DALHOUSIE UNIVERSITY
SCHULICH SCHOOL OF LAW

INFORMATION POLICY LAB

THINK OF THE CHILDREN

The Policy Trade-offs of Digital Age Verification

Edited by Michael Karanicolas, Finn Mitra, and Marium Nawal Oishee

May 2026

Table of Contents

Foreword

By Michael Karanicolas, Associate Professor of Law, James S. Palmer Chair in Public Policy & Law, Dalhousie University

It is hard to think of an issue which inspires as much passionate engagement as child protection. Around the world, many of our most important achievements, and our most consequential policy mistakes, have been pushed forward under the banner of helping or protecting children. As digital technologies have transformed society, a heated debate is emerging over their impact on child development, and the appropriate regulatory response to promote child safety online.

For advocates of stronger regulation, the status quo is pure madness. Virtually every society imposes strict rules preventing children from accessing things that are harmful to their wellbeing or development, from pornography, to addictive substances like cigarettes, to antisocial activities like gambling. From that perspective, the idea that any child with a web connection can obtain unfettered access to the excesses of the digital world, from hardcore pornography to toxic hate speech, is a supreme act of societal negligence. Child protection advocates point to a long list of victims of our permissive digital culture, from children driven to suicide by cyberbullying, to growing rates of anxiety and depression, to the rapid rise in social media addiction. These are powerful arguments, which explain why age verification rules, including in some cases total bans on youth access to social media, have gained so much traction in recent years.

And yet, as with many digital policy challenges, the solutions are not as simple as they appear, and present complex trade-offs both for children and for our digital society as a whole. Age verification technology, as it currently exists, is neither particularly effective, nor does it offer reliable privacy protections. To the contrary, experts have painted these proposals as a security nightmare, that introduces new threat vectors for targeting highly sensitive personally identifiable information (PII), and which normalizes increasingly invasive digital surveillance. There are legitimate questions about these laws' efficacy in targeting the root cause of ills impacting children, both because of a lack of data that causally ties digital technologies to these problems, and because innovative and creative young people are likely to find ways around whatever rules are imposed.

The purpose of this publication is to provide a comprehensive scoping of the age verification landscape, and the trade-offs that are likely to accompany various solutions, to provide an informed background for a contentious area of policy debate. More than anything else, as global momentum towards age verification continues to grow, it is important to be clear-eyed about the implications of various proposals for child safety, privacy, freedom of expression and, above all else, for the nature of digital communications over the coming decades. Standard setting work that is taking place at the moment is likely to be hugely influential in setting the parameters for how our future internet will function. It is critical that policy-makers think carefully about the implications of the regulatory models they impose.

About this Report

This publication was developed as part of Dalhousie University's Information Policy Lab, an innovative new experiential learning class aimed at onboarding students into the tech policy space and developing their critical analytical capabilities by training them to answer emerging policy questions. The chapters were drafted by the Policy Lab participants, under the guidance of faculty members with

subject matter expertise in the regulation of new technologies, and in consultation with external experts from industry, civil society, and academia with specialized knowledge of the questions under examination.

The authors wish to thank experts who provided insight into the research and editing process for this publication, including Aliya Bhatia, Suzie Dunn, Justin Hendrix, Gillian Findlay, David Fraser, Tyler Henry, Ben Lennett, Sen. Julie Miville-Dechêne, Sean O'Brien, Jenna Poste, Iain Rankin, Katelyn Ringrose, Melanie Selvadurai, Basia Walczak, and Val Webber, all of whom provided helpful feedback and inputs for the development of this work, though the opinions and conclusions expressed are solely those of the authors. Thanks as well to Juliana Gallin, for designing the formatting and cover.

For more information about the Information Policy Lab, or this publication, feel free to reach out to us at karanicolas@dal.ca.

Executive Summary

Around the world, there is growing legislative momentum towards adopting digital age verification and age assurance measures targeted at protecting children from inappropriate online content, or restricting their access to social media. While these initiatives are driven by genuine child-protection concerns, there are significant differences both in how these rules have been implemented and in the scope of content they cover. This Report considers the trade-offs embedded in age verification policies, particularly insofar as they may negatively impact digital privacy and freedom of expression, as well as harm child welfare among marginalized groups who rely on digital media for education, cultural engagement, and self-development.

Age verification can include a range of different technologies and regulatory requirements, which may be targeted at publishers, device manufacturers, or other actors within the digital information ecosystem such as app stores. Techniques for assessing the age of users may include "age estimation", which refers to algorithmic guessing of age, based on behaviour, facial analysis through selfies, voice examination, or other signals, "age inference", which uses contextual clues such as a user's account or browsing history to assess age, and "age verification", which assesses documentary or biometric proof to demonstrate identity. These models provide varying levels of accuracy, but all present distinct challenges in terms of privacy and security.

Although the push towards age verification suggests a growing policy consensus on the pressing need to curb children's access to certain forms of digital content, and social media in particular, the research picture is more nuanced. Studies which link social media use to developmental harms, such as depression or anxiety, and are overwhelmingly correlational, and there is limited direct evidence of a causal link. Moreover, the benefits and harms of social media use are not evenly distributed, as the importance of social media as a tool to support identity exploration and community building are particularly high among marginalized groups, such as First Nations or refugee youth. An analogous situation exists with regards to access to pornographic content, where early exposure may be correlationally, though not causally, tied to distorted understandings of intimacy and other negative outcomes. However, once again, positionality is critical, as research suggests that LGBTQIA+ youth are both less susceptible to these harmful adverse effects, and more reliant on pornography to explore and develop their sexual identities. In the case of both pornography and social media, individual experiences vary significantly, including based on age, developmental stage, frequency of exposure, social context, the availability of support networks, and the precise nature of the content, or the platform, they are exposed to, all of which challenges the bright line distinctions provided by most laws. In short, while there are potential concerns related to both youth access to social media and to pornographic content online, broad access restrictions fail to capture the nuance of differential impacts, and risk exacerbating existing information gaps rather than improving child welfare outcomes.

These trade-offs are particularly concerning in light of the significant risks to privacy and freedom of expression presented by existing age verification models. Publisher-level systems multiply data-collection points and present novel vectors for cyberattacks targeting highly sensitive personal information. Behavioural and AI-based models depend on pervasive surveillance and opaque profiling, raising concerns about accuracy, bias, data repurposing, and platform consolidation. Device-level approaches reduce repeated verification but concentrate risk in centralized systems, creating attractive targets for cyber criminals.

From a freedom of expression perspective, age-verification regimes condition access to lawful information on identity disclosure, eroding online anonymity and generating chilling effects. These effects are not limited to adult content: legal uncertainty encourages platforms to over-comply, resulting in the suppression of lawful educational, artistic, and sexual-health materials. As a result, youth lose access to precisely the information that supports safe development. The burdens of verification systems are also unevenly distributed, with disproportionate impacts on marginalized groups who face greater barriers to verification through standard means.

Ultimately, this Report finds that age verification presents an overly simplistic solution to multifaceted and complex social programs and that, more than anything else, the policy ecosystem would benefit from additional research into the precise relationship between digital technologies and developmental harms. Jurisdictions which have yet to introduce age verification rules should carefully observe those that have implemented them, to assess both their positive and negative impacts, and above all their efficacy in addressing the overarching child safety concerns that motivated their passage. Governments would also benefit from expanding youth support services and strengthening education which targets both digital literacy and sexual health. Where age verification legislation is under consideration, the Report offers the following legislative best practices:

1. **Focus on proportional, risk-based regulation**
   Laws should be narrowly targeted to demonstrable harms and applied only where necessary, rather than imposed as a universal requirement across mixed-use platforms.
2. **Prioritize privacy and data minimization by design**
   Any age-assurance framework should minimize data collection, avoid static identifiers, prohibit function creep, and enforce clear deletion and transparency requirements.
3. **Preserve anonymity and access to lawful information**
   Policymakers should recognize online anonymity as a key element of the right to freedom of expression, and to fostering help-seeking behaviour, especially for youth and marginalized communities.
4. **Invest in evidence-based alternatives**
   Comprehensive sexual-health education, child-centred platform design, targeted content moderation, and accessible mental-health and support services may be more tailored solutions to directly address underlying harms without broad rights trade-offs.
5. **Proceed cautiously and iteratively**
   Given unresolved technical, legal, and equity concerns, governments should commit to robust consultation with technical experts, as well as stakeholders from marginalized communities, including hearing from young people themselves, before entrenching age-verification infrastructure.

Protecting children online is an essential policy objective, but current legislative models threaten to entrench new infrastructures of pervasive surveillance in service of uncertain gains for child welfare. This is neither a sufficient nor a proportionate solution. A rights-respecting, evidence-informed approach centred on harm reduction and youth empowerment offers a more sustainable and effective path forward.

CHAPTER 1
Introduction to the Legislative Landscape

By Roy Maianski

Age-assurance laws have emerged as a major point of contention in internet regulation. Rules aimed at restricting underage access to online content have been passed or proposed across a number of jurisdictions, including Canada, the United Kingdom, France, Brazil and, as of late 2025, roughly half of U.S. states.[1] The widespread deployment of age-assurance regulations has generated a novel set of problems, shaped by contemporary concerns about digital privacy, platform governance, and state power.

Generally, age-assurance laws seek to restrict children's access to particular categories of online content and, in some jurisdictions, to address the harms associated with children's social media use. While children's online safety is often described as a laudable goal, critics have noted the trade-offs that these laws entail. One concern is that the internet provides substantial educational benefits to youth, and that overly broad restrictions may limit access to supportive communities and informational resources which many minors rely on.[2]

Age-assurance laws also raise freedom of expression concerns for all internet users, including through their potential to disproportionately silence marginalized voices and LGBTQ+ content under the guise of child protection.[3] Age-verification laws may also present critical privacy and security risks.[4] Age verification systems often require users to submit personal identification data online, creating new vulnerabilities for misuse or hacking. Without strong privacy safeguards, data collected for age verification may be retained or shared with third parties, thereby exacerbating risks of surveillance and identity theft.[5] Compelling users to upload government-issued identification raises significant privacy risks, especially when the data is tied to adult-content platforms. Advocates for internet freedom further stress that age-verification laws erode the right to anonymous speech by creating ID checkpoints.[6]

This chapter introduces how legal doctrines around the trend of age-gating the internet have evolved over time.

---

[1] Age Verification Laws Hit 25 States as Congress Weighs 19 Bills", *The TechBuzz* (Dec 2025), online: https://www.techbuzz.ai/articles/age-verification-laws-hit-25-states-as-congress-weighs-19-bills.

[2] Paige Collings, "Global Age Verification Measures: 2024 in Review", Electronic Frontier Foundation (27 Dec 2024), online: https://www.eff.org/deeplinks/2024/12/global-age-verification-measures-2024-year-review.

[3] Eric Goldman, "The 'Segregate-and-Suppress' Approach to Regulating Child Safety Online" (2025) 28 Stanford Tech L. Rev. 173, online: https://law.stanford.edu/wp-content/uploads/2025/07/Segregate-and-Suppress.pdf

[4] See, e.g., a Joint statement of security and privacy scientists and researchers on Age Assurance: https://csa-scientist-open-letter.org/ageverif-Feb2026.

[5] Christine Marsden, "Age-Verification Laws in the Era of Digital Privacy" (2025) 10:2 National Security Law Journal 210, online: https://www.nslj.org/wp-content/uploads/Marsden-10.2-v272.pdf.

[6] Freedom House, "Freedom on the Net 2025: An Uncertain Future for the Global Internet" (Washington DC, Dec 2025), online: https://freedomhouse.org/sites/default/files/202512/FOTN%202025_final_digital_120525.pdf.

1. The Evolution of Online Age-Verification Doctrines

Debates surrounding young people's access to harmful content have traditionally focused around pornography. These concerns long predate the internet. In the United States, the law has long held that obscene content (pornography) can be restricted from minors.[7] However, in *Butler v. Michigan* (1957), the U.S. Supreme Court ruled that child-protection measures cannot justify broad prohibitions on adults' lawful access to content.[8] As Justice Frankfurter wrote, the effect of such restrictions is to "burn the house to roast the pig".[9]

The arrival of the commercial internet in the 1990s prompted the first, largely futile, federal effort to regulate minors' online access to adult content —the *Communications Decency Act* (CDA) of 1996.[10] The CDA sought to restrict minors' access to "patently offensive content."[11] This legislation was mostly invalidated on First Amendment grounds in *Reno v. ACLU* (1997) with the U.S. Supreme Court holding that the law infringed on the freedom of expression rights of adults.[12] In 1998, Congress enacted the *Child Online Protection Act* (COPA), a law targeting pornography websites and other "harmful materials" on the internet.[13] However, this effort also failed, with the Supreme Court ruling that the law's reliance on "community standards" language to define harmful content made it unconstitutionally overbroad.[14]

The modern history of age-verification began in 2017, with the United Kingdom's proposed *Digital Economy Act,* which would have required pornographic websites to deploy age-verification systems. However, the UK government abandoned the plan in 2019, citing a desire to legislate "more comprehensively" on the matter.[15] Another early player in the age-verification landscape was China, who, in 2019, introduced regulations restricting children's access to video games. In order to enforce this regulatory regime, Chinese technology firms integrated government identification databases and experimented with facial recognition systems. By 2021, gaming company Tencent had deployed a system that scanned players' faces and cross-referenced them with the national ID registry to identify underage users attempting to circumvent the restrictions.[16]

Over the early 2020s, the age-verification trend accelerated in response to heightened public concern over children's exposure to both pornography and social media. The United Kingdom, following its earlier aborted efforts from 2017, incorporated child protection measures into the more comprehensive *Online Safety Act* (OSA) in 2023.[17] The OSA established a duty of care for online services to protect users (especially minors) from harmful content. Its scope extends to virtually all platforms, including social media, search engines, messaging apps, and pornographic websites, mandating the implementation of

---

[7] *Roth v. United States,* 354 U.S. 476 (1957).

