David Young Law
Compliance Bulletin

May 2026

Protecting children online – age verification concerns and social media bans

Recent events have brought to a head the issue of protecting children and youth against online harms.

Most recently, the families of seven victims of the mass shooting in Tumbler Ridge BC have sued OpenAI, the provider of the ChatGPT AI platform. Their action alleges that the platform was negligent in not taking steps to prevent the 18-year old shooter from learning about gun violence through its online service. In March, Meta and You Tube were found liable in California for substantial damages caused to youth by addiction to social media and, in New Mexico, Meta was found liable for misleading consumers and endangering children respect to the safety of its platforms.[1]

In response to the resulting concerns, governments and regulators have taken or are considering a number of potential protective measures. Receiving much attention are the proposals for a social media ban for children and youth, which has been adopted in a number of international jurisdictions[2] and is proposed in Manitoba.[3]

On a broader plane, the federal government is grappling with introducing online harms legislation focussed on protecting youth, is planning to reintroduce a reformed privacy law to update the now 25-year old private sector privacy law, PIPEDA,[4] and is considering what or whether regulation of artificial intelligence (AI) is needed. Any AI regulation could include requirements for notifying regulators or law enforcement about potential dangers posed by users of systems such as chat bots.

At a different level, initiatives to protect children and youth online through content and design moderation as well as access controls have evolved, importantly through privacy regulator guidance and, in some jurisdictions, legislation.[5]

Why is age verification relevant?

Many of these existing or potential interventions directed at protecting youth from online harms require protocols for an age control. The objective is to ensure that relevant persons (i.e. youth) will not be able to access specified websites, or content, or if they can do so, their communications are moderated to ensure that content and interactions (such as collection of personal information) are youth-protective. The function of verifying the age of the individual is most universally referred to as “age assurance” but more colloquially, “age verification”.

---

[1] Jury in Los Angeles finds Meta and YouTube liable in landmark social media addiction trial, CBC, March 25, 2026; Jury finds Meta liable in case over child sexual exploitation on its platforms, CNN, March 24, 2026.
[2] See for example: Australia, Social media age restrictions, eSafety Commissioner, April 2, 2026.
[3] Manitoba set to become 1st province to ban social media for children, Global News, April 26, 2026.
[4] *Personal Information Protection and Electronic Commerce Act.*
[5] See for example: Age appropriate design code, Information Commissioner's Office (UK).

David Young Law • Hudson’s Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

What are the issues?

However, there are significant concerns with operationalizing an age control rule, either through legislation (such as a mandated youth harms law[6] or a social media ban) or through more nuanced approaches to online protections such as mandating content moderation for youth-oriented sites. The most significant concerns relate to potential privacy risks resulting from the extensive collection of personal data needed to operationalize an age-based control.

However other concerns also exist, specifically human rights, equity and discrimination risks posed by the nature of the information that may be collected to support an age determination, and the potentially unequal access to technologies that may be required to utilize an age determination protocol.[7]

Age assurance protocols – privacy and technology concerns

There are a number of age assurance methodologies, some of which have been in use for many years, typically for controlling access to websites and online shopping venues.[8] However now their potential application has expanded exponentially with the advent of concerns for online harms in particular regarding children and youth.

Declaration protocols provide for the user, or a person who knows them (such as a parent), to state that the user is above a defined age, without any verification procedure to confirm the validity of the declared age. These may involve the user actioning a web page functionality stating, for example, "I am over 18 years old". Alternatively, an account holder who is known to be of the required age may provide an assurance to the platform that the subject user is of the required age. Under none of these methodologies is a procedure for verification provided, so the age determination relies entirely on the confidence that the platform has in the person providing the declaration to being truthful.

Relative to other age protocols (see below), age declaration can be considered the least secure since it may be circumvented easily. However, by contrast with other protocols, it is the most privacy protective since very little personal information is collected by the platform.

Age verification protocols require the individual to provide a verifiable document proving age. This may include provision of an image of a government-issued identity document containing their date of birth and permitting verification of the identity of the individual such as by taking a photo online of the user's face, or alternatively, by providing a digital identity credential issued by a government or other trusted party.

