February 5, 2024

Online Age Verification is Crucial and Bill S-210 Gets It Wrong

By: Emily B. Laidlaw

Matter Commented On: Bill S-210, *An Act to restrict young persons' online access to sexually explicit material*, 1st Sess, 44th Parl, 2021.

Age verification is a tool that verifies a user's age before permitting them to access certain online content, websites, or apps. It is primarily advocated for the purpose of verifying the ages of users and creators on pornography sites. Age verification can have wider application and has been proposed as a solution to an array of child safety issues on social media, including algorithms pushing content about eating disorders, self-harm, misinformation, and viral "challenges", to luring and cyber-bullying. For example, many platforms ban users under 13 years old and/or have child protection measures for 13-17-year-olds, such as blocking direct messaging, limiting screen time, or curating age-appropriate content. TikTok, for example, has such tools, but relies entirely on user self-verification of age and encouragement of parental oversight (such as their service, Family Pairing).

Enter Bill S-210, *An Act to restrict young persons' online access to sexually explicit material*. Its goal is narrowly to protect children from accessing sexually explicit content online, therefore the broader ways that age verification might be used to enforce age limits on social media is outside of its scope. The objectives of S-210 are laudable. Children should not be viewing pornography. But the Bill has problems, which are twofold. First, the Bill is fundamentally flawed as drafted. Second, even if the drafting language can be fixed, age verification belongs in a broader package of online safety legislation, which will hopefully soon be introduced by the Federal Government (see my commentary with Taylor Owen here and here). Age verification is only one piece of the child-protection puzzle. A holistic approach to children's rights and safety includes legislation that tackles content moderation, algorithmic accountability, and platform design.

Age verification is important to child safety, but it is a high-risk undertaking that requires safeguards and careful constraint if mandated in legislation. Many individuals are working hard to develop technology that delivers all of this. To understand the legislation and why it should cause such alarm, it is helpful to understand more about age verification technology and the context of the child protection issues.

Age Verification in Context

On its face, age verification seems relatively straightforward and uncontroversial. After all, in the physical world youthful-looking individuals are asked to provide identification by a store clerk before purchasing alcohol, cigarettes, or pornography. Until recently, the open ethos of internet

governance supported a do-nothing approach by states, leaving it to the market and parents to manage any risks of harm. Left in the dust has been child protection.

A study by the UK Children's Commissioner reveals that the average age children first see pornography is 13, with 10% of children seeing pornography by the age of nine. In 2023, the U.S. Surgeon General issued an advisory as to the harms of social media on youth mental health. On January 25, 2023, the B.C. Government announced plans to amend legislation to enable it to sue social media for negligent design of their algorithms. Much like lawsuits against big tobacco and opioid manufacturers, they will seek to recover the costs of the public harms of social media, such as the costs of treatment, counselling, and education. Similar litigation is underway in the USA. Social media, all-round, is bad news for kids without careful parameters.

Age verification emerges from this toxic mess as a viable option to strengthen child protection, including children's privacy rights, in spaces that are posing increasing risks to children's mental and physical health. The problem is that age verification in the online realm is difficult to deploy without creating a significant threat to privacy, security, and freedom of expression. As a proportionate measure to protect children, it tends to fall woefully short. Methods might include age estimation using AI or combined with human oversight, confirmation through a parent's account, hard identifiers such as driver's licenses and passports, or a third party verification service.

Often, such mechanisms incentivize a general system of surveillance, tracking all kinds of lawful interactions in an effort to find the bad ones. This can have a chilling effect on freedom of expression, privacy, and anonymity, particularly for vulnerable youth figuring out who they are. Inevitably the process involves the collection and analysis of data, thwarting the principle of data minimization. Without security standards, a company is incentivized to put in place a rudimentary system, e.g. requiring users to upload IDs without a commensurate level of security for such sensitive data. If hard identifiers are required, this excludes individuals without identification, primarily individuals with lower incomes. If focused on pornography, depending on the verification system, it risks stigmatizing access to pornography, especially if the government acts as verifier as the first iteration of Bill S-210 proposed. Let's not forget that for adults pornography is legal. It can also be easy to circumvent age verification e.g. steal your parent's ID or use a VPN. If age estimation is used, there is a built-in risk of error. Depending on the technique used, AI is used to scan faces, monitor browser history, or other behavioural indicators (12-year-olds might say that they are 18 but usually still act 12), which amplifies the privacy concerns.

