Feedback on the Office of the Privacy Commissioner of Canada's Draft guidance on privacy and age assurance

A follow-up submission building on our September 2024 feedback to the OPC's exploratory consultation

Submitted by:
Sara M. Grimes, PhD,
Wolfe Chair in Scientific and Technological Literacy, Professor in Communication Studies, and
Director of the Kids Play Tech Lab, McGill University (Montreal, QC)
Correspondence: sara.grimes@mcgill.ca
August 2026

I welcome the opportunity to comment on the two draft guidance documents released by the Office of the Privacy Commissioner of Canada (OPC) on May 4, 2026, *Assessing whether and how to use age assurance* (the "Operator Guidance") and *Designing age assurance to be privacy-protective* (the "Developer Guidance")[1]. I write in my capacity as a full professor in Communication Studies, Wolfe Chair in Scientific and Technological Literacy, and director of the Kids Play Tech Lab at McGill University, with expertise on the impacts of digital platforms on children's privacy and other rights, and as a co-author of a September 2024 submission to the OPC's earlier exploratory consultation on privacy and age assurance.[2] This feedback is offered as a focused follow-up rather than a fresh submission. Rather than restate our earlier analysis, I take this opportunity to assess what the draft guidance has taken up, what remains open, and what has changed in the intervening period that bears on the questions now before the Office.

I note at the outset that the OPC has moved considerably toward some of the core positions we and other experts in the areas of children's rights and digital citizenship advanced in responses submitted to the original 2024 call for submissions on these key issues. Indeed, I am pleased to see that several of our own recommendations are reflected, in whole or in substance, across the two documents. My purpose here is to support those specific areas of congruence, to identify the small number of places where the guidance is either internally inconsistent or silent on a material risk age assurance tools and methods present to children's privacy and wellbeing, and to bring forward evidence that has emerged since our last submission, including findings from a children's consultation conducted in collaboration with the OPC itself by myself and Professor Valerie Steeves in 2025.[3]

[1] Office of the Privacy Commissioner of Canada, Assessing whether and how to use age assurance – Guidance for websites and online services (draft for consultation, May 4, 2026), https://www.priv.gc.ca/en/privacy-topics/age-assurance/aa-gd-web/; and Designing age assurance to be privacy-protective – Guidance for age assurance developers (draft for consultation, May 4, 2026), https://www.priv.gc.ca/en/privacy-topics/age-assurance/aa-gd-developers/.
[2] Riley McNair and Sara M. Grimes, submission to the Office of the Privacy Commissioner of Canada's exploratory consultation on privacy and age assurance (September 2024). https://utoronto.scholaris.ca/items/2dbe3ff2-df25-4f0c-bfc7-9b7ce3b49b51
[3] Youth Summit on the Best Interests of the Child in the Digital Environment, a collaboration between the eQuality Project at the University of Ottawa (Valerie Steeves), the Kids Play Tech Lab at McGill University (Sara M. Grimes), and the OPC, held in November 2025; see the published preliminary report at note 5.

1. What the draft guidance has taken up

I wish to begin by acknowledging the areas in which the draft guidance reflects the substance of our 2024 recommendations and commend the OPC for incorporating these child-centric, evidence-based positions in the draft guidance.