[8] *Butler v. Michigan,* 352 U.S. 380 (1957).

[9] *Ibid.*

[10] Marsden, *Supra* Note 5.

[11] United States, Communications Decency Act of 1996, Pub L No 104-104, § 230, 110 Stat 56 (codified at 47 USC § 223).

[12] *Reno v. American Civil Liberties Union,* 521 U.S. 844 (1997).

[13] Marsden, *supra* Note 5.

[14] *Ashcroft v. Am C.L. Union,* 542 U.S. 656, 674 (2004).

[15] UK Parliament, "*Minister questioned on the future of age verification for online pornography*" (8 October 2019), online: Parliament.uk https://www.parliament.uk/business/news/2019/october/uq-on-online-pornography-age-verification

[16] Lauren Feiner & Arjun Kharpal, "China to ban kids from playing online games for more than three hours per week" (30 August 2021), CNBC, online: https://www.cnbc.com/2021/08/30/china-to-ban-kids-from-playing-online-games-for-more-than-three-hours-per-week.html.

[17] Online Safety Act 2023, c. 50 (UK).

"highly effective" age assurance measures.[18] The Act empowers Ofcom, as the regulatory body, to set codes of practice, as well as screen and approve acceptable technologies.[19] The child safety provisions came fully into force in July 2025, though their implementation has encountered several challenges. There are reports of widespread circumvention, with virtual private network (VPN) usage increasing significantly in the UK since the OSA went into effect.[20] Additionally, concerns have been raised that broad statutory definitions have extended age-gating practices beyond pornography, as traditionally understood, to now include a range of sexual health information, news, and other materials that may be relevant and educational for young people.[21]

In late 2024, Australia's Parliament passed the Online Safety Amendment ("Social Media Minimum Age") Bill 2024, which prevents children under 16 from accessing social media.[22] This legislation requires companies to take reasonable steps to verify users' ages and imposes monetary penalties for non-compliance.[23] As enforcement progresses, Australian regulators have commenced testing various age-assurance technologies through different pilot programs.[24] Like in the United Kingdom, Australia's law has faced challenges to its efficacy, as early reporting notes widespread circumvention by young people.[25] The law has also faces legal challenges from teenagers alleging that it places an undue burden on the civic freedom of political communication.[26]

In May 2024, France enacted Loi n° 2024-449, which grants age-verification enforcement authority to the Regulatory Authority for Audiovisual and Digital Communication (ARCOM), empowering the agency to enforce age-verification.[27] In June 2025, Pornhub blocked access to its website for all users in France —its second-largest market—in protest of the age-verification law, with some French politicians welcoming the outcome.[28]

Although the United States currently lacks a comprehensive federal policy on age verification, a patch-

---

[18] *Ibid* at s.12 (6).

[19] UK Dept. for Science, Innovation & Technology, "Online Safety Act: Explainer" (24 Apr 2025), online: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer.

[20] Liv McMahon, *"VPNs top download charts as age-verification law kicks in"* (28 July 2025), BBC News, online: https://www.bbc.com/news/articles/cn72ydj70g5o.

[21] Paul Sandle, *"UK's online-safety law is putting free-speech at risk, X says"* (1 August 2025), Reuters, online: https://www.reuters.com/world/uk/uks-online-safety-law-is-putting-free-speech-risk-x-says-2025-08-01/.

[22] eSafety Commissioner (Australia), "Social Media Age Restrictions", online: https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions

[23] *Ibid.*

[24] Josh Taylor, "Trial of tech that could be used to keep Australian under-16s off social media finds some errors 'inevitable'", *The Guardian* (31 Aug 2025), online: https://www.theguardian.com/australia-news/2025/aug/31/age-assurance-technology-trial-report-australia-under-16-social-media-ban-some-errors-inevitable.

[25] eSafety Commissioner (Australia), "Under the new age restrictions: March 2026 Early insights from Australian parents", online: https://www.esafety.gov.au/sites/default/files/2026-03/Under-the-new-age-restrictions-Early-insights-from-Australian-parents-March2026.pdf.

[26] Elizabeth Byrne & Jade Toomey, "High Court agrees to hear teenagers' challenge to under 16s social media ban", ABC News (4 Dec 2025), online: https://www.abc.net.au/news/2025-12-04/court-agrees-hear-teens-challenge-to-under-16-social-media-ban/106103338.

[27] Orrick, "The SREN Law: 5 Things to Know About New French Legislation to Supplement the EU Data Act, Digital Services Act, GDPR and More" (4 June 2024), online: https://www.orrick.com/en/Insights/2024/06/The-SREN-Law-5-Things-to-Know-About-New-French-Legislation-to-Supplement-the-EU-Data-Act.

[28] Anna Cooban, "Pornhub exits France, its second-biggest market, over age verification law", CNN (4 June 2025), online: https://www.cnn.com/2025/06/04/tech/pornhub-exits-france-age-verification-intl.

work of age-assurance laws have emerged at the state level. In 2022, Louisiana became the first state to enact an age verification law, targeting pornographic content.[29] In 2023, the states of Arkansas, Mississippi, Montana, North Carolina, Texas, and Virginia followed suit.[30] These laws require websites with at least 33.3% pornographic content to verify users' ages. As of June 2025, 22 states had enacted regulatory regimes regarding child online privacy protections; 19 states mandated age-verification to access adult content; 12 states required age-verification for social media use; and 6 states regulated social media design codes.[31] These state-level laws generally impose civil fines or allow lawsuits against pornographic sites that fail to age-gate access. The constitutionality of age-verification laws was examined by the United States Supreme Court in June 2025 in *Free Speech Coalition, Inc. v. Paxton*.[32] In that case, Texas's age-verification law was upheld against a First Amendment challenge, with the Court ruling that the law only incidentally burdens the protected speech of adults.

More recently, a few states have adopted legislation targeting age verification at the device or app-store level. These measures include Utah's *App Store Accountability Act,* Texas' *App Store Accountability Act,* and California's *Digital Age Assurance Act.* The latter requires that, beginning in 2027, new devices, including smartphones, computers, and app marketplaces must prompt users to input their age during setup, while existing devices must receive operating system updates to collect such age-related data.[33]

2. Ongoing Legislative Developments

Over the course of 2025, age verification initiatives gained significant momentum across several additional jurisdictions. In Canada, the Office of the Privacy Commissioner (OPC) conducted an exploratory consultation to evaluate emerging age-assurance technologies and their privacy implications, accepting submissions from industry, civil society, and academic stakeholders.[34] The OPC identified a number of considerations to inform policy development, such the need for risk-based assessment as to how these measures are applied, the need to consider these systems are a means to achieving safer online environments for youth (as opposed to an end in themselves), and the harms associated with both the risks these systems sought to address as well as the harms from their misuse.

Bill S-209 *("Protecting Young Persons from Exposure to Pornography Act"),* was introduced in May 2025.[35] The Bill's sponsor, Senator Julie Miville-Dechêne, has advocated for regulation in this space since at least 2020. Notably, the bill makes it illegal to allow minors to access pornographic content, framing reasonable use of age-verification and age-estimation as defences, rather than affirmative obligations.

---

[29] Louisiana, H.B. 142, 2023 Reg. Sess. (La.).

[30] New America (Open Technology Institute), "Pursuing Kids Safety through Online Age Verification Legislation" (2024), online: https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/pursuing-kids-safety-through-online-age-verification-legislation/.

[31] Nerd Harder: A Typology of Techno-Legal Solutionist Logics in Child Online Safety Laws - https://onlinelibrary.wiley.com/doi/10.1002/poi3.70012#poi370012-bib-0125.

[32] *Free Speech Coalition v. Paxton,* 606 U.S. ___ (2025).

[33] Lauren Feiner & Dominic Preston, "California enacts its own internet age-gating law", The Verge (13 Oct 2025), online: https://www.theverge.com/798871/california-governor-newsom-age-gating-ab-1043.

[34] Office of the Privacy Commissioner of Canada, "Consultation on Age Assurance: What We Heard" (2025), online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-age/report_age_2025/.

[35] Bill S-209, An Act to amend the Criminal Code (protection of children), 1st Sess, 45th Parl, Canada, 2025, pmbl (first reading), ["S-209"].

The Bill also provides a legitimate purpose defence, expressly creating exceptions for content related to "science, medicine, and the arts" and narrowing the scope of liability to providers of sexually explicit content. S-209 also excludes from liability organizations which incidentally provide access to pornographic content. The Bill includes a number of values that must be reflected in qualifying age verification/estimation systems, including that they must be "highly-effective", conducted by third-parties, abiding by data minimization principles and compliant with the best practices in the field. Where a company has been found in violation of the law, an oversight body's first action should be to issue a notice of violation, including recommendations for resolving the issue. A company that complies with a regulator's notice and recommendations will be discharged of liability. If it is not resolved, S-209 provides that the regulator may seek a blocking order which is binding on internet service providers. The offending organization can also be subject to criminal fines of $250,000 CAD for a first offence and up to $500,000 CAD for subsequent offences. Reporting suggests that a social media ban for children under 16 may separately be under consideration, though as of April 2026, this has yet to be introduced.[36]

The European Union (EU) is exploring its own unified approach to age verification. Article 28 of the *Digital Services Act* (2024) calls for Codes of Conduct on online child protection.[37] The EU is considering an electronic ID wallet that could serve across websites.[38] In South America, Brazil became the first Latin American jurisdiction to pass a sweeping child online safety law in 2025.[39] In addition to regulating targeted advertising to youth, the Brazilian legislation also imposes age-assurance requirements on providers. In Asia, the Indian government has considered using the national biometric system Aadhaar for online age-verification.[40]

The global rise of age-verification laws reflects a striking regulatory shift in favour of more stringent child safety rules. Yet, as the following chapters demonstrate, operationalization of age-gating has collided with constitutional restrictions, technological constraints and unresolved tensions between privacy, safety and free expression. The next chapter turns to the contemporary technological landscape, examining how industry is shaping this evolving field.

---

[36] Catharine Tunney, "Liberal members vote in favour of age restrictions for social media, AI chatbots", *CBC News* (11 Apr. 2026), online: https://www.cbc.ca/news/politics/liberal-party-vote-on-social-media-age-restrictions-9.7159746.

[37] Svea Windwehr & Alexis Hancock, "Digital Identities and the Future of Age Verification in Europe", Electronic Frontier Foundation (23 Apr 2025), online: https://www.eff.org/deeplinks/2025/04/digital-identities-and-future-age-verification-europe.

[38] European Commission, "The EU approach to age verification", *Shaping Europe's Digital Future* (13 Oct 2025), online: https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification.

[39] Human Rights Watch, "Brazil Passes Landmark Law to Protect Children Online" (17 Sept 2025), online: https://www.hrw.org/news/2025/09/17/brazil-passes-landmark-law-to-protect-children-online.

[40] "Supreme Court suggests Aadhaar-based age verification to protect minors from inappropriate online content", *The Telegraph* (Kolkata, 28 Nov 2025), online: https://www.telegraphindia.com/entertainment/supreme-court-suggests-aadhaar-based-age-verification-to-protect-minors-from-inappropriate-online-content/cid/2135212.

CHAPTER 2
Understanding the Technological and Industry Landscape

By Michael Melamed

The policy push towards age verification systems aimed at protecting minors online has led to the emergence of several technological solutions and a growing industry focused on age verification and online safety technologies. As a general taxonomy, these techniques may include "age estimation", which refers to algorithmic guessing of age, based on behaviour, facial analysis through selfies, voice examination, or other signals, "age inference", which uses contextual clues such as a user's account or browsing history to assess age, and "age verification", which assesses documentary or biometric proof to demonstrate identity.[1]

The main proposed approaches focus on publisher-level age verification systems, A.I. and machine learning-based age-estimation, and device-level age verification.

1. Publisher-Level Age Verification

The publisher-level model envisioned in most legislative proposals makes internet publishers, whether they are websites or other forms of content hosts, legally obligated to age-verify all site visitors. In Bill S-209, for example, it is stated that "any organization making pornographic material available on the internet for commercial purposes has a responsibility to ensure that it is not accessed by young persons".[2] Most websites, even large platforms with vast technical capacity, typically rely on third-party vendors for age-verification. For example, Meta partners with specialized services such as Yoti for verification functions, although they also employ their own in-house A.I.-based age-estimation tools. In general, companies tend to prioritize low-cost and low-friction solutions, even though these may not always be the most appropriate or safest options for their users.

Third-party verification offers compliance advantages to platforms by way of shifting part of their responsibility for accuracy, security, and regulatory conformity onto specialized third-party entities. Some legislative proposals, including Bill S-209, have reinforced this trend through an express preference for arm's-length verification.

Privacy Considerations

The emergence of third-party age verification vendors has created an entirely new layer of private intermediaries whose primary business model is to collect and verify some of the most sensitive personal information that individuals can have. The novelty of this industry means that government IDs, drivers' licenses, and credit cards are entrusted to companies that may have a thin track record for

---

[1] Rindala Alajaji, "Age Verification, Estimation, Assurance — Oh My! A Guide to Terminology" (30 October 2025), online (blog): <eff.org/deeplinks/2025/10/age-verification-estimation-assurance-oh-my-guide-terminology>.