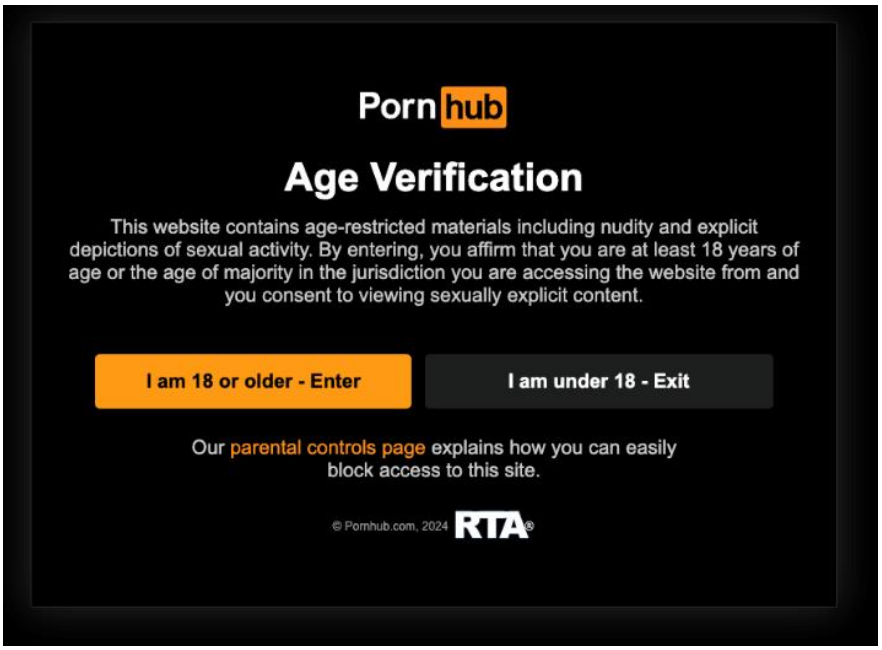
Many technology experts have been working hard at developing privacy-preserving age verification technology, such as a third-party verifier that issues a token, which is stripped of personal information. Digital ID companies, such as Yoti, have begun to be used by social media like Meta for age verification purposes. The technology is swiftly evolving, but *evolving* is the key word.

For the above reasons, some privacy and cybersecurity advocates argue that age verification should not be used at all. As European Digital Rights reminded us, "you can't 'childproof' the internet." Australia, for example, explored mandatory age verification for pornography sites and eventually abandoned it. Other jurisdictions are ploughing ahead. Part 5 of the UK's *Online Safety Act*

requires age verification for commercial pornography providers, thus excluding sites that purely host user-generated content, e.g. creator content on OnlyFans. The European Union's *Digital Services Act* (*DSA*) is vaguer and simply states that very large online platforms must mitigate risks by "taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate" (at Article 35(1)(j)). As part of a broader effort at child protection, this vagueness is arguably appropriate, although it leaves a lot to the regulator's interpretation. Various US states have passed age verification laws leading Pornhub, for example, to block access in several states.

Age Verification in Practice

It is helpful to illustrate how age verification (or lack thereof) currently works with a few examples. Pornhub (formerly MindGeek, now Aylo, recently bought by Ethical Capital Partners) presents the following warning when you first enter the site:



Once a user confirms they are 18 or older, they are immediately presented with several video snippets of sexually explicit material. It is shockingly easy for a minor to access a treasure trove of sexually explicit material unless a parent has implemented and routinely checks safety measures, e.g. Google SafeSearch, Apple Screen Time.