- **Privacy protection by default, before age assurance.** The Guidance states that age assurance should not be the default condition for accessing the Internet and should be one of several risk-based approaches. It directs organizations to ask whether a potential harm is specific to children or would affect all users, and, if the latter, whether the protection could simply be applied to everyone. It also endorses an "off-by-default" approach in which individuals establish that they are above an age threshold to unlock potentially harmful features, rather than proving they are below one to receive protections. This reflects our 2024 Recommendation 4.
- **A need-first structure.** The Operator Guidance requires an organization to establish that age assurance is warranted — by legal requirement or by a demonstrated, child-specific potential harm affecting a non-trivial number of child users — before turning to questions of method. This sequencing reflects our 2024 Recommendation 5.
- **Content of the harm threshold, and exclusion as a harm.** The Operator Guidance gives substantive examples of practices that do and do not cross the harm threshold, and it requires an organization that would exclude children because of its own data practices to document why those practices are inherent to the service. This requirement recognizes that exclusion can itself harm a child by cutting off access to community and informational resources. This partially aligns with our 2024 Recommendation 6.
- **Constraints on profiling and secondary use.** The Developer Guidance prohibits secondary use and disclosure of information collected for age assurance, bars retention of information about a user's age-assured activities, and strongly encourages "double anonymity." This addresses a substantial part of our 2024 Recommendation 3.

These are meaningful advances and I commend the OPC for prioritizing children's rights and best interests on these points. The remainder of this submission concerns areas the draft guidance leaves unresolved.

2. Harmonizing the guidance with the OPC's own biometrics guidance

Our 2024 Recommendation 2 asked for special provisions governing biometric data in age assurance, on the ground that biometric data are unique, largely unalterable, and comprehensive, such that a breach is categorically different in kind from other data losses because, e.g., a child cannot reissue their face.

In 2025, the OPC adopted a similar position in its *Guidance for processing biometrics – for businesses* (August 2025)[4], establishing that biometric information capable of uniquely identifying an individual is sensitive information "regardless of the context in which it is collected, used, or disclosed," because it is "stable over time, difficult to change, and innately linked with an individual's identity." That guidance treats facial age estimation as a form of "biometric classification" and cautions that classification systems "may still consist of uniquely identifying information" even when identification is not their purpose. It states, critically, that

[4] Office of the Privacy Commissioner of Canada, Guidance for processing biometrics – for businesses (August 11, 2025), https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/biometrics/gd_bio_org-final/.

biometric information can be sensitive "even if it is only used or retained for a brief period of time" — giving the example of a facial-analysis system that assigns a numerical representation to a face, which involves collecting sensitive biometric information "even if the system deletes the information within milliseconds."

However, the May 2026 draft guidance does not clearly connect to this regime. The Operator Guidance presents facial age estimation as an appropriate high-assurance option wherever there is a legal requirement or a significant potential harm, provided it is implemented "in a privacy-protective manner." Neither draft cross-references the August 2025 biometrics guidance or its heightened obligations such as the "appropriate purpose" test that must be satisfied before consent, the general rule of express consent for sensitive biometric information, and mandatory breach reporting on the basis that a breach of sensitive biometric information carries a high likelihood of a real risk of significant harm. The sole bridge between the two bodies of work is a discussion of the 2020 Cadillac Fairview joint investigation[5] in the Developer Guidance, which is itself a biometrics-guidance precedent. This hints at the connection, but only implicitly.

This disconnect creates a potential inconsistency: on-device processing and deletion-on-generation, as described in the Developer Guidance, could be read to imply that facial age estimation is low-risk because the underlying data are held only briefly, even though the OPC's own biometrics guidance forecloses this interpretation with its "within milliseconds" example. I therefore recommend the following clarification:

R1. The age assurance guidance should cross-reference the August 2025 biometrics guidance and state expressly that biometric age estimation presumptively engages its heightened-sensitivity obligations, including the appropriate purpose assessment, express consent, and mandatory breach reporting. Any implication that brief retention or on-device processing lowers the sensitivity of biometric age estimation should be corrected in line with the OPC's previously stated position.

3. Close the behavioural-inference carve-out and address secondary use for AI

Our 2024 Recommendation 3 asked the OPC to look beyond identification to other privacy harms that arise when data collected for age assurance are used to model populations or to train and optimize AI systems. Many such harms do not depend on any individual being identified but nonetheless can pose significant threats to citizens' autonomy and self-determination. The Developer Guidance addresses the profiling dimension well, but it does not address the AI-training and secondary-modelling dimension at all.