[2] Bill S-209, An Act to amend the Criminal Code (protection of children), 1st Sess, 45th Parl, Canada, 2025, pmbl (first reading), ["S-209"].

data protection or effective security. The use of these vendors creates a cryptic environment where "the average user won't know who is privy to their private information, how secure it is, or how it's stored" and that data breaches, when they take place, may be particularly harmful.[3] The uneven enforcement obligations placed on internet publishers, the substantial and continuous costs associated with outsourcing verification services, and the lack of industry best practices in a novel and largely untested sector are all areas of concern.

Third-party age verification vendors such as Yoti often pitch themselves as "privacy-first", describing their service as offering age checks "designed to only share the result of the age check … without collecting user data." They emphasize features like selfie-based age-estimation, stating that images are deleted instantly following checks, with device-based age tokens that only store the age check's outcome. However, there is still limited evidence proving that their service will not result in tracking or retention of user data, and investigations have identified gaps between Yoti's "privacy-first" branding and its practices from a data protection standpoint, finding that their website and app have engaged in non-consensual third-party tracking and device fingerprinting.[4]

Data Sovereignty and Jurisdictional Considerations

Age-verification systems frequently rely on third-party vendors operating trans-national businesses, therefore intensifying existing challenges of data sovereignty and jurisdictional concerns across Canada and abroad. In Canada, privacy officials are asserting digital sovereignty as "the most pressing policy and democratic issue of our time",[5] stressing that sensitive personal data must be "subject to Canadian law" rather than simply being stored domestically. However, enforcement remains difficult in practice, as data stored or processed by foreign-owned companies may be subject to extraterritorial access laws in other jurisdictions. Age-verification mandates, such as Bill S-209, therefore feed into an existing governance problem in which national privacy protections struggle to keep pace with globally distributed data infrastructures.

2. AI and Machine-Learning-Based Age-Estimation

Another developing solution is AI and machine-learning-based age-estimation, which estimates users' ages by mining their online behavioural data. Announcing that YouTube will be piloting AI age-estimation technologies in 2025, the company's director of product management for youth, James Beser, stated "this technology will allow us to infer a user's age and then use that signal, regardless of the birthday in the account, to deliver our age-appropriate product experiences and protections."[6] Although this option does not necessitate the transfer or collection of sensitive documentation, such as government IDs or credit cards, it nonetheless requires wholesale tracking of users' online behaviour in a manner which poses privacy concerns of its own. These technologies closely observe internet users and store

---

[3] Kevin Maimann, "'Can I see some ID?' As online age verification spreads, so do privacy concerns" (3 August 2025), online: <cbc.ca/news/online-safety-act-privacy-1.7598113>.

[4] Mint Secure, "Data protection and IT security issues with age verification app 'Yoti'" (5 June 2025), online: <mint-secure.de/dataprotection-it-security-risks-with-ageverificationapp-yoti>.

[5] Madison McLauchlan, "Canada hopes to build a sovereign cloud to counter US dominance. It won't be easy" (25 September 2025), online: <betakit.com/canadian-sovereign-cloud-evan-solomon-all-in/>.

[6] Blake Montgomery, "YouTube to gauge US users' ages with AI after UK and Australia add age checks" (30 July 2025), online: <theguardian.com/technology/2025/jul/30/youtube-google-ai-age-verification>.

individuals' behavioural profiles, raising concerns that such profiles may be exploited for advertising, training future AI models, predictive analytics, or in myriad other ways that users cannot foresee or control. Depending on behavioural data for age estimation presumes that users will constantly be logged into the platform-based tracking systems, expanding the companies' visibility into users' digital lives by continuously logging, storing, and analysing practically all user activity. This dynamic risks furthering large platforms' dominance as only they can have the extensive data ecosystems necessary for behavioural age-estimation.

3. Device-Level Age Verification

One final proposed technological model to highlight is age verification at the device level. These systems may involve authenticating a device at the point of purchase, thus programming it to prevent users' attempts to access mature content if they are underage.[7] Other efforts push for authentication to take place at the app-store level.[8] While largely uncharted, and with many unresolved questions, this technological method of age verification presents some practical advantages compared to other proposed solutions, such as through centralizing authentication, which reduces the burden of repeated identification. Age verification at the device-level has its own enforcement challenges, however, such as devices being shared between family members or the sale of devices by the original owner to third parties after the initial point of purchase.

4. Mapping Key Industry Players

Internet Publishers

Many of the larger internet publishers, including Meta and YouTube, have developed internal age-verification and age-estimation systems. Meta uses a self-created A.I.-based age-estimation tool, referred to as its "adult classifier", which evaluates account behaviour, follower lists, content interactions, and birthday posts to categorize users as older or younger than 18 years of age.[9] Meta has stated that if its A.I. calculations are incorrect, other options are offered to users. On Instagram, for example, Meta partners with third-party verification vendor Yoti to collect and verify government IDs of users seeking to modify their age within the app. Beyond the collection of IDs, Instagram has tested additional verification options, including video selfie collections and social vouching, where mutual followers above the age of 18 can "vouch" for a user's age.

YouTube is rolling out a similar system where the platform's internal A.I.-based age-estimation software operates as a first line of defence, with the goal being that this technological method works for the vast majority of users. Like Meta, YouTube appears to reserve the use of third-party ID collection for situations where its A.I. age-estimation system generates incorrect results or lacks confidence in estimating users' ages.

---

[7] Segpay, "User-Based Vs. Device-Based Age Verification: Protecting Minors Online" (17 October 2024), online (blog): <segpay.com/blog/user-device-age-verification/>.

[8] Dominic Preston, "Meta and Spotify are teaming up to lobby against Apple and Google" (1 May 2025), online: <theverge.com/news/659443/meta-spotify-match-garmin-lobby-group-apple-google-age-verification>.

[9] Andrew Hutchinson, "Meta's Developing an AI System To Detect Teens Lying About Their Age" (4 November 2024), online: <socialmediatoday.com/news/metas-developing-a-ai-system-to-detect-teens-lying-about-age/731917/>.

Smaller internet publishers, however, often do not have the option of treating third-party verification vendors as a fallback. Small-scale content publishers, such as fanfiction communities, independent creator pages, or niche blogs with occasional adult-themed material, do not have the capacity to build customized age-estimation software like Meta and YouTube, and instead will have to rely solely on third-party age verification vendors. Adult content is another industry where this is prevalent.[10]

Third-Party Age Verification Vendors

Some of the key players in the third-party vendor industry include Yoti, AgeChecked, Verifymy, and GBG. Yoti is one of the largest and most universally cited age verification vendors, working with high-profile platforms such as Instagram and OnlyFans. Comparatively, UK-based Verifymy and AgeChecked operate on a smaller scale.

These vendors offer a range of solutions to clients, including document scans and selfie matches, database checks, credit card authorizations, reusable digital age tokens, and AI tools to estimate users' ages. Due to Yoti's size and prominence in the industry, as well as existing partnerships with well-resourced companies like Meta and OnlyFans, it serves as an illustrative example of the types of products and services offered within the third-party verification vendor industry.

Yoti offers software which estimates users' ages from a selfie. The company's website describes this offering as "good for: people without ID documents, global coverage, and low friction".[11] Furthermore, like many of the other vendors, it offers ID-based verification where users may upload government identification such as passports or drivers' licenses and optionally link it to a "digital ID". The platform also offers reusable age tokens, whereby once a user completes an age check, Yoti issues a token that proves age compliance so they can be verified for future transactions without repeating the full verification process, so long as the token fulfils the publisher's criteria.

However, despite relatively widespread industry adoption, there have been both privacy and accuracy and fairness concerned raised about these products. The UK's Office of Communications stated, "age assurance technologies which scan your face and estimate your age don't work very well on children because children can look so different at different ages." Yoti responded to these concerns, by asserting that their "True Positive Rate for 13- to 17-year-olds correctly estimated as under the age of 21 is 99.3%."[12] There are significant limitations to this claim, however, as Yoti's threshold age of 21 as its benchmark is far higher than the age cutoffs contemplated in most age-verification proposals. While Yoti's research proves it can distinguish a 13-17-year-old from a 21-year-old, it does not address efficacy for users on the cusp of the legally relevant threshold, where accuracy is both most consequential and technically challenging.

Device Companies

As device-level age verification becomes an emerging proposed technological solution to the online child-protection issue, it brings a different group of stakeholders into focus. The main players at this level include major device manufacturers such as Apple, Microsoft, Google, Samsung, and other An-

---

[10] Yoti, "How OnlyFans became the first UK subscription-based platform to protect children and create age-appropriate experiences" (16 June 2023), online: <yoti.com/blog/how-onlyfans-became-the-first-uk-subscription-based-platform-to-protect-children-and-create-age-appropriate-experiences/>.

[11] Yoti, "Age estimation" (last visited 18 December 2025), online: <developers.yoti.com/age-verification/age-estimation>.

[12] Yoti, *Yoti Facial Age Estimation* (London: Yoti, 2025).

droid Original Equipment Manufacturers (OEMs). Proposals to authenticate age at the point of purchase, so that age verification status is tied to the device, would have significant impacts on device companies' operations. Other ideas, including authentication at the app-store level, would shift the burden to platform gatekeepers such as the Apple App Store and Google Play.

CHAPTER 3
Age Verification and Child Welfare

By Alyssa Laing

Concerns regarding children's media use are not a new phenomenon. Each time a new medium emerges, debates follow about distraction, exposure to inappropriate content, and the trade-offs around media as an educational tool.[1] Historically, these concerns are driven more in moral panic than in evidence, as the long-term impacts of media exposure on child development are a complex area to study.[2]

Digital platforms have attracted unprecedented levels of investment and research and development funding from both governments and powerful corporate actors, enabling far more extensive and sophisticated analysis into media's impacts on the public.[3] Consequently, modern concerns about young people's experiences in digital environments carry greater legitimacy than in earlier debates about media. Some scholarly research links excessive technology use to internet addiction, social withdrawal, obesity, anxiety, depression, and the risk of suicide at far greater rates compared to prior media forms.[4] However, much of the existing literature relies on correlational methods, resulting in incomplete and inconclusive evidence, which warrants a critical assessment of whether current anxieties about children's social media and pornography use represent genuinely new risks to youth or whether these concerns are simply a modern repetition of longstanding debates surrounding youth and media.[5]

---

[1] David Buckingham, *The Impact of the Media on Children and Young People with a particular focus on computer games and the internet* (University of London, Centre for the Study of Children, Youth and Media, Institute of Education, 2007); Ella Wartella, "A brief History of Children and Media Research" (25 January 2018), online (pdf): <nichd.nih.gov/sites/default/files/2018 03/WartellaHistChildMediaResearch.pdf> [perma.cc/JA5Y-AKKQ]; Gordon P. D. Ingram, *Adolescent Use of New Media and Internet Technologies: Debating Risks and Opportunities in the Digital Age* (New York, Routledge, 2023); Jane Ledingham, C. Anne Ledingham & John Richardson, *The Effects of Media Violence on Children,* for the National Clearinghouse on Family Violence (Ottawa, Health Canada, 1993).

[2] See E.g. Norma Pecora, John P Murray & Ellen A Wartella, *Children and Television: Fifty Years of Research* (New Jersey: Lawerence Erlbaum Associates, 2007).

[3] See generally Barbara Ortutay & Haleluya Hadero, "Social Media Companies Made $11 Billion in US Ad Revenue from Minors, Harvard Study Finds" (27 December 2023), online: <finance.yahoo.com/news/social-media-companies-made-11-190158239.html> [perma.cc/63QV-7H2X]; Pingler, "How Much Does R&D for Social Media Cost?" (28 April 2023), online:<pingler.com/blog/how-much-does-rd-for-social-media-cost-lets-calculate-it-now-to-avoid-overpayments/> [perma.cc/N8ZM-TP8P]; Amanda Raffoul et al., "Social Media Platforms Generate Billions of Dollars in Revenue from U.S. Youth: Findings from a Simulated Revenue Model" (2023) 18:12 PLoS One 1.

[4] See e.g. Jean M. Twenge, "Increases in Depression, Self-Harm, and Suicide Among U.S. Adolescents After 2012 and Links to Technology Use: Possible Mechanisms" (2020) 2:1 Psychiatric Research & Clinical Practice.

[5] See e.g. P. D. Ingram, *supra* note 1.

