

**Submission to the Office of the Privacy Commissioner of Canada
Exploratory Consultation on Privacy and Age Assurance**

September 10, 2024

The Evangelical Fellowship of Canada (EFC) appreciates the opportunity to participate in this exploratory consultation. We believe initiatives to protect children and youth online are crucial.

The EFC is the national association of evangelical Christians in Canada. Established in 1964, the EFC provides a national forum for Canada's four million Evangelicals and a constructive voice for biblical principles in life and society.

Our approach to this issue is based on the biblical principles of respect for human life and dignity, justice and care for those who are vulnerable. We note that these principles are also reflected in Canadian law and public policy.

We provide our comments on the Office of the Privacy Commissioner's questions, below.

1. *What additional context should we be aware of in developing our future work? Are there other key resources (guidance documents; principles; standards; research; etc.) we should review?*

International jurisdictions

There are many international initiatives on age assurance, as countries around the world are recognizing the need to protect children online and are developing different mechanisms to do so. Countries within the European Union have been particularly active,¹ and several U.S. states have passed legislation and regulations,² as well. The euConsent project has demonstrated that online age checks can be simple and convenient while guaranteeing the privacy of users.³

International bodies are recognizing the negative impact of harmful content online on children and youth, and recommending countries take action to protect them. In November 2023, the

¹ <https://www.osborneclarke.com/insights/age-assurance-focus-european-regulatory-action-online-protection-minors>

² <https://www.pbs.org/newshour/politics/utah-law-requiring-age-verification-for-porn-sites-remains-in-effect-after-judge-dismisses-lawsuit>

³ <https://euconsent.eu/a-summary-of-the-achievements-and-lessons-learned-of-the-euconsent-project-and-what-comes-next/>

UN General Assembly adopted by consensus the *Resolution on the Rights of the Child in the digital environment*.⁴ This resolution states that the General Assembly is “deeply concerned that increased unsupervised use of digital technologies has exacerbated children’s, including adolescents’, exposure to risks, harms and all forms of violence” online, including exposure to violent and sexual content. In this resolution, the General Assembly:

48. Encourages States to make efforts towards mainstreaming children’s needs in all digital policies, and public and private investment, providing all children with equal and effective access to age-appropriate information, and information on their rights, and to high-quality online resources, including on digital skills and literacy, and protecting children from online risks and harm, as well as arbitrary or unlawful interference with their privacy on social media, as well as preventing children’s exposure to violent and sexual content, gambling, exploitation and abuse, and the promotion of or incitement to life-threatening activities;

General comment no. 25 on the UN Convention of the Rights of the Child states:

*114. States parties should ensure that appropriate enforcement mechanisms are in place and support children, parents and caregivers in gaining access to the protections that apply. They should legislate to ensure that children are protected from harmful goods, such as weapons or drugs, or services, such as gambling. Robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements.*⁵

Canada can learn from these international precedents and follow through on international commitments.

Online access by youth

In a survey conducted in 2021, three-quarters (77%) of Canadian youth reported they have their own smartphone.⁶ The percentage is slightly lower among the younger age brackets, with the majority (57%) of 9- to 11-year-olds having their own smartphone, compared to 81% of 12- to 13-year-olds and almost all (93%) 14- to 17-year-olds.

Of young Canadians who have their own smartphones, one in three (34%) received it between the ages of 6 and 10, half received it between 11 to 13 years of age.⁷ Among youth who do not have their own smartphones, 44% have access to someone else’s.

⁴ <https://documents.un.org/doc/undoc/ltd/n23/342/80/pdf/n2334280.pdf>

⁵ <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPrICAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUI9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t>

⁶ <https://mediasmarts.ca/sites/default/files/2022-11/life-online-report-en-final-11-22.pdf>

⁷ <https://mediasmarts.ca/sites/default/files/2022-11/life-online-report-en-final-11-22.pdf>

About one in three Canadian students (32%) in grades 7 to 11 say they have seen pornography online without looking for it. The majority (60%) say it pops up on the websites they visit.⁸

Research commissioned by the British Board of Film Classification found that children and teens are watching and coming across pornography at young ages.⁹ It found that half of 11- to 13-year-olds (51%) and two-thirds of 14- to 15-year-olds (66%) had viewed pornography online. Some children were as young as 7 or 8 years of age at their first exposure. For more than 60% of youth aged 11–13 years, their first viewing of pornography was accidental. Youth are easily able to access free pornography sites that do not have any meaningful age verification in place.

