

Consumer Choice Center Comments on Designing age assurance to be privacy-protective – Guidance for age assurance developers

August 4, 2026

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

The **Consumer Choice Center** is an independent, non-partisan consumer advocacy group championing the benefits of freedom of choice, innovation, and abundance in everyday life. We champion smart policies that are fit for growth, promote lifestyle choice, and defend technological innovation.

Herein, we will offer our comments on the [Designing age assurance to be privacy-protective – Guidance for age assurance developers](#) (henceforth “the Guidelines”), albeit from a consumer-focused perspective of Canadian consumers.

General Views on the Consultation

The aim of the Office of the Privacy Commissioner of Canada (henceforth “the Commissioner”) of consulting on the privacy concerns of developers building age-assurance technology is laudable. The Consumer Choice Center also works to make sure the privacy of Canadians is forefront when considering online regulations and legislation. While our goals align, where we would like to provide recommendations for this consultation is to encourage the Privacy Commissioner to further consider the great harms that could be caused to children and to all Canadians if age-assurance technology becomes subject to federal mandates or requirements. We base this on the widespread amount of expert evidence that age assurance does not work as a policy in helping children avoid online harms through social media, and cannot be effectively executed by developers in a way that completely protects consumers from data breaches, even with the use of these government Guidelines.

Our Response to the Commissioner's Concern Over Canadian Internet User Privacy Protection

The Commissioner has officially stated that “[\(age assurance\) systems must be designed to be privacy protective to avoid creating an undue impact on the privacy rights of Internet users](#)”. In order to ensure that, the Guidelines lay out several ways that the Commissioner expects them to develop this technology to avoid privacy protection concerns. While this is a laudable concern to highlight to developers, the Consumer Choice Center would like to remind the Commissioner that there is simply no way to completely ensure privacy protection, and any developer claiming to be able to make that happen is misleading the Commissioner's office. Using the word “*must*” shows that the Commissioner is requiring that age assurance systems be secure, but that simply cannot be done, even with the ideas the Commissioner has outlined in these Guidelines.

The Electronic Frontier Foundation has [stated clearly](#) that there is simply no technology currently developed that can verify a user's age in a way that protects their privacy. Even though Bill S-210 claims that online age verification technology is increasingly sophisticated, none of them can offer age verification as of yet that protects user privacy.

This fact [has been backed up](#) by highly respected University of Ottawa professor Michael Geist, who is also the Canada Research Chair in Internet and E-commerce Law at the University of Ottawa. He is an expert in this area, and he has been clear to point out in his writing as well as in his appearances before Parliament that there cannot simply be a “nerd harder” solution to the problem of age verification and privacy. In other words, the government cannot simply expect developers to just “try harder” and get smarter in order to solve a problem that likely does not have a solution. Indeed, these Guidelines do have the Commissioner telling developers they “must” find a way to make age verification safe and unbreachable, and yet experts are warning again and again that this is not physically possible. It is not a matter of will, it is a matter of ability. It should be private businesses, who are already

subject to privacy laws in case of leaks, that make this happen, rather than through a government mandate that could open users up to serious privacy breaches by mandating how age assurance is done and by whom.

A [submission](#) by the Internet Society to the Standing Committee on Public Safety and National Security on Bill S-210 showed that that age verification data would be ripe for exploitation by criminals for scams and theft, and to foreign adversaries. To quote the submission directly. “If Internet traffic were left unencrypted to allow access to content by Internet intermediaries, this unencrypted data would be susceptible to a wide range of threats.” This is very concerning to Canadian consumers.

In the Guidelines, the Commissioner asks that age assurance providers “[do not retain any information about the individual's online activities and, where possible, design systems to ensure that such information cannot be collected.](#)” There are several issues with this sentence. First, as [OpenMedia has said](#), there is not much that can be done about what happens to Canadians’ data once it is collected by the verification vendor that the site has employed to check someone’s age. It is unclear who keeps the information and for how long and even how it is kept. It could even be sold, as there’s no way to make sure that does not happen. Second, the fact that the Commissioner has included the words “where possible” makes this even more likely to become a problem, since those two words could be interpreted as a loophole for verification vendors if they ever have scrutiny applied to their activities.