1. Youth and Social Media

Governments worldwide have documented a range of concerns and harms related to social media use among young people.[6] For example, the Australian Government reported that social media exposes children to harmful content such as the promotion of unhealthy lifestyles, sextortion, scams, self-harm behaviours, discrimination and hate speech while also negatively affecting their well-being and social cohesion.[7] Young people face an increasing risk of developing a range of physical and psychological health issues associated with excessive social media use, including obesity, musculoskeletal and motor disorders, anxiety, attention-deficit/hyperactivity disorder, insomnia, and depression, according to studies conducted by the United Kingdom and Canadian governments.[8]

Beyond the catalogue of direct harms of social media use on young people, research also highlights how they can extend deeply into family life. Parental testimony commonly reveals a profound sense of grief, guilt, and regret in the aftermath of traumatic events or tragedies linked to their children's social media use.[9] Beyond the immediate sadness, impacted parents may blame themselves for failing to impose stricter controls on their children's social media use and express painful recognition that their lives—and those of their children—have been irrevocably altered.[10]

Many governments are understandably taking a risk-focused approach, such as prohibiting social media use for youths under the age of 16.[11] Research suggests that social media has fuelled the demand for early smartphone use, which correlates with children having access to these platforms at increasingly younger ages.[12] Earlier access can heighten the risk of harm, and research suggests that the age of ac-

---

[6] See Joint Select Committee on Social Media and Australian Society, *Social Media: The Good, The Bad, and The Ugly*, for the Parliament of Australia (Canberra, Senate Printing Unit, 2024); Public Health Agency of Canada, *Mental Health and Problematic Social Media Use in Canadian Adolescents: Findings from the 2018 Health Behaviour of School-aged Children (HBSC) Study* (Ottawa, Public Health Agency of Canada, 2022) [PHAC "Problematic Social Media"]; Public Health Agency of Canada, *Connections and Relationships in Canadian Adolescents Findings from the 2018 Health Behaviour in School-aged Children (HBSC) Study* (Ottawa, Public Health Agency of Canada, 2022) [PHAC "Connections and Relationships"]; House of Commons, Science and Technology Committee, *Impact Of Social Media And Screen-Use on Young People's Health* for the United Kingdom Parliament (London, Parliamentary Copyright House of Commons, 2019); *Online Safety Act,* (UK), 2023; The U.S Surgeon General's Advisory, "Social Media and Youth Mental Health" (2023), online(pdf): <hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf> [perma.cc/ FNX5-6WCF].

[7] Joint Select Committee on Social Media and Australian Society, *supra* note 6.

[8] See e.g. *Ibid;* Saray Ramirez et al, "Use of Technology and Its Association with Academic Performance and Life Satisfaction Among Children and Adolescents" (2021) 12:764054 J Front. Psychiatry 1; PHAC "Problematic Social Media", *supra* note 6; House of Commons, *supra* note 6.

[9] Joint Select Committee on Social Media and Australian Society, *supra* note 6.

[10] *Ibid.*

[11] See The Associated Press, "Malaysia To Ban Social Media For Children Under 16 Next Year", *CTV News* (24 November 2025), online: < ctvnews.ca/world/article/malaysia-to-ban-social-media-for-children-under-16-next-year/> [perma.cc/ 5CWA-6BXE]: Jamey Keaten, "Another Country Agrees To Ban Social Media For Children Under 15", *Independent* (8 November 2025), online: <independent.co.uk/news/world/europe/denmark-social-media-ban-under-16-australia-b2861303.html> [perma.cc/ 7C8F-SE78]; Ministry of Children and Families, Ministry of Digitalisation and Public Governance, Office of the Prime Minister, News Release, "Norway Moves Forward with Age Limit for Social Media" (6 November 2025), online: < regjeringen.no/en/whats-new/norway-moves-forward-with-age-limit-for-social-media/id3108682/> [perma.cc/ 9AH3-YF6U].

[12] Tara Thiagarajan, Jennifer Newson & Shailender Swaminathan, "Protecting the Developing Mind in a Digital Age: A Global Policy Imperative" (2025) 23:3 J Human Development & Capabilities 493; Amen Clinics, "What Happens When Kids Get Smartphones Too Early?" (11 November 2025), online: <instagram.com/p/DQ7uQHmEjua/?igsh=NnRlMWM-3d2txbHl2&img_index=1> [perma.cc/ 74YL-ZY3Z]; Jonathan Haidt, *"The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness"* (New York, Penguin Publishing Group, 2024).

cess will continue to decrease over time if unregulated.[13] In view of both the current risks that social media poses to children and their families and the foreseeability of an increased likelihood of future harm, a push towards preventative measures is understandable.

On the other hand, in assessing the appropriate regulatory posture legislators must weigh preventative measures against the beneficial impacts of these technologies, which many government investigations fail to engage with.[14] Academics have highlighted that social media helps foster social support and connections, enables self-expression and creativity, improves access to information, encourages help-seeking behaviours, and supports mental-health self-reporting.[15] Research indicates that social media is particularly significant in the lives of marginalized, vulnerable, or socially diverse communities, providing them with meaningful spaces for identity exploration, community building, and social support that may be less accessible offline.[16] For example, First Nations youth emphasize the role of social media in supporting community self-determination and rekindling kinship ties disrupted by colonization.[17] Refugee youth have highlighted social media as a means to address complex mental health challenges, share lived experiences of forced migration and assist in environmental adaptation.[18] Moreover, for LGBTQIA+ youth, social media offers access to safe spaces to explore identity and orientation while providing support to navigate and mitigate physical and emotional safety risks.[19] Although marginalized youth are not immune to the general dangers of social media and may even face heightened exposure to specific harms, their greater potential to experience meaningful benefits cannot be overlooked.[20]

Regulatory approaches which seek to block access to social media, without having built-in ameliorating mechanisms, risk serving the best interests of some children at the expense of other marginalized groups, reinforcing existing structural inequalities and harming marginalized youth who need governmental protection the most.[21]

---

[13] See e.g. *Ibid*; Jonah David, "Wired for Worry: How smartphones and social media are harming Canadian Youth" (April 2025), online (pdf): < macdonaldlaurier.ca/wp-content/uploads/2025/04/20250319_Smartphones_social-media-Davids_PAPER-v4-FINAL.pdf> [perma.cc/ PP45-FAK7].

[14] The reports by the Canadian and Australian governments detailing social media's harmful impacts on youth, which grounded the pursuit of preventative measures in these jurisdictions, included no discussion of beneficial impacts; see *supra,* note 6.

[15] See e.g. House of Commons, *supra* note 6; PHAC, "Connections and Relationships", *supra* note 6; U.S Surgeon General's Advisory, *supra* note 6; Joint Select Committee on Social Media and Australian Society, *supra* note 6.

[16] Joint Select Committee on Social Media and Australian Society, *supra* note 6; U.S Surgeon General's Advisory, *supra* note 6; Zahra M Clayborne et al, "Associations between social media use and positive mental health among adolescents: Findings from the Canadian Health Behaviour in School-aged Children Study" (2025) 1:181 J Psychiatric Research; Carolina Are, Catherine Talbot & Pam Briggs, "Social Media Affordances of LGBTQIA+ Expression and Community Formation" (2024) 31:4 Sage J 1401.

[17] Joint Select Committee on Social Media and Australian Society, *supra* note 6.

[18] *Ibid.*

[19] *Ibid.*

[20] See e.g. Celia Fisher, Xiangyu Tao & Madeline Ford, "Social Media: A Double-Edged Sword for LGBTQ+ Youth" (2024) 156:108194 J Computers in Human Behavior.

[21] See generally Daniel J Hemel, "The Equality–Equity Dilemma in Cost–Benefit Analysis: Comment on Daniel Farber's Inequality and Regulation: Designing Rules to Address Race, Poverty, and Environmental Justice" (2023) 3:1 American JL and Equity.

2. Youth and Pornography

An analogous discourse exists with respect to the debates surrounding the impacts of pornography use on youth.[22] Proponents of online age verification understandably raise concerns due to the growing body of research that associates pornography consumption with several adverse outcomes, including heightened male aggressiveness, the objectification of women, distorted understandings of intimacy, unrealistic body image expectations, and an increased risk of sexual violence against women.[23] Moreover, and as with social media, children are exposed to pornography at increasingly younger ages.[24]

Studies estimate that the average age of first exposure to pornography is between 11 and 12 years old.[25] However, some researchers claim that in reality, children as young as eight years old can easily access pornography through various internet platforms, including dedicated pornography websites and social media sites such as X and Instagram, widening the likelihood of children experiencing these adverse effects.[26] In light of the effects in combination with the increasing availability of accessing pornography, governments have emphasized the urgency of implementing regulatory measures.[27]

However, despite the legitimacy of these concerns, research on youth exposure to pornography suffers from the same methodological limitation that characterizes studies on social media: it is correlational in nature.[28] As a result, directly ascribing these adverse effects to a particular source is inherently challenging due to the long-term and cumulative nature of these developmental impacts, as well as the vast array of media capable of shaping children's attitudes and perceptions in society. For example, studies have shown that "manosphere" influencers like Andrew Tate contribute to many of the same adverse effects as pornography.[29] These influencers, whose primary audience consists of young men and adolescents, have been widely associated with the promotion of overtly hateful and misogynistic ideolo-

---

[22] See e.g. Children's Commissioner, "A Lot of It Is Actually Just Abuse: Young People and Pornography" (31 January 2023), online(pdf): < childrenscommissioner.gov.uk/resource/a-lot-of-it-is-actually-just-abuse-young-people-and-pornography/> [perma.cc/ 545Y-KGL3].

[23] See e.g. Children's Commissioner, *supra* note 22; Recovery Alberta: Mental Health and Addiction Services, "Fact Sheet: Child & Youth Problematic Online Pornography" (last modified June 2025), online(pdf): <albertahealthservices.ca/assets/info/amh/if-amh-ydt-fact-sheet-child-and-youth-problematic-online-pornography.pdf> [perma.cc/ MS57-3NAM]; American College of Pediatricians, "The Impact of Pornography on Children" (May 2024), online(pdf): <acpeds.org/the-impact-of-pornography-on-children/> [perma.cc/ XGE4-YVX3]; Luca Cerniglia & Silvia Cimino, "Pornography Consumption in Pre-/Early Adolescents: A Study on the Links with Emotion Regulation and Internalizing/Externalizing Symptoms" (2024) 43:34 Current Psychology; UNICEF, "Protection of children from the harmful impacts of pornography: Pornographic content can harm children" (last accessed 16 December 2025), online: < unicef.org/harmful-content-online> [perma.cc/ 63AF-44JY].

[24] Children's Commissioner, *supra* note 22; Recovery Alberta: Mental Health and Addiction Services, *supra* note 23; Philipa Wain, "Children's commissioner: Pornography affecting 8-year-olds' behaviour", *BBC* (9 May 2023), online: <bbc.com/news/technology-65534354> [perma.cc/ 9XMG-7L93].

[25] See *Ibid.*

[26] *Ibid;* Canadian Centre for Child Protection Inc, "Exposure to Sexually Explicit Material" (last accessed 16 December 2025), online: <protectkidsonline.ca/app/en/helpful_information_exposure_to_sexually_explicit_material#:~:text=The%20reality%20is%20that%20children,and%20teens%20who%20view%20it> [perma.cc/ 56YJ-SPMH].

[27] See e.g. *Online Safety Act, supra* note 6; Bill S-209, *An Act to Restrict Young Persons' Online Access to Pornographic Material,* 1st Sess, 45 Parl, 2025.

[28] See e.g. P.D. Ingram, *supra* note 1.

[29] See Jochen Peter & Patti M Valkenburg, "Adolescents' Exposure to a Sexualized Media Environment and Their Notions of Women as Sex Objects" (2007) 56:381 J Sex Roles 381; Craig Haslop et al., "Mainstreaming the Manosphere's Misogyny Through Affective Homosocial Currencies: Exploring How Teen Boys Navigate the Andrew Tate Effect" (2024) 1:11 J Social Media & Society 1.

gies that commodify and frame women as property, emphasize that men adopt traditional gender roles in their relationships and homelives, and that it is a male's duty to preserve hegemonic masculinity.[30]

This underscores an even more complex issue underpinning the online age verification debate which is that many of these effects are not necessarily attributed to the media itself, but rather to the emergence of broader anti-feminism and male nationalist movements, and other cultural phenomena supported by societal institutions and prominent corporate actors in the digital information economy.[31] It is, therefore, unsurprising that researchers have stressed how many of these adverse effects are highly gendered and relate to heteronormative ideals.[32]

3. The Need for Nuance

As with social media, the effects of pornography are not universal, but rather somewhat dependent on one's positionality. Regulators should be mindful of the differential impacts that exposure to pornographic content may have across different groups.

The LGBTQIA+ community represents a potent example. Researchers have suggested that LGBTQIA+ youth are not as susceptible as heteronormative youth to specific adverse effects from pornography use.[33] Instead, on balance, pornography use appears to be more beneficial to the community than it is harmful.[34] Studies have highlighted that the limited accessibility of educational sexual health, particularly in the LGBTQIA+ context, has correlated with LGBTQIA+ youth relying more on pornography to learn about sexual activities and to explore and develop their sexual identities.[35] Sexual health education is not only limited in the LGBTQIA+ context, but also remains generally constrained due to stigma and privacy norms. For this reason, researchers suggest that pornography often fills the gaps that schools and homes fail to address, not only for LGBTQIA+ youth, but for all children.[36]

Similarly, there is growing evidence that a youth's age is also an essential factor in how they experience

---

[30] Craig Haslop, *supra* note 29.

[31] See generally Standing Committee on Health, "Report on The Public Health Effects of The Ease of Access and Viewing of Online Violent and Degrading Sexually Explicit Material on Children, Women and Men", for the Canadian Parliament, online (pdf):<ourcommons.ca/Content/Committee/421/HESA/Reports/RP9027245/hesarp11/hesarp11-e.pdf> [perma.cc/ CV8H-8AN4].