The procedure involves significant privacy concerns. The primary concern is that the protocol involves the collection and presumably retention of age-related information by the platform or a third party service provider, which will include not

[6] See: Bill S-209, An Act to restrict young persons' online access to pornographic material.
[7] See Briefing note: Proposed OPC Position and Actions on Age Assurance, Sept. 24, 2024.
[8] See, for example, Children's Online Privacy Protection Rule ("COPPA"), 16 CFR Part 312.

only date of birth but also sufficient other identity information (such as home address) to validate linking the age with the individual, with attendant risks for privacy protection.[9]

However a further, significant, concern is that such age/identity information will need to be collected for *all potential visitors* to the platform in order to ensure that only age-validated users can access it. Such a collection protocol not only would involve the collection of personal information from potentially all internet users but also the retention of an ever-growing database of users' information, with attendant risks for privacy protection. While it may be possible to narrow the application of such a requirement for specific youth-oriented sites, the impact for its application in the context of a social media ban is potentially great since such a ban could require all users to provided age verification in order to access those platforms.

Age estimation is a protocol by which an individual's age is estimated based on their features or behaviours instead of specific ID documentation, typically by an AI system. Age estimation methods establish that a user is likely to be of a certain age, or falls within an age range, or is over or under a certain age. These can include: biometric analysis by which an image of an individual's face, or a sample of their voice, is captured and analyzed to determine an estimated age or age range, or behavioural analysis such as by which an individual's interactions with a platform or some other form of online activity is analyzed to determine an estimated age or age range.

Age estimation protocols represent the most privacy-invasive methodology for age control. The technology may involve even tracking users' friends, their posts, messages, and any other indicia to obtain an accurate estimation of their age, thus putting users at greater risk.[10] The privacy risks noted above with respect to age verification would apply equally to age estimation.

Understanding these potential risks, there has been controversy among privacy regulators and technology experts worldwide on whether age assurance should be used, even in the face of growing concern with the harms potentially faced by children and youth online.

In a statement arguing against current adoption of the technology, an international alliance of security and privacy scientists has called for a moratorium on deployment until there is consensus on the net benefits that age assurance technologies can bring, and there is the technical feasibility for such a deployment.[11]

They summarize their concerns as follows:

> Age-assurance checks are easy to bypass, … using VPNs, bought or borrowed credentials, or props or AI-based tools to change the users' appearance. Such checks also require the creation of Internet-wide trust infrastructures that do not exist today, whose technical deployment would be quite complex, and whose worldwide legal enforcement seems doubtful. They … not only might be ineffective, but can actually diminish

[9] See, for example: 70,000 government ID photos exposed in Discord user hack; Discord blamed the breach on a third-party vendor, (NBC News, Oct. 9, 2025)
[10] The Illusion of Protection: Why Canada's Growing Push to Ban Social Media for Kids Won't Work, Michael Geist Blog post, April 28, 2026.
[11] Joint statement of security and privacy scientists and researchers on Age Assurance, March 9, 2026.

> safety online by exposing users to malware and scams when they resort to alternative services that do not implement verification …. [and will] massively reduce privacy online by forcing users to reveal more information to service providers ….

OPC's policy on age assurance

Notwithstanding above-noted concerns, the federal Office of the Privacy Commissioner (OPC), aligning with other privacy regulatory stakeholders internationally,[12] has determined that age assurance constitutes a privacy-protective mechanism to support children's and youth privacy rights online and that it should be deployed – or mandated – with caution, on the condition that the potential privacy risks associated with its use are addressed and mitigated.

The OPC has published a *Policy Note* and proposed guidance for website operators and developers relating to the need and usage of age assurance.[13] The proposed guidance reflects the OPC's conclusions from a year-long consultation on age assurance[14] as well as insights gained from a sweep study of such protocols in diverse international jurisdictions.[15]

In its *Policy Note* regarding age assurance, the OPC identifies potential privacy concerns including breach, unauthorized tracking and profiling, and disproportionate or unequal collection of information or application of access restrictions based on differential characteristics of user groups.