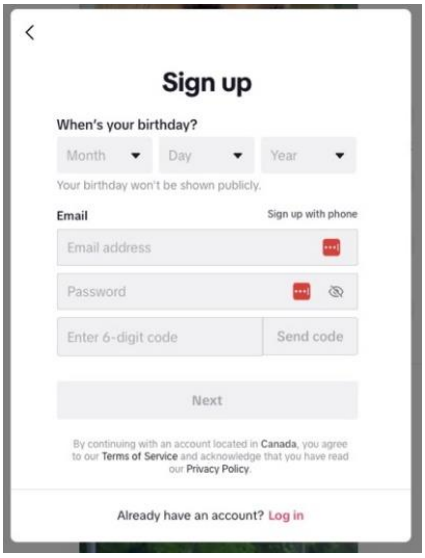
OnlyFans uses a mix of technology and human moderation to verify the age of fans. They advise,

> It is against our Terms of Service and our Acceptable Use Policy for anyone who is under 18 years old to view, access or post content on OnlyFans. We invest heavily in technology and human moderation teams to make sure this policy is followed. If anyone seeks to get around these policies and controls, OnlyFans will take appropriate action against them.

OnlyFans' verification requirements differ by country, presumably to comply with legal requirements. Verification can include "personally identifying information, confirmations, payments details, and documents."

Thus far my focus has been on verification of users. Another dimension is verifying the age of those uploading the videos and/or in the videos. They are not the focus of Bill S-210 but tend to be captured by whatever system is put in place. Creator safety has a different dynamic, stretching well beyond age verification to include issues of consent and exploitation. There are two different groups. The first group are the creators - adult entertainers and sex workers - for whom these sites should be designed. Any age verification law must guard against unintended consequences to these individuals and their communities, such as stigmatization, and should promote their safety and security. The second group are victims, whose abuse is live-streamed or recorded and uploaded without verification that the content was created or shared consensually. It is beyond this short commentary to dive deep on verification from these angles, although it is foundational to online safety in these spaces. Creators are subject to strict age verification criteria by OnlyFans, requiring nine items that verify identity. PornHub was exposed for its failure to protect victims in the New York Times exposé "The Children of Pornhub". Unverified videos were deleted, and creators must now verify using the Model Program.

Beyond pornography platforms, age verification measures vary, and platforms are not entirely transparent, a point in favour of an online safety commissioner to provide oversight. There is no law in Canada mandating a minimum age to access social media, although duties apply to platforms in the narrow context of privacy. With the exception of Quebec (*Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 at s 4.1), no Canadian private sector privacy law specifically addresses children's privacy, although privacy commissioners do take special note of the privacy rights of children (Federally, see *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5). As discussed, TikTok relies on self-verification of age, and 13-17 year olds are subject to automatic restrictions, such as no private messaging, a daily one-hour screen limit, and muting notifications later at night.



Similarly, Meta requires age self-verification to sign up for Instagram, which defaults to a private account for anyone under 16. However, a child can select to make their account public, and users 16 and older default to a public account. Meta has also partnered with Yoti for age estimation and uses AI to track behavioural indicators.

While some steps are taken to strengthen the weakness of self-verification, in general these child protection measures are only as good as their parental oversight or a child's honesty.

Why Bill S-210 is not the Answer

Bill S-210 was introduced as a private members bill by Senator Julie Miville-Dechêne in 2021 (listen to her recent robust debate about the Bill with Professor Michael Geist here). At that time, I testified before the Senate and expressed concerns about the substance of the Bill although not the goals. The Bill made its way through the Senate and a second reading in the House of Commons. The next step is committee review. With the prospect of online harms legislation I expected that this Bill would wither on the vine, but that is not the case.

Bill S-210 provides that any internet service that for commercial purposes makes available sexually explicit material to a young person is guilty of an offence (at s 5). It is a defence if the internet service uses a prescribed age verification technology (at s 6(1)), which will be set out in regulations (at s 11). If an enforcement authority has reasonable grounds to believe an offence has been committed, they can issue a notice to the internet service which, among other things, identifies steps the internet service must take to comply with the Act within a set period of time (at s 8). If the internet service fails to comply, the enforcement authority can apply to the Federal Court for a website blocking order (at s 9). The Bill pre-emptively acknowledges (and implicitly approves) blocking more than sexually explicit material or blocking access to such material by adults (at s 9(5)).