[32] See generally Chunyan et al., "Pornography Use and Perceived Gender Norms Among Young Adolescents in Urban Poor Environments: A Cross-site Study" (2021) 69:1 J Adolescent Health 31; Beáta Bóthe et al., "Problematic and Non-Problematic Pornography Use Among LGBTQ Adolescents: a Systematic Literature Review" (2019) 6:1 Current Addiction Reports 478; Isabelle Flory & Eran Shor, " Porn is Blunt [...] I Had Way More LGBTQ+ Friendly Education Through Porn": The Experiences of LGBTQ+ Individuals with Online Pornography" (2025) 28:4 J of Sexualities 1506; Claire Meehan, "Watching Porn, (Un)Doing Gender? Young People's Experiences and Understandings of Online Porn" (2025) 54:2 Archives Sexual Behavior 721.

[33] See e.g. Isabelle Flory & Eran Shor, *supra* note 32.

[34] *Ibid.*

[35] See e.g. Anonymous Author, "Letter In Strong Opposition of Bill S-210", online(pdf): <ourcommons.ca/Content/Committee/441/SECU/Brief/> [perma.cc/ W732-3C9Q]; British Columbia Civil Liberties, "Submissions to the House of Commons Standing Committee on Public Safety and National Security regarding Bill S-210, An Act to restrict young persons' online access to sexually explicit material" (31 May 2024), online(pdf): <ourcommons.ca/Committees/en/SECU/> [perma.cc/ UXF4-T77N]; Isabelle Flory & Eran Shor, *supra* note 32; Beáta Bóthe et al, *supra* note 32.

[36] Isabelle Flory & Eran Shor, *supra* note 32.

pornography.[37] By the age of 16, most teens have begun to develop adult-like cognitive abilities, whereas said ability is typically absent for those under the age of 15.[38] Accordingly, studies suggest that teens, as opposed to younger youth, can not only critically engage with pornography but also can distinguish fantasy from reality, self-regulate, and therefore are more likely to benefit from access to pornography and be less vulnerable to the adverse effects.[39]

Beyond the need to account for youths' intersectional identities, effective policymaking must consider how pornography typology shapes how young people interact with and experience it. Researchers have suggested that more "extreme" or "hardcore" pornographic content is intrinsically more harmful to youth than so-called "soft pornography".[40] Although bright-line distinctions among these categories are difficult to draw, the latter forms of content are generally not associated with increased aggression, measurable changes in individual attitudes, or other direct harms to youth, and more likely to play a positive or educational role in sexual development.[41] This nuance is reflected in the Parliament of Canada's Standing Committee on Health report on the *"Public Health Effects of the Ease of Access and Viewing of Online Violent and Degrading Sexually Explicit Material on Children, Women and Men",* in the decision of *R v Butler,* and even more recently in Canadian Parliamentary debates around Bill S-209.[42]

Despite these findings, nuanced consideration of pornography typology is not meaningfully reflected in ongoing age verification debates, which tend to conflate virtually all sexual content. This is at least partially the result of pornography itself being poorly-defined.[43] Academics have long grappled with the complexity of defining, categorizing, and distinguishing pornography which may be harmful from forms which are beneficial or benign.[44] Trying to achieve this nuance from a regulatory perspective is challenging, especially when considering how the above intersectional factors must also be incorporated, alongside other relevant factors such as user frequency, when findings are divided and unclear.[45]

While regulating youth access to online pornography is an inherently complex undertaking, the dominant regulatory approach of prohibiting pornography until the age of 18 is overly broad and fails to meaningfully engage with the spectrum of factors that shape young people's experiences, despite there

---

[37] See e.g. Giselle Woodley et al., "Critical young consumers: what types of porn do teens watch, and why?" (2025) Media Intl Australia 1.

[38] Alberta Health, "Cognitive Development, Ages 15 to 18 Years" (last accessed 12 December 2025), online: <myhealth.alberta.ca/Health/Pages/conditions.aspx?hwid=te7285&lang=en-ca#te7285-sec> [perma.cc/ UU5S-XJCF].

[39] See Giselle Woodley et al., *supra* note 37; Paul Bryon et al., "Reading for Realness: Porn Literacies, Digital Media, and Young People" (2021) 25:1 Sexuality & Culture 786.

[40] Giselle Woodley et al., *supra* note 37.

[41] See e.g. *Ibid.*

[42] Standing Committee on Health, *supra* note 31; *R v Butler,* 1992 CanLII 124 (SCC); "Bill S-209, An Act to restrict young persons' online access to pornographic material", 2nd reading, *Debates of the Senate,* 1-154, No 5 (3 June 2025) at 1648 (Hon Julie Miville-Dechêne); "Bill S-209, An Act to restrict young persons' online access to pornographic material", 2nd reading, Debates of the Senate , 1-154, No 5 (10 June 2025) at 1602 (Hon Yonah Martin).

[43] Giselle Woodley et al, *supra* note 37; Alan Mckee et al., *"What Do We Know About the Effects of Pornography After Fifty Years of Academic Research?"* (Abingdon, Oxon: Routledge, 2022).

[44] *Ibid.*

[45] *CF* Hamida Mubasshera, "Pornography Usage During adolescence: Does it Lead to Risky Sexual Behavior?" (2022) 33:1682 J Health Econs 1682; Andrew Przybylski & Netta Weinstein, "A Large-Scale Test of the Goldilocks Hypothesis: Quantifying the Relations Between Digital-Screen Use and the Mental Well-Being of Adolescents" (2017) 28:2 Psychological Science 204; Marie- Ève et al., "When Pornography Use Feels Out of Control: The Moderation Effect of Relationship and Sexual Satisfaction" (2018) 44:4 J Sex & Marital Therapy 343.

being potential to do so.[46] Taking such an approach risks oversimplifying a multifaceted issue, and failing to properly engage with the complex trade-offs that prohibitions present for children, families, and our digital society. To effectively balance the harmful risks of pornography exposure against its potential benefits, regulators should design a more nuanced, evidence-informed online age verification framework or seek alternative regulatory measures, as proponents on both sides of the online age verification debate have raised legitimate justifications for their positions.

4. Lessons for Regulators

Growing public concern about youth exposure to harmful digital content online makes it reasonable for lawmakers to explore protections. However, the research into this area suggests a need to be wary of overly simplistic solutions. Social media use may be associated with both harms and benefits, including heavily differential impacts based on both the identity of the user and the nature of the use. Generally speaking, pornography use is correlated with harms in youth. However, a deeper review of the research appears to suggest that attributing a causal link between youth pornography use and harm is overbroad. Many youth navigate sexual content without measurable negative outcomes, and some – especially within the LGBTQIA+ community – report benefits from access to identity-affirming or educational resources.[47] An appropriately nuanced perspective recognizes that outcomes are heavily impacted by multiple factors, such as access to educational sexual health resources, cognitive development, and pornography typology.[48]

Mandatory age verification does not address this complexity. It does not improve the quality or availability of sexual-health information, reduce algorithmic amplification of misogyny, or strengthen support services, nor does it address fundamental social problems which are contributing to depression, anxiety, suicidal ideation, or the lack of treatment options to address these conditions as they arise. Most regulatory approaches fail to account for the variation in impact across the wide range of online content and the progression of cognitive development throughout teenage years. Instead, age verification collapses a multi-factor social problem into a single access-control mechanism. It treats youth experiences as a monolith and offers a deceptively simple narrative: verify age, block minors, solve harm. The reality of the complex issue at hand calls for a more nuanced approach.

Governments seeking to promote healthy child development should consider measures that are flexible, incremental, and capable of capturing the differential impacts of both digital technologies as a whole and adult content specifically on young people. One such measure that fulfils these elements and that has also been recommended by researchers is implementing a comprehensive sexual health curriculum in schools, which includes education about pornography, its impacts, and the ways that it can be both beneficial and harmful.[49] Such measures reflect a harm reductionist approach while still addressing the concerns of social media and pornography exposure.

Studies on the impact of educational interventions have emphasized that heterosexual and marginalized youth experienced beneficial outcomes in relation to their behavioural and attitudinal changes,

---

[46] *Supra* note 27.

[47] Beáta Bőthe et al, "Problematic and Non-Problematic Pornography Use Among LGBTQ Adolescents: a Systematic Literature Review" (2019), online: https://saillab.ca/wp-content/uploads/2020/08/Bothe2019_Article_ProblematicAndNon-ProblematicP.pdf

[48] *Supra* note 45.

[49] Standing Committee on Health, *supra* note 31 at 8-9.

media knowledge, and media criticism, and that it was found to be an effective way to mitigate risky behaviours.[50] For example, there is strong evidence that this curriculum changed perceptions that girls like to be called derogatory names, and the perception that it is sexy when girls cry, vomit or get choked during sex was substantially reduced, a specific concern emphasized in the UK Commissioners' Report on Youth and Pornography.[51] By equipping youth with critical analysis tools, not only is children's agency being respected, but it has also been shown that it persuaded pornography-naïve youth from seeking out harmful content.[52]

A recent study on the status of sexual health education across Canada has identified that pornography literacy, and in particular digital pornography curriculum, has not been adequately implemented across Canada.[53] Expanding sexual health education also broadly aligns with the UN's Sustainable Development Goals, a set of guiding principles adopted by all United Nations members in 2015.[54]

A similar case can be made for nuanced solutions to harms flowing from social media use. While banning users below a particular age threshold fails to account for the differential, and sometimes beneficial, uses of these technologies, there are a range of architectural, technological, and design-based solutions which are available to target the specific harms more directly. A recent study by Sandra Cortesi and Urs Gasser argues for a design-centric approach to child safety, which emphasizes fostering trust, creating accessible pathways for help-seeking, and embedded guardrails to support autonomy, education, and participation.[55]

Given the complexity of child development, what is needed above all is further study, to avoid prematurely legislating in a space that remains largely unknown. By adopting calibrated, evidence-based approaches, regulators are still addressing legitimate concerns surrounding youth and online content; however, they are doing so in a manner that equally supports the health of the next generation, irrespective of background.

More adaptive measures, such as comprehensive education and design interventions, better align with the multifaceted nature of the issue and the variability of youth experiences. These approaches do not foreclose future intervention, but instead prioritize evidence-based harm reduction while the research landscape continues to evolve. A cautious approach is particularly vital given the potential trade-offs to privacy and freedom of expression inherent in age verification, as explored in the following chapters.

---

[50] Emily Rothman et al., "A Pornography Literacy Class for Youth: Results of a Feasibility and Efficacy Pilot Study" (2018) 13:1 Am J Sexuality Education 1.

[51] Children's Commissioner, *supra* note 22.

[52] Rothman et al., *supra* note 50.

[53] Action Canada for Sexual Health & Rights, *"The State of Sex-Ed in Canada"* (2 April 2020), online(pdf): <actioncanadashr.org/sites/default/files/2019-09/Action%20Canada_StateofSexEd_F%20-%20web%20version%20EN.pdf> [perma.cc/ C678-ZMDM]; UNESCO, "Comprehensive sexuality education: For Healthy, Informed and Empowered Learners" (last accessed 9 December 2025), online: <unesco.org/en/health-education/cse> [perma.cc/4XER-HN9P].

[54] Government of Canada, "Canada and the Sustainable Development Goals" (4 November 2025), online: <canada.ca/en/employment-social-development/programs/agenda-2030.html> [perma.cc/ 2VR5-JP4W].

[55] Sandra Cortesi & Urs Gasser, "Digital child safety at the frontier: From evidence to action" (2026) 392:6793 Science 30, online: <https://www.science.org/eprint/NEMPXBIZKZKUKNQVVHPM/full?activationRedirect=/doi/full/10.1126/science.aec7804>.

CHAPTER 4
Age Verification and Privacy

By Matthew Brennan, Finn Mitra, and Graham Muise

Online surveillance has evolved into a ubiquitous aspect of our digital lives. This is mainly the result of the dominant role that the trade in personally identifiable information (PII) plays in the digital economy, though governments have also capitalized on this trend to develop their own mass surveillance networks.[1] While the pervasive nature of modern surveillance has reshaped public understanding of privacy, breaches of the right to privacy can still have catastrophic consequences for their victims.[2]

Recent years have seen a rash of high-profile data breaches of apparently secure systems, such as the credit monitoring service provider Equifax, whose 2017 breach compromised sensitive financial information of 145.5 million Americans.[3] Verification systems can provide a particularly harmful vector of attack. In July 2025, the Tea Dating Advice application (Tea) suffered a catastrophic breach which disclosed the identities of tens of thousands of its users.[4] Tea, which was meant to provide a secure forum for women to anonymously share information about men they were dating or interested in, including potential red flags related to abusive behaviour, collected photos and drivers' licenses to legitimize claims made on the application and enhance the safety of users. The breach led to serious concerns of physical harm among many of the app's users, who had used the system to discuss abusive experiences with former intimate partners.

The Tea breach is a good example of how the damage of privacy violations can move beyond financial harms and impact people's dignity, personal freedom, and safety.[5] A victim may have feelings of fear, anxiety, or embarrassment following the release of their sensitive information.[6] This is an internalized and behavioural harm, where the victim may be more cautious to share information online in the future, and chilled from expressing themselves as a result.[7] Victims may be inhibited from future, productive uses of the internet, such as participation in age verification schemes, or other legitimate

---

[1] Michael Karanicolas, "Travel Guide to the Digital World: Surveillance and International Standards" (2014) Global Partners Digital at 18. <https://www.gp-digital.org/wp-content/uploads/2014/08/Travel-Guide-to-the-Digital-World-Surveillanvce-and-International-Standards-1.pdf> [Karanicolas]

[2] Eric Durnell et al, "Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale" (2020) 36:19 Intl J Human-Computer Interaction at 1834. <https://doi.org/10.1080/10447318.2020.1794626> [Durnell et al]

[3] Tyler Moore, "On the harms arising from the Equifax data breach of 2017" (2017) 19 Intl J Critical Infrastructure Protection at 47. <https://doi.org/10.1016/j.ijcip.2017.10.004> [Moore]

[4] Steven M Bellovin, "Privacy-Preserving Age Verification—and Its Limitations" (2025) IAB/W3C Workshop on Age-Based Restrictions on Content Access at 6. <https://www.cs.columbia.edu/~smb/papers/age-verify.pdf> [Bellovin].