To minimize these potential risks, the OPC states that websites and systems developers need to: minimize collection and avoid retention of personal information; limit the information included in an age assurance result; prohibit secondary use or disclosure of personal information collected for age assurance; minimize, and not retain or disclose, information generated during the age assurance process (excepting the final result); prohibit retention or use of information about the individual's online activities and, where possible, design systems to ensure that such information cannot be collected; and ensure that the age assurance process does not disadvantage any societal group.

Conclusions

The landscape of child and youth online protection is at a cross-road. Increasing concerns regarding the potential harm that may be done to young people, or be done by them, are militating toward adoption of mandated age-control rules and methodologies. However, in their current state of development, these methodologies present significant privacy and other societal risks, not only to young people, but potentially to all internet users. At one point, the OPC suggested

---

[12] See: Briefing note: Proposed OPC Position and Actions on Age Assurance, March 27, 2024; Joint Statement on a Common International Approach to Age Assurance, Sept. 19, 2024; Guidance on highly effective age assurance and other Part 5 duties, UK OfCom, January 16, 2025; Age Assurance Technology Trial, Australia, August 2025.

[13] Age Assurance – Policy Note, Assessing whether and how to use age assurance – Guidance for websites and online services, Designing age assurance to be privacy-protective – Guidance for age assurance developers, Office of the Privacy Commissioner of Canada, May 4, 2026.

[14] Consultation on age assurance – What We Heard, Office of the Privacy Commissioner of Canada, March 21, 2025.

[15] See: Global Privacy Enforcement Network (GPEN) Sweep Report: Children's Privacy, Office of the Privacy Commissioner of Canada, Information Commissioner's Office, the United Kingdom, Office of the Data Protection Authority of the Bailiwick of Guernsey, March 2026

that the risks posed by any age-control methodology should be proportionate to the risks that such a control is intended to prevent.[16] In other words, methodologies that present higher risks should only be used for access to platforms that pose a commensurate level of high risk.

The OPC has not pursued this criterion and instead has emphasized that alternatives to age control should be used where possible,[17] recognizing that age controls will be required in certain instances. In addition, the OPC has chronicled the use of potentially non-identifying methodologies for age control.[18] Consistent with the view of the international experts that age assurance technologies should not be adopted under currently known technologies,[19] it seems logical that adoption/mandating implementation of such technologies should be paused pending development of robust privacy-protective frameworks.

Mandated social media bans present all of the issues noted above for age-control methodologies, with the added concerns regarding their likely operational and societal challenges. Commentators have argued that website governance and accountability directly addressing protection of children and youth from online harms is the preferable option.[20] Like with age-control technologies more broadly, it may be appropriate to pause the implementation of such bans until robust privacy methodologies are in place.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca

[16] Consultation on age assurance – What We Heard, Office of the Privacy Commissioner of Canada, March 21, 2025.
[17] Per the OPC's website guidance: Once an organization has determined that its website or service is likely to be accessed by children and poses potential harm to them, it should consider whether there are reasonable risk mitigation approaches other than age assurance that could address the potential harm.
For example, behavioural advertising that relies on a detailed profile of individuals poses a potential harm to children. Rather than addressing this by applying age assurance to all users from the outset, an organization should instead consider:
- Prohibiting (or only using ad services that prohibit) the use of any inference that a user is, or may be, a child for the purpose of behavioural advertising;
- Discontinuing behavioural advertising if it becomes aware that the user is a child (for instance, automatically opting out any user who indicates that they are a child during an account creation phase or whose device sends a signal indicating that the user is a child); and,
- Making appropriate opt-out controls readily available.
[18] Per the OPC's developer guidance: Proofs of concept or demonstrations by the French CNIL, Spanish AEPD, and European Commission all show that double anonymity is possible. This can be achieved by measures such as involving an intermediary (such as an app) that passes messages between the relying party and the age assurance service provider, or by providing the individual with a reusable credential that can be stored in a digital wallet. Age assurance providers are not required to meet this requirement, but the OPC strongly encourages double anonymity to be built into systems, as a privacy protection.
[19] See above, note 11
[20] See: The Illusion of Protection: Why Canada's Growing Push to Ban Social Media for Kids Won't Work, Michael Geist Blog post, April 28, 2026.