First, the Developer Guidance requirement that information generated during the age assurance process be deleted once an age signal is generated "does not apply to situations in which age assurance relies on analysis of information already collected by the organization," in which case "the organization's usual retention schedule would apply." Age inference drawn from data a platform already holds, which is often part of behavioural age estimation, is thereby exempted from the deletion rule that governs freshly collected data. This is the mechanism most likely to be used by the large platforms children actually use, and it is the mechanism through which age-assurance data can be folded into existing profiling and model-training pipelines. As we noted in 2024, in the big data economy, data need not specifically identify anyone to be valuable, and value is frequently found only later, once a use is identified in the context of larger datasets.

[5] OPC, PIPEDA Report of Findings #2020-004 (joint investigation of Cadillac Fairview Corporation Ltd, 2020), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

Second, the Developer Guidance's prohibition on secondary use admits an exception for "certain limited processing if the individual is clearly informed and provides express consent." Consent as a gate on the secondary use of children's age-assurance data, which often includes biometric data, reproduces the very model that a best-interests, privacy-by-default approach is meant to displace—and is especially inadequate when the data subject is a child. I therefore recommend:

R2. The deletion obligation should not turn on whether data were freshly collected or already held. Where an organization performs age inference on data it already holds, the guidance should require that the age determination not be retained, associated with the user's profile, or used to train or optimize any model. Organizations should treat such "inferences" as a distinct processing purpose subject to minimization, not fold it into their previous "usual retention schedules." The guidance should also clarify that personal information collected or generated for age assurance must not be used to develop or optimize AI systems and confirm that this would qualify as a secondary use.

4. Supply an evidentiary standard and resolve a contradiction now before Parliament

Our 2024 Recommendation 5 asked the OPC to require high-quality evidence of the need for age-based restrictions before issuing guidance on how to implement them. The draft guidance adopts the need-first structure but attaches no evidentiary standard to it. The threshold, "potential harm," is left undefined, to be assessed by the organization itself, and the Operator Guidance's introduction refers to a "growing body of evidence" of harm without citation. The standard of evidence an organization must meet to establish a child-specific harm should be clearly articulated, along with specific requirements that the basis of its definition and assessment be documented and available to the OPC.

The OPC already has directly relevant evidence to draw on here. The 2025 Global Privacy Enforcement Network (GPEN) Sweep coordinated by the OPC with the UK ICO and the Bailiwick of Guernsey ODPA, and published in March 2026, examined 876 websites and apps across 27 authorities, and found that while roughly 45% of reviewed services now employ some form of age gating, reviewers were able to easily circumvent those controls on 72% of the services that used them—most often where the service relied on self-declaration of age.[6] Evidence on the early impact of the Australian social media age ban, in force since December 2025, also suggests gaps and limits in tool efficacy. The eSafety Commissioner's first compliance report (March 2026) documented platforms permitting repeated age-assurance attempts until a check was passed, and later (July 2026) reported that a substantial number of children retained accounts, created new ones, or passed age-assurance checks.[7] An independent survey conducted by the Molly Rose Foundation in April 2026 found children under the threshold continuing to use existing accounts, with 70% reporting that it was "easy" to

[6] Global Privacy Enforcement Network, GPEN Sweep Report: Children's Privacy (March 2026), coordinated by the Office of the Privacy Commissioner of Canada, the UK Information Commissioner's Office, and the Office of the Data Protection Authority of the Bailiwick of Guernsey. https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-networks/international-privacy-sweep/2026_sweep/opc-sweep-report-2026/

[7] eSafety Commissioner (Australia), Social Media Minimum Age: Compliance Update (March 2026). https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions; eSafety Commissioner (Australia), Early Days, Early Insights: Understanding Experiences of Social Media Age Restrictions at the Three-month Follow-up (July 2026). https://www.esafety.gov.au/sites/default/files/2026-07/Early-days-early-insights-SMMA-evaluation-three-months-July-2026.pdf?v=1785695847633

circumvent the ban.[8] Read together, this mounting evidence indicates that some of the most commonly deployed age assurance tools are at least partially ineffective at their stated task while frequently entailing additional and (in the case of behavioural and age inference systems) ongoing data collection. This was also the proportionality concern at the centre of our 2024 submission.