[5] Aggeliki Tsohou & Thanos Papaioannou, "Impacts of Information Privacy Violations" in Sushil Jajodia, Pierangela Samarati & Moti Yung, eds, Encyclopedia of Cryptography, Security and Privacy (Berlin: Springer, 2021) at 1. <https://doi.org/s10.1007/978-3-642-27739-9_1614-1> [Tsohou & Papaioannou].

[6] Suvineetha Herath, Haywood Gelman, & Lisa McKee, "Privacy Harm and Non-Compliance from a Legal Perspective" (2023) 2023:2 J Cybersecurity Education, Research & Practice at 3. <https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/3/?utm_source=digitalcommons.kennesaw.edu%2Fjcerp%2Fvol2023%2Fiss2%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages> [Herath, Gelman & McKee].

[7] Philipp K Masur & Sabine Trepte, "Transformative or Not? How Privacy Violation Experiences Influence Online Privacy Concerns and Online Information Disclosure" (2021) 47:1 Human Communication Research at 53. <https://doi.org/10.1093/hcr/hqaa012> [Masur & Trepte].

requests for PII.[8]

The level of harm that results from a breach is heavily dependent on the nature of the data collected.[9] Location information, for example, plays a legitimate role in most age verification systems by determining the appropriate age restrictions that apply within their jurisdiction. However, location data can also be used to pinpoint users in the real world. Data associated with age verification systems may include not just information directly inputted into the website to establish a person's age,[10] but also other ancillary interactions with the age verification technology or system, like a digital footprint left at the age-gated website,[11] as well as other contextual information about a user, such as device type or location.[12]

The sensitive nature of age verification data makes it a high-value commodity, as well as a target for cyber criminals, or even state actors interested in finding compromising information about potential targets.[13] The data collected through digital surveillance can pinpoint users at a specific site, often an adult site, during the age verification process.[14] Then, that information can be connected to a larger user profile containing other private data.[15]

Even in the absence of a data breach, the spread of age verification raises novel risks due to the potential to normalize invasive data collection and surveillance of internet users.[16] Increased complacency towards online identification checks creates an avenue for bad actors to imitate reputable websites and solicit users' identifying information.[17] Such phishing schemes, whereby a fraudulent website prompts individuals to disclose sensitive information, can compromise user privacy even in the absence of any technical security breach.

Together, these concerns demonstrate the importance of moving cautiously and intentionally with regards to age verification, and ensuring that proposed solutions meet appropriate standards of privacy, safety, security and integrity. The following sections briefly discuss the current state of age verification systems, including appropriate privacy concerns related to the different age verification models which have been deployed.

---

[8] Masur & Trepte, *Ibid.*

[9] Tsohou & Papaioannou, *supra* note 5.

[10] Tsohou & Papaioannou, *Ibid.*

[11] Tsohou & Papaioannou *Ibid.*

[12] Tsohou & Papaioannou *Ibid.*

[13] Yinhao Jiang et al, "Pervasive User Data Collection from Cyberspace: Privacy Concerns and Countermeasures" (2024) 8:5 Cryptography at 5 & 13. <https://doi.org/10.3390/cryptography8010005> [Jiang et al]

[14] Bellovin, *supra* note 4.

[15] Anri Nishnianidze, "Surveillance in the Digital Age" (2024) 20:37 European Scientific J at 16. <https://doi.org/10.19044/esj.2024.v20n37p1> [Nishnianidze].

[16] Jonas Lund-Tønnesen & Karin Fossheim, "Excessive Digital Surveillance and Data Privacy Invasion as a Creeping Crisis" (2025) 16:1 Risk, Hazards & Crisis in Public Policy at 7. <https://doi.org/10.1002/rhc3.70005> [Lund-Tønnesen & Fossheim].

[17] Murray, Alana, Huma Chhipa & Johnathan Yerby, "Cyber risk, privacy, and the legal complexities of age verification for adult content platforms" (2025) 26:4 IIS at 338, online: <https://iacis.org/iis/2025/4_iis_2025_332-347.pdf>.

1. Digital Age Verification Methods

Traditionally, governments and private entities restricted minors' access to age-inappropriate goods and services through the use of manual ID checks, in which a designated agent confirmed the age of an individual by assessing their appearance against a piece of identification which included their date-of-birth. Manual ID checks have never been perfect, and determined youths have always managed to find various workarounds to access alcohol or other age-gated goods, but the use of government identification remains the preferred method for verifying age in a variety of physical contexts, from tobacco stores to bars to adult entertainment venues.

However, translating age verification to the online environment introduces fundamental challenges that do not exist in physical spaces. Most obviously, manual ID checks are generally a transient process. When a person shows their ID at a bar, the bouncer or bartender does not retain any record of the sensitive personal information featured on the IDs, they merely make a mental note that the person is of appropriate age and move on. By contrast, digital age verification necessarily requires the creation, transmission, and at least temporary storage of electronic records of sensitive personal information. These methods present different risk profiles depending on the types of information collected and their relative vulnerability to attack, but the nature of digital communications means there is no way to avoid them entirely.[18] The most common age verification methods are through self-declaration, identification, biometrics, and behavioural analysis.[19]

Self-Declarations

The least invasive – and least effective – method of ascertaining an internet user's age is through a self-declaration. Users typically click a button confirming they are 18 or older, or manually enter a date of birth, without any subsequent verification of the information provided. While this process collects little sensitive information, it effectively relies on the honour system to root out underage users, and is therefore easily circumvented by users, including minors, who may input false information.[20]

Most legislative frameworks seeking to protect minors online have moved beyond self-declaration toward more robust verification methods, though each comes with its own set of privacy and security trade-offs.

Identification Verification

Digital Identification verification requires users to upload government-issued IDs, such as a driver's license or passport, or a credit card, for review in order to determine their age. In some cases, a real-time picture is taken and compared to a photo ID to evaluate if the user is the same person on the ID.

For years, many people have been sceptical of inputting credit card information into adult websites,

---

[18] Shete, Navnath Lahu, Manisha Maddel & Zarina Shaikh, *A Comparative Analysis of Cybersecurity Scams: Unveiling the Evolution from Past to Present* (2024).

[19] Murray, Alana, Huma Chhipa & Johnathan Yerby, "Cyber risk, privacy, and the legal complexities of age verification for adult content platforms" (2025) 26:4 IIS, online: <https://iacis.org/iis/2025/4_iis_2025_332-347.pdf>; Emrah Diler, "Age verification in a digital world" (2022), online: Fraud.com <https://www.fraud.com/post/age-verification-in-a-digital-world>.

[20] Christine Marsden, "Age-Verification Laws in the Era of Digital Privacy" (2020) 10:2 National Security LJ 210 at 226-228.

and for understandable reasons.[21] If the website experienced a data breach, both privacy and financial security could be jeopardized. Phishing, the online scamming method of pretending to be a legitimate actor to get targets to give up valuable personal information, has been a threat on the internet for decades,[22] and has improved in sophistication as technology develops.[23] As the number of minors with access to credit cards has significantly increased, credit cards have also become correspondingly less reliable as a marker of whether a person is over 18.[24] The use of credit cards as a proxy for age verification also necessarily excludes people who do not have credit cards, for example because they lack a sufficiently strong credit history.

Uploading a scanned photo ID is fundamentally riskier than having your age verified via a credit card, since it opens the door to additional forms of identity theft if a breach occurs. While some legal frameworks, such as Canada's S-209, mandate that identification data is to be deleted upon verification, there are nonetheless opportunities for interception in transit, or as a result of other security failures. In situations where an ID and a picture are required, either dataset being breached could implicate the other, and a greater amount of your digital and physical likeness would be available for potential use in identity theft.

If non-trivial portions of the internet are accessible only via age verification, and internet users who are underage or otherwise reticent to engage with the verification system seek to circumvent these requirements, it is reasonable to expect that age verification will drive a growing demand for fraudulent identification services, or other avenues to circumvent age verification systems, which potentially expose internet users to other forms of cybercrime.

Requiring users to digitally upload identification to access routine online services also increases the risk of social engineering attacks. As frequent identity checks become normalized, malicious actors gain more opportunities to impersonate and blend in with legitimate verification requests. Users also become more trusting as identity verification processes become habitual, an established marker of vulnerability to social engineering.[25]

Paradoxically, increasingly sophisticated verification methods may heighten rather than mitigate the security risk. While measures such as requiring multiple forms of identification or real-time photo verification may improve the accuracy of verification, they also amplify the potential harm of breaches, interception, or successful phishing attempts by increasing the volume and sensitivity of the data collected. Additionally, more complex verification processes demand greater technical literacy from users in order to navigate them safely. Social engineering exploits precisely this asymmetry: phishing attempts are more likely to succeed when users lack sufficient technical knowledge to distinguish legitimate requests from convincing imitations.[26] Thus, greater technological sophistication may exac-

---

[21] Barker et al, "Credit card fraud: awareness and prevention | Journal of Financial Crime | Emerald Publishing" (2008) 15:4 Emerald Publishing.

[22] Ferreira, Ana & Pedro Vieira-Marques, "Phishing Through Time: A Ten Year Story based on Abstracts" (2018) CINTESIS.

[23] Putra, Fauzan Prasetyo Eka et al, "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study" (2024) 4:1 Brilliance: Research of Artificial Intelligence 413–421.

[24] Collins, J Michael, Jeff Larrimore & Carly Urban, "Does Access to Bank Accounts as a Minor Improve Financial Capability? Evidence from Minor Bank Account Laws" (2021) Rochester, NY, online: <https://papers.ssrn.com/abstract=3972904>.

[25] Z. Wang et al, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods" (2021) 9 IEEE Access 11895 at 11903.

26 *Ibid* at 11903.

erbate both the likelihood of successful attacks and the harm flowing from them.

Biometric Verification

Biometric verification uses imaging of a user's face or fingerprints to check their age, comparing landmark features within the imaging against a statistical probability of those features in different demographics.[27] It typically employs multi-modal facial recognition using A.I.-powered deep learning systems, trained on datasets of faces to make connections between similarities.[28] Biometric verification naturally requires a user's device to have a working camera and may not contain an adequate alternative for those whose devices do not.

Implementing biometric verification requires the training of an A.I.-powered system, a process which presents its own privacy concerns. The datasets upon which these systems train are often sourced by broadly scraping sensitive, biographical data from across the internet. The process of acquiring training data for A.I. models lacks transparency and accountability, with minimal regulation in most jurisdictions.[29] A sample of high profile cases, such as the University of Washington scraping the pictures of over three million users in 2015 to make the MegaFace database that many tech companies now use,[30] or Facebook's payout of $650,000,000 over illegally collecting and storing biometric data,[31] are generally illustrative of the foundational problems that permeate this industry.

Facial recognition and age estimation technology is still developing, and remains inconsistent in terms of its reliability.[32] Factors like facial coverings, facial hair, and make-up greatly alter perceived age.[33] Distinguishing between users in the 13-18 year-old age range is the least accurate, despite that being the main target assessment group for age verification systems.[34] This is especially problematic for models that seek to restrict content at multiple age groups (i.e. 13+, 16+, and 18+). Different rates at which individuals go through puberty, changing body fat and muscle ratios, the onset and degree of acne, and other factors that affect facial appearance are at their most inconsistent during the period most relevant for age-gating purposes. These authentication challenges could lead to either an under-restrictive approach, whereby the systems accept a stronger likelihood of erroneously admitting underage users, or an over-restrictive approach, which wrongfully denies access to users who are over 18.

---

[27] Abdul-Al, Mohamed et al, "The Evolution of Biometric Authentication: A Deep Dive Into Multi-Modal Facial Recognition: A Review Case Study" (2024) 12 IEEE Access 179010.

[28] Choudhry, Mani Deepak et al, "Security and Privacy Issues in AI-based Biometric Systems" in *AI Based Advancements in Biometrics and its Applications* (CRC Press, 2024).

[29] Stephanie Forbes, "Balancing innovation with fairness: What transparency in AI means for copyright law" (21 January 2026), online: International Association of Privacy Professionals https://iapp.org/news/a/balancing-innovation-with-fairness-what-transparency-in-ai-means-for-copyright-law; See also California's *Training Data Transparency Act*, a landmark effort in the largely unregulated space which came into effect on January 1, 2026, online: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2013>.

[30] Harvey, Adam, "Creative Commons Biometrics" (2022) Adam Harvey Studio, online: <https://adam.harvey.studio/creative-commons/>.

[31] "Facebook raises settlement to $650 million in facial recognition lawsuit", Reuters (1 August 2020), online: <https://www.reuters.com/article/sustainability/facebook-raises-settlement-to-650-million-in-facial-recognition-lawsuit-idUSKCN24W312/>.

[32] Malik, Gaurav, "Biometric Authentication-Risks and advancements in biometric security systems" (2024) 6:3 Journal of Computer Science and Technology Studies 159–180.