Children and youth easily bypass current basic age declaration measures, for example, by giving a false date of birth. Research commissioned by Ofcom found 60% of children under the age of 13 who use social media accounts have their own profiles, despite not being old enough – and 39% of 8 to 12 year olds have a social media profile user age of 16+.¹⁰

There are currently age assurance technologies being used with respect to online gambling sites in Canada. Perhaps age assurance technologies could be designed to be used in more than one context where users are limited to adults. A federally regulated registry of approved third-party age assurance technologies could be employed to protect minors from accessing online gambling, some types of online gaming, violent or sexually explicit content, and more.

Easily accessible explicit and violent content

According to a recent study, the landing pages of mainstream pornography sites suggest sexually violent content to first-time viewers. The April 2021 *British Journal of Criminology* study found that 1 in 8 of the titles shown to first-time viewers on mainstream pornography sites described sexually violent acts.¹¹ The authors state in their conclusion:

Our study offers new and compelling evidence that the boundary between what is and is not sexual violence is distorted by mainstream online pornography platforms. Using the largest sample of online pornographic content collected to date, we have found that one in eight titles on the front page of mainstream pornography sites describe acts that would fall under the most widely used policy definition of sexual violence. ... The titles we have reported on here are not found by users of their own volition beyond a decision to access pornography. They are not displayed as a result of a user's search terms or site history, nor are they only accessed through niche sites specializing in violent pornography. They are freely available on

⁸ <https://mediasmarts.ca/sites/default/files/2023-01/Encountering%20Harmful%20and%20Discomforting%20Content%20Report%20-%20YCWPhase%20IV.pdf>

⁹ <https://www.bbfc.co.uk/about-us/news/children-see-pornography-as-young-as-seven-new-report-finds>

¹⁰ <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/childrens-online-user-ages/children-user-ages-chart-pack.pdf?v=328540>

¹¹ <https://academic.oup.com/bjc/article/61/5/1243/6208896>

the landing pages of the most popular porn sites in the United Kingdom. ... Similarly, we found that depictions of practices that meet criminal standards of sexual violence, including rape, incest and so-called 'revenge porn', are labelled in ways that not only minimize or remove their criminality but often mock or belittle the possibility of harm.¹²

Disturbingly, the study's authors note that "teen" was the most frequently occurring word in all the titles, including the titles referring to sexual violence. The most common form of sexual violence occurring was sexual activity between family members, such as parent-child or siblings. The second most common form of sexual violence was physical aggression and sexual assault, which included titles with terms like "force," "punch," "molest" and "brutal."¹³

Another study published in 2020, in the *Archives of Sexual Behavior*, found that 45% of randomly selected videos on Pornhub depicted at least one act of physical aggression. The most common types of physical aggression were spanking, gagging, slapping, hair pulling and choking. Women were virtually always (97%) the target of aggression.¹⁴

As well, new AI technology makes it easier for youth to create and to view sexually explicit images online. Between 96% and 98% of deepfake videos available online feature sexual content.¹⁵ There is also an increase in the use of AI to create deepfake nudes, "One boy with his phone in the course of an afternoon can victimize 40 girls, minor girls."¹⁶

These AI technologies are already being used to carry out image-based sexual abuse. The Government of Canada must ensure the appropriate tools are in place to respond to them and ensure justice for those who are victimized. We strongly encourage the OPC to consider the privacy implications of these technologies. We note legislation on digital forgeries of intimate images, known as the DEFIANCE Act, 2024 S.3696/H.7569, is progressing through the U.S. Congress.¹⁷

2. Are there other significant privacy considerations we should be aware of?

It is evident that self-regulation has not worked. There may not even be compliance with existing regulations, or a very lax approach to regulations unless there is strict enforcement, as evident in the OPC report, *Investigation into Aylo (formerly MindGeek)'s Compliance with PIPEDA*.¹⁸ The OPC report indicates that MindGeek did not take reasonable or effective steps to

¹² <https://academic.oup.com/bjc/article/61/5/1243/6208896>

¹³ <https://academic.oup.com/bjc/article/61/5/1243/6208896>

¹⁴ <https://link.springer.com/article/10.1007/s10508-020-01773-0>

¹⁵ <https://www.ohchr.org/sites/default/files/documents/issues/children/sr/cfis/existing-emerging/subm-existing-emerging-sexually-aca-university-toronto-dr-sara-grimes-cewen.pdf>

¹⁶ <https://www.nytimes.com/2024/04/22/technology/deepfake-ai-nudes-high-school-laws.html>

¹⁷ <https://www.congress.gov/bill/118th-congress/senate-bill/3696/text>

¹⁸ <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2024/pipeda-2024-001/>

ensure consent for content uploaded to the Pornhub website, even when its own internal reports suggested that content was being uploaded without requisite consent.