Given these facts put forward by experts, going forward with age verification mandates for social media led by these Guidelines would be an irresponsible action on the part of the Office of the Privacy Commissioner. Knowingly entering Canadian consumers into a scenario where their privacy will most likely be breached since there is nothing that can stop hackers from collecting age verification data might result in a loss of confidence of Canadians in their Privacy Commissioner’s office. This would not be a favourable outcome for consumers since the Commissioner is a highly respected institution in Canada that protects Canadians from their elected officials and staff when they breach the public’s confidence.

Our Response to the Guidelines requiring that information included in age assurance be limited

An important concern by the Commissioner that is relayed through the Guidelines is that developers *must* limit the information included in age assurance results. Here is the [specific text](#) from the Guidelines:

***“2. Limit the information included in an age assurance result.
Age assurance providers must:***

- *Include no more information than is necessary in an age assurance result.*
- *Justify the inclusion of any information in an age assurance result other than the individual’s age range or a ‘yes/no’ signal indicating whether the individual is above a given age.”*

We recognize that the Commissioner is trying to make sure that only the most basic information is captured by age verification. However, it is important to note that even minimal information is linked to IP addresses, which are linked to specific individual internet users. It is clear that the Commissioner is aware of this issue since the very [next section reads](#):

“3. Avoid secondary use or disclosure of personal information collected for age assurance.

Age assurance providers must:

- *Not use personal information collected for age assurance for any other purpose.*
- *Not disclose personal information collected for age assurance.*

Age assurance providers should:

- *Demonstrate that these practices are followed, such as through an independent audit or conformity assessment.”*

Clearly, the Commissioner is worried about the collection of this data even if it is simply an age range and/or a yes or no answer (pass/fail logic). As we stated based on the evidence from various tech experts in the last section, there is no way to actually protect privacy even with minimal questions. It is simply

not possible, even if the Commission is saying the words “must” and “should.” It is further concerning to Canadian consumers that an independent audit or assessment is placed under the “should” category rather than the “must” category since an independent assessment should be absolutely necessary especially since the government is mandating this for developers.

In terms of the Commissioner’s concern of trying to protect children on the internet, unfortunately it is important to realise that even an age range and/or a yes or no question is subject to linkage with an internet user. That linkage could end up harming children more than the intention of the age verification guidelines themselves.

An article by the American nonpartisan think tank R Street shows that age assurance data collection [leads to child identity theft](#). This has also been raised as an issue through a [submission](#) to the Canadian parliament by the organization Bridge2Future, which works to stop commercial sexual exploitation of women and children. They stated:

“Any effective form of Age Verification requires a government issued ID or credit card. This conclusion flows from the understanding that you need to be an adult to apply for your own credit card. In Canada, a person 14 years of age can be included in the authorized users with a family card option.”

No matter the actual way it is collected, the fact remains that the possibility of this data being used for fraud is there, and that is something that could ruin a child’s future forever. Requiring the hand-over of IDs that contribute to already-troubling acts of fraud against children is something that must be taken into consideration by the government when they are the ones mandating this assurance, how it is done, and by whom.

Our Response to the Guideline’s primary principle of helping children avoid harm on the Internet

We find the Commissioner's concern regarding shielding children from harm on the Internet combined with concerns about the private information of Canadians to be a good measure. However, it is important for the Commissioner to take into consideration that government-led age verification simply does not work as practiced thus far, and has not worked where it has been tried.

In the United Kingdom, a country whose government has been one of the pioneers of age assurance, has essentially failed to achieve their goal. OpenMedia [shows](#) that the UK's system is proving ineffective because it is quite easy for kids to simply use a VPN to circumvent age verification.