A contradiction the guidance should address directly

The current legislative context reveals a structural feature of the draft Operator Guidance that warrants reconsideration. Under section 2.1, an organization may justify preventing access either by demonstrating a child-specific harm or by pointing to a legal requirement. Where a statute mandates the restriction, the organization need only identify the specific requirement and show that age assurance is required by the legislation, or that alternatives were considered and found unsuitable. In that branch, no independent evidence of harm is required and the statutory mandate substitutes for the evidentiary analysis that is the strongest feature of this guidance.

Two bills currently before Parliament bear on this. As introduced in June 2026, Bill C-34 (the Safe Social Media Act)[9] would establish age-based restrictions on holding accounts with regulated social media services; Bill C-36 (the Protecting Privacy and Consumer Data Act)[10], as introduced, treats children's personal information as inherently "sensitive" and deserving of heightened protections. Should C-34 be enacted with an age-restriction mandate in its present form, it would supply exactly the kind of "legal requirement" that, under section 2.1, allows an organization to bypass the OPC's need-first, evidence-based analysis for precisely the services where such an analysis matters most. The same enforcement mechanism would compel the collection of the sensitive children's data that C-36 identifies as most deserving of protection, and that this guidance elsewhere seeks to minimize. I do not take a position here on which instrument would, as a matter of law, prevail. My point is that the guidance and these two bills, as drafted, pull in opposite directions, and that this tension should be acknowledged, if not addressed.

R3. The guidance should articulate the standard of evidence required to establish a child-specific potential harm, drawing where relevant on the OPC's own GPEN Sweep findings, and require that the basis be documented. It should also clarify that the "legal requirement" branch of section 2.1 governs only whether age assurance is warranted, not how it is carried out. An organization relying on such a statute, including the age-based access statutes now before Parliament, remains subject to the guidance's minimization, proportionality, and privacy-by-default expectations, which a statutory mandate should not become a route around.

5. Honour the child-participation evidence the OPC now holds

Our 2024 Recommendation 1 asked the OPC to consult children of diverse ages directly, so that any guidance would reflect their needs and experiences. In the interval, the OPC convened a Youth Council and published

[8] Molly Rose Foundation, Australia's social media ban – is it working? (April 2026). https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf

[9] Bill C-34, An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts (Safe Social Media Act), 1st Sess., 45th Parliament (first reading 10 June 2026; at second reading), https://www.parl.ca/legisinfo/en/bill/45-1/c-34.

[10] Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, 1st Sess, 45th Parl (first reading 15 June 2026), https://www.parl.ca/legisinfo/en/bill/45-1/c-36.

reports from OPC-led youth focus groups alongside the May 2026 guidance. It also collaborated with my colleague Professor Valerie Steeves (University of Ottawa) and myself (McGill University) on a children's consultation: the Youth Summit on the Best Interests of the Child in the Digital Environment, held in Ottawa in November 2025 with preliminary results published in February 2026.[11]

It is therefore notable that the two guidance documents do not draw on this material. Neither cites the youth focus groups or the consultation findings, and neither operationalizes the child's right to be heard. The UN Convention on the Rights of the Child (UNCRC),[12] the General Comment No. 25 on children's rights in the digital environment (GC25),[13] Child Rights Impact Assessment (CRIA), and the Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight (Putting best interests of young people at the forefront of privacy and access to personal information, October 2023)[14] appear once, in section 2.2.1 of the Operator Guidance, as "useful tools and resources" for identifying harms, serving as a reading list rather than a recommended standard. Best interests is named but is not made the measure against which choices are assessed, and the guidance operates throughout on binary age thresholds ("above a given age") rather than the evolving-capacities approach that GC25, the 2025 Youth Summit, and our 2024 submission all call for. Children appear consistently as objects of protection and not as rights-holders or participants. Moreover, the appeals mechanism proposed for wrongly excluded users is not described in terms a child could realistically use.