There are four primary flaws with Bill S-210.

1. ***Age Verification Belongs in Online Harms Legislation***

Age verification fits in online harms legislation, because true child protection requires a holistic approach. I expect that the Federal Government will introduce legislation modelled on the UK or EU. While different from each other, the core approach is the same, namely requiring online platforms to be responsible corporate actors by imposing a duty of care/due diligence requirement to manage the systemic risks of harm of their services. Taylor Owen and I summarized the core components that should form the basis of a Canadian law as follows:

> (1) A duty on platforms to act responsibly, including by upholding fundamental rights, protecting users from harm, and conducting risk assessments on products used by Canadians.
> (2) A special duty to protect children from harm.
> (3) The creation of a regulator, with the power to investigate and audit platforms, mandate corrective action, and impose fines.
> (4) Mandatory transparency by platforms, including data sharing with researchers and an avenue to audit and verify that they are meeting their legal obligations.

(5) A victim-centred forum for recourse for users impacted by platforms' content moderation practices.

The Government has two potential options. It can impose a general obligation mirrored on the *DSA*, wherein age verification might be part of how social media demonstrates it mitigates risks to children. Or, in addition to general child safety measures, age verification can be required in narrow circumstances. In the UK, for example, age verification is required for providers of pornographic content to ensure that "children are not normally able to encounter" such content (*DSA* at s 81(2)).

Age-appropriate social media is critical for healthy development of children. Online safety legislation is poised to deliver this, and narrowly slicing off age verification technology in the context of pornography does not do enough to protect children.

Recommendation: Age verification should be addressed in online safety legislation as part of a broader package of child protection measures, including algorithmic accountability, content moderation, platform design, and commissioner oversight.

2. The Scope is far too Broad

Bill S-210 captures any and all internet services in its scope. Section 5 provides that "any organization that, for commercial purposes, makes available sexually explicit material on the Internet to a young person is guilty of an offence".

As OpenMedia commented in their letter, it would put much of the internet "behind an age gate". 'Makes available' is broad. Senator Miville-Dechêne confirms that the target is pornography providers. However, as drafted s 5 includes any internet service that enables content to be accessed, which would include social media, search engines and internet access providers. All of these services 'make available' sexually explicit material, because users post it even if it is against their terms and conditions. And all of these organizations make such material available for commercial purposes, because their profit derives from advertising or subscription services and similar. The provision should be re-drafted to narrowly target commercial pornography providers.

Further, sexually explicit material refers to the definition in s 171.1(1) of the *Criminal Code*, RSC 1985, c C-46 (Bill S-210 at s 2), which includes visual, audio, and written material. This is too broad for the implementation of age verification and would include sexually explicit written material.

Recommendation: Narrow the scope to commercial pornography providers or platforms whose dominant purpose is to make available sexually explicit material. Narrow the definition of sexually explicit material to visual material.

3. The Website Blocking Provisions are Likely Unconstitutional

The enforcement authority may apply to the Federal Court to order website blocking if an internet service makes available sexually explicit material and fails to take remedial steps ordered by the

authority (at ss 8-9). The Bill appropriately leaves website blocking as a last resort mechanism and requires a court order. However, in a surprising twist, the Bill explicitly contemplates overbroad website blocking and appears to condone it (at s 9(5)). It is worth setting out s 9(5) in its entirety as, in my view, this provision would likely not survive constitutional scrutiny by a court:

> **9(5)** If the Federal Court determines that it is necessary to ensure that the sexually explicit material is not made available to young persons on the Internet in Canada, an order made under subsection (4) may have the effect of preventing persons in Canada from being able to access
> **(a)** material other than sexually explicit material made available by the organization that has been given notice under subsection 8(1); or
> **(b)** sexually explicit material made available by the organization that has been given notice under subsection 8(1) even if the person seeking to access the material is not a young person.