In [Australia](#), more than one million Australian teens have reported they are still using the social media they are supposed to be banned from since the ban became effective in December. They are simply using fake birthdays, borrowed accounts, or a VPN to access the internet from a different location. This is further concerning because if children are able to bypass these bans, and know that these are something that can get themselves or their parents in trouble with the law, it is less likely that they will actually go to their parents or a trusted adult if something bad does happen to them on the Internet. They won't want to get in trouble for doing something the government has told them they aren't allowed to do, thereby isolating these children in their time of need.

Our Response to the Commissioner's instruction that the age assurance process should not disadvantage any group

The Consumer Choice Center agrees with the Commissioner that there should be an emphasis on age assurance not be disadvantageous to any equity-deserving group. The guidelines state the following:

"6. The age assurance process should not disadvantage any group. Age assurance providers must:

- *Proactively take measures to identify limitations to the accuracy of their age assurance methods based on group characteristics.*
- *Disclose to relying parties any known limitations in effectiveness, if they cannot be addressed.*

Age assurance providers **should**:

- *Ensure that equally privacy-protective alternative age assurance processes are available should it be likely or known that individuals of an equity-deserving group will be less able to successfully pass an age assurance check.”*

As we stated in the paragraphs above, one major group that will be disadvantaged by government-led age assurance measures will be children themselves. They are a vulnerable group that would be negatively affected despite the Guidelines attempt to prevent that. They will be subject to fraud by submitting their information, they will be less likely to confide in a trusted adult if something bad is happening to them on the internet, and they will be subject to all of this for a program that has proven to be ineffective, easily manipulated, and impossible to do perfectly by developers. Children will also be blocked by age assurance from accessing communities that they might rely on for support from other children their age, or that celebrate their unique talents and hobbies like sports, art, and anything else they want to talk to others about.

Another vulnerable group that has already seen discrimination from age assurance is the 2SLGBTQI+ community. [OpenMedia](#) has pointed out that one disadvantage of age assurance in the UK is that, because of automated filters that wanted to comply with age verification rules, the filters often ended up blocking 2SLGBTQI+ forums and sexual health education resources, two things that vulnerable young people certainly should be able to access. This issue goes beyond the Commissioner’s concern that vulnerable groups could not pass an age-verification check, it’s a fundamental issue that could harm young people’s mental health and ability to access vital communities. Those vulnerable young people also may not want anyone to know they are accessing certain sites for fear of repercussions from their families or communities, which means they may be less likely to access through social

media the communities that are extremely important to them in a world that might be isolating otherwise.

The end of anonymity is bad news for all Canadians but particularly for those belonging to a vulnerable group. Some groups do not have government-issued IDs for various reasons, others simply want their right to anonymity protected. A Dalhousie University policy panel [argues](#) that age verification limits constitutionally protected anonymity. They also worry about a chilling effect that could take place due to this end of anonymity. This could have even more negative repercussions to those within vulnerable groups. The Dalhousie panel itself went on to point out that “marginalized youth are likely to be particularly hard hit by the loss of avenues for community-building, engagement and education that are not available offline.”

This is a serious concern for us at the Consumer Choice Center, and also presents yet another expert opinion on why these Guidelines will not be enough to fill the serious implementation holes of government-mandated social media age assurance, and will not quell the Canadian consumer’s fear surrounding privacy protection.

Conclusion

Overall, the Consumer Choice Center supports the Office of the Privacy Commissioner’s intention in presenting these Guidelines. We also believe that children should be protected on the Internet. However, we have written this recommendation to strongly urge the Commissioner to rethink government-mandated age assurance mandates as a positive policy to protect children online on social media. We have shown in this Response that the issues the Guidelines put forward cannot be adhered to, no matter how well intentioned the Commissioner or the developers may be. We strongly urge the Commissioner to argue for the scrapping of government-imposed social media age assurance mandates since they cannot meet the standards of the Guidelines, and to encourage the private sector to develop the best technologies for this purpose. It is our final recommendation that the Government move forward instead with a plan to encourage, and even invest

in, programming that encourages parents and trusted adults to take charge of children's activities online, and the use of technological innovation that can help adults make sure children are accessing the internet in a positive way.

Respectfully,

Sabine Benoit
Canadian Policy Associate
Consumer Choice Center