratory consultation. FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.[1] FPF welcomes this opportunity to respond to the OPC's invitation for preliminary comment.

In general, FPF considers the OPC is appropriately approaching age assurance in a nuanced, informed, and balanced way, especially by highlighting in its preliminary positions: the privacy risks associated to age assurance systems, that age assurance systems should be proportionate to the privacy and access risks, the need to support strong privacy by design, and the potential for inequitable outcomes. Given the OPC's preliminary positions, the Future of Privacy Forum submits the following recommendations:

1. **An existing legal framework is necessary for the efficacy and enforceability of the Guidance Document, as well as for FPF and others to provide the most helpful recommendations, recognizing that in the absence of a legal mandate, age assurance should only be used when strictly necessary and only to prevent particular harms.**
2. **The Guidance Document should distinguish among and describe the age assurance methods available and highlight for each use case the risks involved, rejecting a one-size-fits-all approach in favor of an age assurance method proportionate to the risks of each use case.**
3. **The Guidance Document should recognize data minimization as a key mitigation measure to deal with privacy risks of age assurance systems.**
4. **The Guidance Document should analyze each specific use case for potential inequitable impacts, especially access equity.**

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.

1. **An existing legal framework is necessary for the efficacy and enforceability of the Guidance Document, as well as for FPF and others to provide the most helpful recommendations.**

FPF recognizes that the insight gathered in the OPC's call for comments "will support the next step(s) of [the OPC's] work, which will include the creation of a draft guidance document about the use and design of age-assurance systems." Given that the OPC intends to undertake "policy and guidance work" on the use, development, and design of age-assurance technologies, FPF recommends prioritizing using the insight gathered to support policymakers in the creation of laws and regulations surrounding age assurance. Having a legal framework in place adds enforceability and efficacy to guidance surrounding the use, development, and design of age assurance technologies. Without a parliamentary mandate, age assurance systems might not be necessary in Canada and may not be successful, and any future guidelines should recognize that **age assurance should only be used when strictly necessary and only to prevent particular harms**.

Legal requirements and legislative context surrounding age assurance in Canada are needed to determine whether the use of age assurance systems are necessary in Canada from the outset, and are also necessary for more specific and tailored recommendations. Compliance recommendations and analysis of risks and harms become more effective when lawmakers have weighed in. For example, in a bill currently being considered in Parliament – Bill S-210: *An Act to restrict young persons' online access to sexually explicit material* – lawmakers offer context to the discussion of age assurance by detailing the harms of the consumption of sexually explicit material by young people and by weighing those harms against privacy rights associated with age verification. Section 11(2)(a) of the bill would require that the technology be reliable. In this case, FPF can point to a recent report put out by the National Institute of Standards and Technology (NIST) on the reliability of age estimation technologies. Furthermore, FPF could also provide examples of similar laws and outcomes in the US where demand for virtual private network (VPN) services in Texas skyrocketed after a state law took effect requiring age verification to access pornographic websites in an attempt to circumvent the age verification.

As there is currently no federal or provincial law that directly addresses this topic of age assurance, and key terms such as "minor" and "sensitive data" need to be defined, the recommendations made herein by FPF are general age assurance guidelines and best practices.

2. **The Guidance Document should distinguish among and describe the age assurance methods available and highlight for each use case the risks involved, rejecting a one-size-fits-all approach in favor of an age assurance method proportionate to the risks of each use case.**

As each use case is different, there is no one-size-fits-all method for age assurance: the context of each specific use case must be carefully considered to determine a proportionate method of age assurance. An appropriate age assurance method provides a level of age assurance (accuracy) proportional to the risks involved in each use case. Risks of age assurance, as outlined in FPF's Age Assurance Infographic, include both access risks, such as limiting legitimate access to content, creating unequal access and issues of equity, limiting teen autonomy, and ability to bypass the age assurance method, as well as privacy risks, such as collection of user's sensitive data, loss of user anonymity, and unexpected or even unauthorized uses of the data collected for age assurance. The OPC's analysis of privacy risks appropriately includes concrete examples of risks associated with age assurance technology, such as expanding avenues for phishing schemes and worsening the trust deficit between Canadians and "Big Tech."

Age assurance methods employed in specific use cases should be proportionate to the identified privacy risks of the service. As age verification collects sensitive user information, it carries the highest privacy risk and is thus most suitable for highly age restrictive services where potential for underage user harm is highest. Declaration involves a low privacy risk, but also provides a lower level of assurance, so it is most appropriate for situations involving low-risk of user harm. Estimation falls between age verification and declaration for privacy risks and accuracy level, and may be appropriate for moderate-risk situations. A layered approach to age assurance systems may be beneficial, such as an age gate declaration prompting a user to enter their birthdate to enter the site generally, with a higher assurance method such as age estimation or verification later on in the user experience to provide access to more sensitive content.

3. **The Guidance Document should recognize data minimization as a key mitigation measure to deal with privacy risks of age assurance systems.**

Though there are privacy risks inherent with collecting data to evaluate a user's age, there are tools that help mitigate those risks. One important method in this toolbox is data minimization: limiting the collection, storage, retention, and processing of data to what is strictly necessary. Immediate deletion of the ID information collected to determine a user's age is another best practice that minimizes data. When it comes to processing data, practices such as on-device processing and separation of processing through a third party can also help mitigate privacy risks. Employing data practices that promote user protection and privacy is a best practice regardless of whether or not age assurance systems are used, an even more important practice when young people are users of the site or service, and perhaps most helpful and effective when paired with age assurance systems.

4. **The Guidance Document should analyze each specific use case for potential inequitable impacts, especially access equity.**

Some methods of age assurance that aim to restrict access to content will have inequitable impacts, especially access inequity. FPF agrees with the OPC's preliminary positions that highlight potential access equity issues associated with certain age verification methods for some user groups, such as unbanked individuals or noncitizens. FPF recommends the OPC keep inequitable access in mind as well when thinking about "alternative means of restricting access to content": these could complement effectiveness of age-assurance systems, but should not be depended upon as a replacement, as not everyone will have access to household-level internet filtering technologies, parental controls, or data privacy education. Thinking about access and other issues of equity when designing age assurance methods and even potentially offering users more than one option for age assurance methods can help minimize inequitable outcomes.

Potential for inequitable impacts should be considered alongside risks when analyzing which age verification method is proportional for each use case. For example, loss of teen autonomy is a potential access risk associated with age assurance. Teen users with means are more likely to be able to circumvent age assurance methods, while teen users from marginalized communities may not have the same means. For a law restricting underage access to online content such as sexually explicit adult content or pornography, the harm of some users being left out may be low, but for a law restricting underage access to social media, where youth from marginalized populations often find a sense of community and belonging, the harm of some users being left out is higher.

FPF appreciates the opportunity to comment on these issues, and we welcome any further opportunity to provide resources or information to assist in this vital effort.

Sincerely,

David Sallay, Director for Youth and Education Privacy, dsallay@fpf.org
Gabriela Zanfir-Fortuna, Vice President for Global Privacy, gzanfir-fortuna@fpf.org
Jim Siegl, Senior Technologist for Youth and Education Privacy, jsiegl@fpf.org
Lee Matheson, Deputy Director for Global Privacy, lmatheson@fpf.org
Alexa Mooney, Youth and Education Policy Counsel, amooney@fpf.org

The Future of Privacy Forum
https://fpf.org/