This is a significant and specific gap that the OPC, with its established track record of prioritizing children's rights and best interests, its work developing a Children's Privacy Code, and its existing evidence base, is uniquely positioned to close. Notably, the eight key interests and four recommendations that emerged from the November 2025 Youth Summit speak to how acutely children understand age appropriateness, restriction, and privacy, showing that they should inform the guidance rather than sit alongside it.

R4. The guidance should draw directly on the OPC's own child and youth consultations and focus-group findings, make the best-interests principle the operative standard against which age-assurance decisions are assessed rather than one resource among several, reference children's evolving capacities rather than binary thresholds alone, and ensure that appeal and redress mechanisms are usable by children. This should carry through into the forthcoming Children's Privacy Code.

6. Clarify who defines "restricted" and "non-restricted" content

Our 2024 Recommendation 6 asked the OPC to clarify how "restricted" and "non-restricted content" would be defined, and by whom. The Operator Guidance answers the "how" in part, through its examples of qualifying and non-qualifying practices, and through its welcome recognition that exclusion can itself be a harm. It does

[11] Youth Summit on the Best Interests of the Child in the Digital Environment: Preliminary Report (Office of the Privacy Commissioner of Canada, February 2026). https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2026/youthsummit_2026/

[12] Convention on the Rights of the Child, 20 November 1989, 1577 UNTS 3 (ratified by Canada 13 December 1991), https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[13] UN Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc CRC/C/GC/25 (2 March 2021), https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

[14] Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight, Putting best interests of young people at the forefront of privacy and access to personal information (October 2023), https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_01/.

not answer the "by whom." The determination remains with the platform, by self-assessment, with the illustrative lists expressly non-exhaustive and no external review, registry, or audit contemplated. As we documented in 2024, there is a long history of services setting age restrictions that bear little relationship to the actual content of the service, in order to avoid the cost of compliance rather than to reflect any assessment of children's developmental readiness. A self-assessment model does little to disrupt that established trend.

R5. The guidance should specify the basis on which content is to be designated restricted or non-restricted and require that each restriction be documented and justified by reference to an identified harm rather than to compliance avoidance or convenience. The guidance should also identify and recommend a mechanism (e.g., audit, registry, or independent review) by and through which those designations can be tested. This should also be reflected in the Children's Privacy Code.

7. Summary of recommendations

In addition to supporting many elements already present in the draft guidance documents, I encourage the OPC to consider the following revisions and clarifications:

R1. Harmonize the age assurance guidance with the OPC's August 2025 biometrics guidance, making its heightened-sensitivity obligations (appropriate purpose assessment, express consent, and breach reporting) presumptively applicable to biometric age estimation.

R2. Close the behavioural-inference carve-out so that age inference on already-held data is subject to the same deletion and non-association requirements as freshly collected data, and clearly state that age-assurance data must not be used to train or optimize AI systems as this constitutes a secondary use.

R3. Articulate the standard of evidence required to establish a child-specific harm, and address how the §2.1 "legal requirement" branch is intended to interact with age-based access statutes now before Parliament, so that a statutory mandate does not become a route around the guidance's own safeguards.

R4. Draw the guidance directly from the OPC's own child and youth consultation evidence, make best interests the operative standard, recognize evolving capacities, and ensure redress mechanisms are usable by children.

R5. Specify the basis on which content and services are designated restricted or non-restricted, require documentation tied to an identified harm, and identify a mechanism by which those designations can be independently tested.

I am available and willing to provide further detail on any of the above, including the underlying research findings, and thank the Office for its continued engagement on these vital questions.