There was a time in the internet governance community when any website blocking was viewed as a disproportionate interference with freedom of expression, because it acts as a prior restraint on the ability to seek and receive information (e.g. see exploration here). As I advised the Senate in 2022, it is a blunt tool, easily circumvented, tends to block more than it should for longer than it should, lacks due process, and tends to be global in reach. Prior restraint is the worst form of censorship, because it prevents the communication from happening in the first place.

However, as the internet matured, courts and human rights advocates have had to grapple with the complicated nature of the internet's global reach and the limits of jurisdiction. A foreign-based website might make pornography available online without any effort to limit access to children. If Bill S-210 passed, it would be enforceable against a Canadian-based internet service, but it would be much more difficult to enforce against a service based elsewhere. Website blocking emerges as a tool to enforce Canadian law within Canada. The problem is that it is too easy for blocking to be done poorly and it tends to be prone to mission creep. For example, in the UK, a court first approved blocking to address copyright infringement then counterfeit goods.

Website blocking has not been richly explored by Canadian courts, and only recently in the context of copyright infringement (see *Rogers Media Inc v John Doe 1*, 2022 FC 775 (CanLII) and *Teksavvy Solutions Inc v Bell Media Inc*, 2021 FCA 100 (CanLII) (*Teksavvy*)). The courts rejected the need for a detailed freedom of expression analysis as unnecessary in light of the "undisputed, ongoing infringement and measures to limit over-blocking" (*Teksavvy* at para 56). A similar '*Charter* light' analysis was used by the Supreme Court of Canada in *Google v Equustek Solutions*, 2017 SCC 34 (CanLII) to address global delisting from search results. In my opinion, all of these cases failed to adequately analyze freedom of expression. That said, they were all cases where the infringement was clear and the scope of the order was a live point of discussion. Bill S-210 is the opposite. Section 9(5) explicitly enables a court to block access to lawful content and does not identify any safeguards.

The role and limits of website blocking under human rights law has been in front of the courts for many years in the UK and the EU, and the Federal Government can draw from their experience to amend s 9. The general principles are as follows:

- Website blocking should be a last resort and necessary to achieve an important objective;
- It should only be ordered by a court;
- It should be proportionate as in narrowly tailored, such as time limits, blocking of specific content or pages and not an entire website;
- There should be stringent safeguards in place to ensure procedural fairness and to guard against collateral effects, such as targeting content beyond that which is illegal. See commentary on recent EU cases here.

Recommendation: Delete s 9(5) and insert criteria for website blocking.

4. The Verification Criteria are not Stringent Enough

Finally, under s 11 the Bill leaves it to regulations to prescribe the age verification method, but identifies the key features that must be present in whatever method is prescribed. This is an appropriate approach to ensuring that the approved age verification method evolves with technology and society, which is best done through regulations. However, the list of key features is under-inclusive. Currently under s 11(2), the Governor in Council would consider if the method:

(a) is reliable;
(b) maintains user privacy and protects user personal information;
(c) collects and uses personal information solely for age-verification purposes, except to the extent required by law;
(d) destroys any personal information collected for age-verification purposes once the verification is completed; and
(e) generally complies with best practices in the fields of age verification and privacy protection.

I recommend two things are added to the list. First, cybersecurity is core to age verification and not currently addressed. It is implicit to the above provisions, but it should be spelled out as regulations might focus on data governance rather than the necessary security safeguards that underpin it. Second, freedom of expression is implicated in any age verification method and therefore must be central to consideration of what is adopted.

Recommendation: Add cybersecurity and freedom of expression as necessary considerations to the adoption of an age verification method.

This post may be cited as: Emily B. Laidlaw, "Online Age Verification is Crucial and Bill S-210 Gets It Wrong" (5 February 2024), online: ABlawg, http://ablawg.ca/wp-content/uploads/2024/02/Blog_EL_Bill_S210.pdf