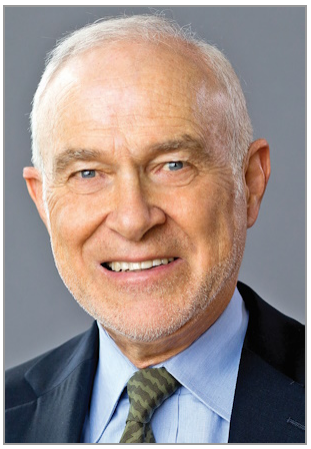
LAW360® Canada

Law360 Canada | 2 Sheppard Avenue East, Box 54 | Toronto, Ontario, M2N 5Y7 Canada | www.law360.ca
Phone: (800) 668-6481 | customerservice@lexisnexis.ca

Online age controls for children: Can they work?

By **David Young**



David Young

Law360 Canada (May 28, 2026, 9:56 AM EDT) -- Recent events such as the Tumbler Ridge shootings have brought to a head the issue of protecting children and youth online. However, the landscape for online harms protection for young people is at a crossroad. Increasing concerns are militating toward adoption of mandated age-control rules in online harms laws and social media bans. Yet in their current state of development, the methodologies for such controls present significant privacy and other societal risks, not only for young people, but potentially all internet users.

Governments and regulators are considering a number of potential protective measures. Receiving much attention are social media bans for children and youth, adopted in a number of international jurisdictions and proposed in Manitoba.

fadfebrian: STOCKPHOTO.COM

The federal government is working toward an online harms law focused on youth as well as a reformed privacy law that may include youth-protective provisions. Additionally, rules regarding content moderation and access controls have evolved, mainly through privacy regulator guidance but in some jurisdictions, legislation.

Interventions directed at protecting youth online for the most part require an age control, commonly referred to as "age verification" but in the technical jargon, "age assurance."

The most significant concerns with operationalizing an age-control rule relate to the potential privacy risks resulting from extensive collection of personal data required for such a system.

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, as well as potentially unequal access to technologies that may be required to utilize such a protocol.

There are a number of age assurance methodologies, some of which have been in use for many years, typically for controlling access to adult websites and online shopping venues. However, now

their potential application has expanded exponentially with the concerns for online harms to children and youth.

The most commonly used age-assurance methodology currently is "self-declaration" in which the user, or a person who knows them (such as a parent), states that the user is above a certain age, without any verification procedure to confirm the validity of the declared age. The age determination relies entirely on the confidence that the platform has in the declaration being accurate. Relative to other, more rigorous protocols, self-declaration is 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.

Two control protocols that provide a more rigorous determination are "age verification" and "age estimation."

Age verification protocols require the individual to provide a verifiable document proving age. This may involve submitting an image of a government-issued identity document containing their date of birth together with verification such as taking an online photo of the user's face.

Age estimation is a protocol based on an individual's features or behaviours instead of specific ID documentation. It can include biometric analysis of an individual's face, or a sample of their voice, or behavioural analysis of interactions with a platform or other online activity.

Both of these protocols involve significant privacy concerns related to the collection and retention of potentially sensitive personal information of prospective website users. A further concern is that such information likely will need to be collected for *all potential visitors* to a platform, with attendant greater risks for privacy protection. While it may be possible to narrow the application of such a requirement to youth-oriented sites, this would not be the case for a social media ban which would require all users to provide age verification in order to access a platform.

Understanding these potential risks, there has been much 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.

However, the majority of privacy regulators internationally has determined that age assurance should be deployed — or mandated — albeit with caution, on the condition that the potential privacy risks are mitigated.

The federal Office of the Privacy Commissioner, aligning with other regulators, has concluded that age controls may be required in certain instances and has published guidance in this regard. The guidance reflects the OPC's conclusions from a year-long consultation on age assurance as well as insights gained from a sweep study of such protocols in diverse international jurisdictions.

The OPC identifies the potential privacy concerns inherent in any age-control methodology including breach, unauthorized tracking and profiling and disproportionate application of access restrictions based on differential characteristics of user groups.

To minimize these potential risks, the OPC sets out privacy-protective criteria for such methodologies, specifically: minimizing collection and retention of personal information; limiting the information included in any age assurance result; prohibiting secondary use of the information; not retaining or disclosing the information generated, except the final result; prohibiting any use of information about the individual's online activities, and ensuring that the age assurance process does not disadvantage any societal group.

On the other hand, recognizing the attendant risks, the OPC has noted the development of non-identifying methodologies for age control. Consistent with the view of the international experts that adoption of age assurance protocols should not move forward under currently known technologies, it

may be argued that development of such non-identifying methodologies should be the priority.

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.

David Young is principal at David Young Law, a privacy and regulatory counsel practice in Toronto.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the author's firm, its clients, LexisNexis Canada, Law360 Canada or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Interested in writing for us? To learn more about how you can add your voice to Law360 Canada, contact Analysis Editor Richard Skinulis at Richard.Skinulis@lexisnexis.ca or call 437-828-6772.