[33] Davis, Hannah & Janice Attard-Johnson, "Your ID, please? The effect of facemasks and makeup on perceptions of age of young adult female faces" (2022) 36:2 Applied Cognitive Psychology 453–459.

[34] https://pages.nist.gov/frvt/reports/aev/fate_aev_report.pdf

Liability-based systems, which provide penalties for erroneously granting access, and no concomitant incentive to ensure that individuals above the age of majority are allowed in, naturally create incentives to be overly restrictive. These mistakes are not evenly distributed across the population. Biometric age evaluation typically performs poorly at identifying individuals from racially marginalized communities or with uncommon medical conditions.[35] Because the technology seeks to identify age based on generalizable norms drawn from training data, it is fundamentally prone to errors among minority groups that exist outside those common boundaries, leading to differential treatment and ultimately differential access. Forcing a two-factor verification for borderline cases compounds privacy risks by requiring a secondary verification source, and can further contribute to marginalization. While users can potentially appeal erroneous decisions, the websites and online platforms behind these systems are typically not known for having effective customer service.[36]

Another challenge stems from advances in deepfake technology, which provide a vector of attack which is rapidly scaling in sophistication. Off-the-shelf deepfake filters already allow individuals to look or sound like someone else, which could help minors to pose as adults. While these tools are not specifically marketed towards circumvention of age verification technologies at the moment, the normalization of age gating will inevitably lead to the development of specialized products designed to bypass these barriers. As deepfake technology continues to advance, these will become more difficult to detect.

Security concerns are also heightened with regards to biometrics. If this species of data is stolen, it cannot be replaced as easily as an ID card, since biometrics are an inherent part of a user's physical identity. A malicious agent with access to biometric verification data could do great harm and potentially prevent the user from being able to use biometrics as a source of verification at all in the future. Biometric data is particularly vulnerable because it creates multiple threat vectors simultaneously: it is inherently identifiable, linkable across different systems, and detectable in ways that allow tracking of individuals across platforms. Centralized databases commonly used for biometric verification compound these risks, as breaches expose not only individual users but entire populations whose biometric data can then be connected and exploited across multiple contexts.

Behavioural Verification

Behavioural verification involves analysing a user's digital footprint, such as their browsing history, social media interactions, digital social network, and purchases, to estimate their age. This method relies on A.I. systems that aggregate and evaluate user data, technology that many large platforms already leverage to construct estimated demographic profiles for users in the context of placing targeted content and advertisements.

A core privacy concern associated with behavioural verification is that it normalizes and requires collection and analysis of user data by the largest players in the tech industry, making it difficult to avoid these systems. Recent moves, such as Google automatically opting gmail users into content analysis, give rise to concerns over the invasive use of personal data.[37] Behavioural verification forces users to allow pervasive tracking of their online habits, often by large U.S.-based companies with problematic

---

[35] Stardust, Zahra et al, "Mandatory age verification for pornography access: Why it can't and won't 'save the children'" (2024) 11:2 Big Data & Society 20539517241252129.

[36] AdCapital8310, *Roblox age verification glitched and now I can't fix my age. What do I do?* (2025), Reddit.

[37] Arntz, Pieter, "[Correction] Gmail can read your emails and attachments to power "smart features"" (20 November 2025), online: *Malwarebytes*

privacy records. It would also force users to associate their day-to-day browsing with adult content access, eliminating anonymity and compounding privacy risks.

The accuracy of behavioural verification depends heavily on the quality of the datasets upon which the underlying AI model is trained, which may lead to discrepancies in accuracy across languages and cultures.[38] Meta's A.I. models were originally trained in English, for example, meaning that assessments for non-English users are likely be less accurate.[39] Other Large Language Models (LLMs), including Google, have also used English as the base language, requiring concepts to be translated into English in a way that creates cultural bias.[40] Behavioural verification is also potentially prone to circumvention, either by underaged users creating secondary accounts aimed at cultivating a digital footprint consistent with an adult or, more commonly, by exploiting shared devices with older household members.

2. Platform-Level Verification

Beyond the choice of verification method, the level at which verification occurs and the parties conducting it have profound implications for privacy and security. Two primary age verification models have emerged: at the platform-level and the device-level. The most common, the platform-level model, requires platforms or third-party age verification companies to verify the age of each individual visiting their website or app. Platform-level frameworks generally either require each website to develop its own verification system, or to contract with third-party age verification service providers to conduct verifications on their behalf.

The primary security concern with platform-level verification stems from the sheer volume of verifications required. Every time a user accesses an adult website or platform, they must submit sensitive personal information, likely through one of the aforementioned age verification methods. In the course of an individual's regular digital experience, they will be subject to a vast number of verifications, demanding various types of sensitive personal data, from government ID to biometric data to browsing history. This process represents a significant privacy intrusion and creates numerous opportunities for data interception, theft, or misuse.

The multitude of entities handling sensitive user data under platform-level models further compounds these risks. If every adult content platform conducts its own age check, the landscape would involve an enormous number of distinct actors collecting, processing, and storing highly sensitive information. Most adult websites do not have the infrastructure to implement robust security measures comparable to those employed by large mainstream platforms or government agencies, making them particularly vulnerable targets for malicious actors. The regulatory challenge of ensuring compliance with privacy best practices from the vast number of adult websites would create an enormous enforcement burden.

---

[38] Mohammed Raiz Shaffique & Simone van der Hof, "Mapping age assurance typologies and requirements" (19 April 2024) European Commission at p 31.

[39] Nicholas, Gabriel & Aliya Bhatia, "Lost in Translation: Large Language Models in Non-English Content Analysis" (2023) Arxiv, online: <http://arxiv.org/abs/2306.07377>.

[40] "New AI-powered live translation and language learning tools in Google Translate" (26 August 2025), online: *Google* <https://blog.google/products/translate/language-learning-live-translate/>; Stokel-Walker, Chris, "AI chatbot models 'think' in English even when using other languages" (8 March 2024), online: *New Scientist*

Complexities surrounding Third-Party Involvement

One avenue to mitigating concerns about forcing every website to carry out their own verification is to move the process through specialized third-party age verification companies, as is required under some existing and contemplated models.[41] While this does not fully resolve concerns about forcing users to engage with a patchwork of different systems, as there are competing models across this industry, there are some advantages to having age verification carried out by a specialized service provider. In particular, these companies can provide services to websites which lack the resources to develop secure in-house options. However, this shift does not eliminate privacy risks, but merely shifts the threat model to a smaller number of higher impact points of failure.[42] Third-party vendors operate under their own market and regulatory incentives, which in some cases favour data-retention, analytics, and product expansion once data is collected.

For example, there is a built-in tension between auditability and data-minimization. Third party contractors will face pressure to demonstrate the accuracy and efficacy of their services, which will need to be done through audits and performance evaluations. Proving compliance requires retaining logs, records, and other unexpected data artifacts which retain sensitive user data, increasing both exposure and the risk of any compromise.[43] Retention of data creates durable, high-value data sets that can be reused, repurposed, and ultimately breached. If one node in a shared verification network is breached, attackers can sometimes pivot across linked systems or reuse identifiers elsewhere, in what security researchers describe as cascading compromise.

Requiring third-party verification also removes a measure of control from the websites. Verifiers that stop providing their services or dissolve could jeopardize both the website and the users' data. Due to the bankruptcy of 23andMe, a company which specialized in genetic testing and ancestry tracing, hackers were able to obtain highly sensitive health and ethnicity information about over 18,000 accounts, alongside data about subjects' birth, sex, gender, and other sensitive markers.[44] At the end of the day, the opacity of verification ecosystem creates its own security and trust issues.

3. Device-Level Verification

An alternative to platform-level verification is to push the responsibility for verifying users' ages to device manufacturers, using an attribute-based approach that enables free access on any given device after a single verification. Here, an initial verification process generates a proof-of-age signal associated with an individual's device. As the individual browses the internet, the device transmits to platforms only the proof-of-age signal, as the attribute for governing access to particular age-gated content or services.

Around the world, two types of prominent device-level models have emerged that place the responsi-

---

[41] *See* Bill S-209, An Act to amend the Criminal Code (protection of children), 1st Sess, 45th Parl, Canada, 2025 (first reading), ["S-209"].

[42] Ilori, Oluwatosin, Nelly Tochi Nwosu & Henry Nwapali Ndidi Naiho, "Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies" (2024) 22:3 World Journal of Advanced Research and Reviews 213–224.

[43] Raji, Inioluwa Deborah et al, *Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing* (New York NY USA: ACM, 2020).

[44] Canada, Office of the Privacy Commissioner of, "Backgrounder: Summary of joint investigation into data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner" (17 June 2025), online:

bility of verification on different entities. In California, the *Digital Age Assurance Act* places a burden on device makers like Apple and Google to collect each user's date-of-birth whenever they set up a laptop, phone, or tablet.[45] Meanwhile, the European Union is piloting a device-level model through a government-controlled age-verification app (AVA) under the *Digital Services Act.*[46]

Privacy and Security Considerations for Device-Level Models

The reduction in verification frequency implied by a device-based approach represents a substantial privacy and security advantage over platform-level models. Instead of submitting sensitive personal information to dozens or hundreds of different platforms over time, individuals only verify their age when they activate a new device. This generates far fewer opportunities for data interception, phishing attempts, and other security compromises from malicious actors. However, device-level models must still find a way to verify the age of users, usually based on one of the methods outlined in section 1 of this chapter, including whatever privacy and security risks may be associated with that method.

Device-level and app-based models also partially mitigate some privacy concerns by shielding platforms from accessing sensitive personal information beyond the proof-of-age attribute itself. When a user visits an age-restricted website, the platform receives only a cryptographic signal or token confirming that the user meets the age requirement, as opposed to a copy of their government ID, biometric scan, or other identifying information. This protects user privacy by minimizing data transmission, ensuring that platforms have access only to information that is strictly necessary.

However, device-level models introduce their own considerations regarding shared devices and secondary device markets. Devices are frequently shared among family members, raising concerns that a device with an adult's proof-of-age could be used by a minor to access restricted content. This challenge could potentially be addressed by leveraging existing technology to enable multiple password-protected user profiles, each with its own age verification status, though these require a baseline level of technological sophistication and conscientiousness to operate consistently (i.e. adult users will need to set up multiple accounts for the different people accessing, and remember to sign out before they turn the device over to someone underage). Device-level models must also raise the risk that minors may purchase used devices in the resale market that have an adult's proof-of-age. While lawmakers could mitigate this risk by legislating mandatory system resets upon resale and penalties for intentional circumvention, these are likely to be only partially effective given the fluid and informal nature of much of the resale market.

Assigning Verification Responsibility

The centralization of verification authority under device-level models presents both advantages and risks. On one hand, concentrating verification functions – either amongst device makers or within

---

[45] Under the DAAA, individuals self-declare their date-of-birth whenever they set up a laptop, phone, or tablet, after which a corresponding proof-of-age signal automatically transmits from the device to apps and websites, who restrict the device's access based on the age rating of the content they host (under 13, 13-16, 16-18, or 18+); See DAAA, ss 1798.501(a)–(b).

[46] Under the European Age Verification Solution, which is currently being piloted in Denmark, France, Greece, Italy, and Spain, individuals download the AVA on each of their devices and may verify their age through a variety of means, including digital ID review, age information collected by national eID schemes, Know Your Customer procedures, and existing databases; See European Commission, "Technical Specification of the Age Verification Solution: Overall Architecture" (2025) at 2.3 , online (technical documentation): <https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications/#23-user-journey> [AVA Overall Architecture].

the government – reduces the number of parties handling sensitive data. Fewer actors equates to fewer databases that could potentially be compromised. Moreover, these parties tend to have far greater resources and expertise to implement robust security measures compared to individual content platforms. Established device makers already handle vast amounts of sensitive user data and have invested heavily in security infrastructure to protect it. Governments are also well-equipped to handle sensitive data responsibly, particularly given their legal obligations to protect citizens' personal information and the accountability mechanisms in place to ensure that they do so.

On the other hand, centralization creates higher-value targets for cyberattacks. While the likelihood of successfully breaching a well-resourced entity is lower, the consequences of such a breach would be an order of magnitude greater. A breach of a centralized device maker or government database would expose the data of a vast number of users, far exceeding the scale of damage from a breach at the platform-level. As past high-profile breaches such as the SolarWinds hack and the U.S. Office of Personnel Management breach illustrate, even highly resourced and sophisticated entities can often struggle to protect sensitive data from attacks.[47] The best way to avoid a harmful breach of sensitive data will always be to refrain from collecting it in the first place.

Opportunities for Offline Verification

One potential response to concerns associated with both device and platform level verification could be to pursue a model which as closely as possible approximates traditional manual ID checks, namely through implementing a form of offline verification. The logistical implementation of offline verification – including accessibility and efficacy considerations – would vary significantly depending on whether verification is conducted by device makers or governments.

For device manufacturers operating under a device-level model like California's, devices could be set in a default "child-safe" mode at the point of manufacture, which sends a signal to websites and other online services that the user is underage. Customers who wished to have the child-safe mode disabled could present a government-issued ID to an authorized sales clerk, or government verification agent, who could verify the user's age in much the same way a bar or tobacconist would. The agent or company representative could then permanently disable the child-safe mode through a secure process provided by the device maker.