There must be regulation/legislation that requires companies to protect children from harmful content. A business model with a focus on profit will not expend the effort or capital needed to put in place age assurance without a state mandate. The onus must be on companies to act.

The EFC's primary focus in this exploratory consultation is on the protection of children. There is a clear need to protect children and youth from harmful content online and from the technologies that are being developed to draw and keep their attention online. There are increasing reports of the negative mental health impacts of social media on youth,¹⁹ the role of algorithms,²⁰ etc.

3. Do you have any comments on our preliminary views?

The EFC supports the OPC position that it is possible to design and use age assurance in a privacy-protective manner. As noted above, other jurisdictions internationally are implementing age assurance in a privacy-protective manner, and Canada is falling behind in its protection of children and youth from harmful content online.

It will take a multifaceted approach to protect children online. No one approach is completely effective or sufficient. Age assurance is one tool among many, but it is an essential tool. There is also an important role for parental controls, education, device-level controls, and other tools. Each action addresses a different area of the problem.

Age assurance does not need to be 100% protective to be helpful. Older teens or more tech-savvy teens may be able to circumvent age assurance technologies. However, age assurance technologies help to prevent accidental or easy exposure to explicit content by young children and others.

Parents may employ Internet filters at home, but this does not prevent children and youth's exposure to explicit or violent content in other locations where wi-fi is available. Device-level controls may not be set in smartphones that are handed down or purchased used. There is also the potential for exposure to explicit or violent content through a classmate or older sibling's device.

¹⁹ <https://www.hhs.gov/about/news/2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html>

²⁰ <https://www.cambridge.org/core/journals/american-journal-of-law-and-medicine/article/abs/algorithms-addiction-and-adolescent-mental-health-an-interdisciplinary-study-to-inform-statelevel-policy-action-to-protect-youth-from-the-dangers-of-social-media/EC9754B533553BDD56827CD9E34DFC25>

Parental controls do not help to protect children whose parents are disengaged or not well-informed of the risks. In fact, these children may be at higher risk of negative effects from exposure to harmful content than children whose parents are engaged and informed.

Age assurance helps to protect all children and youth, not just the ones with parents who have the time and energy to explore protective options. It helps protect children and youth in all the settings they may encounter harmful content outside the home.

Age assurance can be provided through a third party; it does not need to be carried out by the government or a pornography platform. Stringent privacy protections can require that data be deleted immediately after verification. Legislation that mandates age assurance does not need to specify the technological means, so that new technology can be used as it is developed.

4. What complementary steps might the OPC consider taking to promote privacy and online safety for young people?

The OPC may consider whether the minimum age for social media accounts should be reconsidered and whether it should require age assurance for those accounts, as well. As noted above, research commissioned by Ofcom found 60% of children under the age of 13 who use social media accounts have their own profiles, despite not being old enough – and 39% of 8 to 12 year olds have a social media profile user age of 16+. ²¹This minimum age limit needs to be reviewed regularly, particularly as research indicates its negative impact on youth in terms of mental health. ²²

The OPC may want to look at initiatives such as those in the U.S. *Kids Online Safety Act*, which requires social media companies to provide safeguards and tools for minors and parents and enables the strongest safety setting by default; creates a duty of care for online platforms to prevent and mitigate harms to children; disables private messaging to minors from unknown adults and turns off geotagging features; establishes a transparency standard by providing academic and public interest groups access to platforms' data. The OPC may consider whether Canada can and should pursue similar provisions to protect minors.

²¹ <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/childrens-online-user-ages/children-user-ages-chart-pack.pdf?v=328540>

²² <https://www.hhs.gov/about/news/2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html>

Conclusion

The EFC appreciates the Office of the Privacy Commissioner's initiative in prompting meaningful discussion on age assurance. We urge your office to continue researching this topic in order to encourage the development of privacy-protective age assurance guidelines, techniques and services. Canada must take steps toward meaningful protection for children and youth from harmful online content.

EFC TORONTO OFFICE

10 Huntingdale Blvd
Scarborough, ON, M1W 2S5
Toll Free 1-866-302-3362

EFC OTTAWA OFFICE

#810 - 275 Slater Street
Ottawa, ON, K1P 5HP
T 613-233-9868

www.theEFC.ca

EFC@theEFC.ca

twitter.com/theEFC
facebook.com/theEFC