By approximating traditional paradigms of age verification as closely as possible, this approach significantly mitigates security and privacy concerns associated with most existing digital proposals, as it significantly limits the collection and storage of sensitive PII. However, it does not eliminate privacy concerns entirely, especially as many people either lack appropriate government-issued documentation, or are hesitant to share them widely with government agents.[48] Once again, these challenges are particularly prevalent among marginalized groups, such as undocumented immigrants or racialized minorities.

---

[47] Saheed Oladimeji and Sean Michael Kerner, "SolarWinds hack explained: Everything you need to know" (3 November 2023), online: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know; Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America" (12 February 2020), online: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[48] *See, e.g., the impact of ongoing immigration enforcement raids in the United States on targeted communities:* Teresa Liu, "ICE raids in Los Angeles leave immigrants afraid to report discrimination, Los Angeles Daily News (June 27, 2025), online: <https://www.dailynews.com/2025/06/27/ice-raids-in-los-angeles-leave-immigrants-afraid-to-report-discrimination/>.

4. Lessons for Regulators

Implementing an age verification system which is secure, private, effective and reliable presents a range of technological, legal, architectural, and logistical challenges. Not all methods to verify age operate the same, nor do they all require the same type or amount of user data. Minimizing the risk of harm to user privacy should be a top priority in the development and implementation of age verification methods, and legislative schemes should be sensitive to that consideration. To uphold the privacy and security of user data during age verification, controls must be implemented proactively and in a manner which addresses the whole of the system's lifecycle, from user data collection, transmission, processing, and storage, through to deletion.[49] Age verification methods should also be transparent in how data is handled and stored and users should ideally be given the option to choose how their data is used beyond obvious or explicit purposes.[50] Effective age verification should also mandate thorough assessments of potential vectors for attack. Data and methods of transmission that may be at risk should also be characterized, including a thorough consideration of worst-case outcomes.[51]

Data minimization suggests that websites, or other online service providers, must only collect and retain data strictly necessary to perform their function.[52] Specifically, age verification technologies should only collect user data for the purpose of age verification.[53] User data should not be collected or retained if it is not critical to the user's continued access to, or usage of, an age-gated site.[54] Unnecessary data collected and retained by an age verification service provider can result in a heightened risk of that data being accessed by a malicious actor.[55] Similarly, more stakeholders in a data transmission system can increase the risk to the data from cyber criminals, by creating more avenues for attacks or leaks.[56] This practice also specifically combats function creep, as it reduces the value and amount of user data that could be repurposed.[57]

Legislation overseeing both private or government use of personal data should impose limitations on data storage, specify a process and scope for third parties to profit from user data inputs, and impose minimum security requirements on any entity handling user data.[58] From the Equifax breach, it is clear that users should be empowered to exercise control over their own data, when it is held by a third

---

[49] Elisa Orru, "Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance" in Ronald Leenes et al, eds, Data Protection and Privacy: (In)visibilities and Infrastructures (Springer International Publishing, 2017) at 108. <https://link.springer.com/book/10.1007/978-3-319-50796-5> [Orru]

[50] Orru, *Ibid;* Jochen Peter & Patti M Valkenburg, "Adolescents' Online Privacy: Toward a Developmental Perspective" in Sabine Trepte & Leonard Reinecke, eds, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (Berlin: Springer, 2011) at 222. <https://doi.org/10.1007/978-3-642-21521-6>; Ann Cavoukian, "Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head" (2017) 7:4 Health & Tech at 330. <https://link.springer.com/article/10.1007/s12553-017-0207-1>.

[51] Murray, Chhipa & Yerby, *supra* note 17 at 336.

52 Samuel Aiello, "Privacy Principles and Harms: Balancing Protection and Innovation" (2024) 2024:1 Journal of Cybersecurity, Education, Research & Practice at 2. <https://doi.org/10.62915/2472-2707.1167> [Aiello]

[53] Aiello, *Ibid.*

[54] Christine Marsden, "Age-Verification Laws in the Era of Digital Privacy" (2020) 10:2 National Security LJ at 229. <https://www.nslj.org/wp-content/uploads/Marsden-10.2-v272.pdf> [Marsden]

[55] Marsden, *Ibid.*

[56] Murray, Chhipa, & Yerby, *supra* note 17 at 336.

[57] Emilio Mordini, "Ethics and Policy of Biometrics" in Massimo Tistarelli, Stan Z. Li & Rama Chellappa, eds, Handbook of Remote Biometrics for Surveillance and Security (London: Springer, 2009) at 295. <https://link.springer.com/chapter/10.1007/978-1-84882-385-3_12> [Mordini]

[58] Murray, Chhipa & Yerby, *supra* note 17 at 335.

party.[59] It also showed that victims of cybercrime need transparent notification about if or when their data was compromised following a breach.[60]

Websites should not use verification methods that rely on "static", or hard to change, PII, like that contained on a driver's license, or social insurance numbers.[61] This practice reduces the likelihood that stolen data continues to remain useful for cyber criminals long after a breach occurs.[62]

Even if an age verification system offers robust security measures, following best practices that ensure minimal user data is collected, retained, and not repurposed, there are outstanding concerns raised by the pervasive nature of mass surveillance facilitated by age-gating the internet. While the better practices mentioned above help to mitigate security and privacy concerns, the litany of challenges mentioned throughout this section necessitate careful consideration of the inherent costs and trade-offs inherent in any broadly applicable age verification scheme. The legislative intent and purported benefits for age verification schemes, restricting youth access to certain content, must be critically scrutinized against the risks of surrendering privacy in favour of the proliferation of surveillance on the internet.

---

[59] Moore, *supra* note 3 at 48.

[60] Moore *Ibid.*

[61] Moore, *Ibid.*

[62] Moore, *Ibid.*

CHAPTER 5
Age Verification and Freedom of Expression

By William Hepner and Mitchell Mathieson

While the previous chapter focused on the privacy and security risks associated with the collection and storage of sensitive personally identifiable information under age verification laws, this chapter considers the expressive consequences of those processes. Privacy and anonymity are distinct yet intertwined concepts. Privacy concerns the user's control over who sees their data and how it is disclosed, whereas anonymity is the structural shield that allows for communication without any link to a legal identity. This distinction is critical because while a user may trust a platform with their data, the loss of a sense of public anonymity changes the fundamental nature of communications.

Age verification has a profound impact on the right to freedom of expression online. By functionally requiring adults to disclose their identities to access certain areas of the internet, age verification erodes the general right to anonymity and circumscribes the speech rights of minors. Even the mere perception of being monitored can trigger a profound chilling effect, leading to self-censorship and a withdrawal from important social spheres.[1] When users believe their identities are exposed or their digital trails are being tracked, they often hesitate to question authority or express unpopular views, which ultimately weakens public trust and degrades the quality of democratic dialogue.[2] This underscores the necessity of the fundamental ability to choose how and with whom information is shared. Such autonomy is a necessary precondition for a free and democratic society, underpinning the honest and secure exchange of ideas that is required for a healthy informational ecosystem.

1. Anonymity and the Internet

Anonymity is a core aspect of the right to freedom of expression. Historically, anonymous speech allowed authors and commentators to have their ideas evaluated "on the basis of their arguments, devoid from any bias a reader might attach to their identities."[3] Anonymity was an essential protection for groups such as female writers, for whom publishing under pseudonyms upheld virtues of modesty and protected their private lives. More broadly, this buffer allows individuals to engage with sensitive topics that might otherwise lead to social stigma or professional harm, including the ability to discuss religious matters or seek community support for issues such as addiction, illness, or domestic abuse.[4] In these sensitive contexts, the structural shield of anonymity ensures that essential human experiences and diverse perspectives are not driven underground by the threat of public exposure.

Anonymity on the internet presents a unique and often misunderstood paradigm. To the average user,

---

[1] Association for Progressive Communications, *The Right to Freedom of Expression and the Use of Encryption and Anonymity in Digital Communications: Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression* (February 2015) at 9,11.

[2] *Ibid* at 6.

[3] Victoria Ekstrand, "The Many Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law" (9 September 2013), Journal of Technology Law & Policy, Vol 18, No 1, 2013, SSRN: https://ssrn.com/abstract=2322818 at 14.

[4] Association for Progressive Communications, The Right to Freedom of Expression and the Use of Encryption and Anonymity in Digital Communications: Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression (February 2015) at 4.

the digital world often may feel familiar and even intimate, providing a "tremendous feeling of freedom" where secret interests can be pursued and "users can express their unfiltered opinions on things great and trivial without fear of what their family or social circle might think."[5] The internet vastly expands the scope of expression, enabling users to find connection in niche communities with users from around the world. On most platforms, users have the ability to communicate without revealing their identity to other users. For a "gay Ugandan or Russian, or a Saudi atheist," the internet provides the only "open avenue for self-expression and for allowing the oppressed to network with likeminded communities."[6] In these contexts, anonymity is not merely a preference but a safety condition.

Paradoxically, despite the internet's reputation as a safe haven for anonymous engagement, it is actually the "most heavily monitored and tracked medium of expression in history."[7] While the previous chapter discussed the technical privacy and security risks of age verification, these concerns must be understood through their impact on the internet's character as a space for free communication.

2. Anonymity and Freedom of Expression

While anonymity is often critiqued as a structural vulnerability that shields bad actors, it is more accurately understood as a vital democratic safeguard that warrants protection even in the face of digital challenges. Critics argue that the internet "offers too much anonymity," creating an environment where "perpetrators escape detection" and misconduct occurs with "impunity."[8] Similarly, researchers point to the "online disinhibition effect," where the lack of identity cues correlates with increased hostility.[9] However, framing anonymity solely as a catalyst for incivility ignores its profound importance in enabling marginalized voices to speak truth to power, protecting privacy in an era of surveillance, and facilitating open exploration of sensitive topics.

The tension lies in how we value this trade-off. Detractors argue that anonymity degrades the information environment, warning that anonymous speech deprives audiences of credibility cues, potentially causing "epistemic harm" and spreading misinformation.[10] Supporters of identification-based regulation view age verification as a correction to an ecosystem that over-privileges privacy. This perspective often fails to account for the chilling effect that mandatory identification imposes on lawful, valuable speech.

Legal frameworks protecting freedom of expression have long emphasized the distinct value of anonymous speech, recognizing that expression often flourishes where public identification might otherwise suppress it. Globally, the principle that individuals should be able to communicate without revealing their identity informs both international human rights standards and national regulatory frameworks.[11] The Council of Europe's Declaration on Freedom of Communication on the internet

---

[5] Michael Karanicolas, Travel Guide to the Digital World: Surveillance and International Standards (London: Global Partners Digital, 2014) at 6.

[6] *Ibid* at 7.

[7] *Ibid* at 7.

[8] Bryan H. Choi, "The Anonymous Internet" (2013) 72 Md L Rev 501 at 2, 6.

[9] Joseph Graf, Joseph Erba & Ren-Whei Harn, "The Role of Civility and Anonymity on Perceptions of Online Comments" (2017) 20:4 Mass Commun & Soc 526–549 at 527, 532, DOI: 10.1080/15205436.2016.1274763.

[10] *Ibid* at 4, 6.

[11] ARTICLE 19, Right to Online Anonymity: Policy Brief (London: ARTICLE 19, June 2015) at 7, online: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf.

firmly established this principle, advising that "Member States should respect the choice of users of the internet not to disclose their identity."[12] In a 2013 report, the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression underscored the necessity of anonymity, explaining that "Privacy and freedom of expression are interlinked and mutually dependent," and that without ensuring the "privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers... cannot be assured that their communications will not be subject to States' scrutiny."[13]

Anonymity is often understood as being deeply connected with the exercise of expressive rights. The United States Supreme Court, for example, recognized anonymity as a "necessary adjunct to freedom of expression."[14] Functioning as a "shield from the tyranny of the majority," anonymity historically enabled "persecuted groups and sects" to criticize oppressive practices and laws "either anonymously or not at all",[15] maintaining an "honorable tradition of advocacy and dissent."[16] By protecting the speaker from identification and potential reprisal, anonymity ensures that expression is "not unnecessarily inhibited."[17] This protection supports democratic discourse, ensuring that, as the Supreme Court stated, the "interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry."[18]

While Canada's case law on the right to anonymous speech is not as extensive as the United States, the Supreme Court of Canada has repeatedly emphasized the importance of maintaining privacy in digital communications through its section 8 jurisprudence.[19] Although international human rights instruments such as the ICCPR are generally not self-executing in Canada, they inform the interpretation of constitutional rights and reinforce the principle that anonymity can be integral to expressive freedom.

3. Age Verification and its Impact on Digital Speech

Most proposed age verification laws undermine online anonymity by creating a technical environment where access to certain areas of the internet is impossible without formal identification. To function effectively, these systems require a mechanism to verify a user's age, which generally implicate the provision of or access to "static" or hard to change pieces of PII. Because verification is extremely difficult to achieve without such identification, this process necessitates the creation and usually the maintenance of a digital trail, transforming the internet into an environment where every interaction is tied to a verified profile. By collapsing the structural separation between identity and inquiry, age verification laws are a natural challenge to perceptions of online anonymity.

Although the point may seem obvious, it is important to point out that age verification is likely to have

---

[12] Council of Europe, Committee of Ministers, Declaration on freedom of communication on the Internet, (adopted 28 May 2003) 93 Inf Bull 58.

[13] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UNGAOR, 23rd Sess, UN Doc A/HRC/23/40 (2013) at para 79.

[14] Diane Rowland, "Privacy, Freedom of Expression and CyberSLAPPs: Fostering Anonymity on the Internet?" (Paper delivered at the 18th BILETA Conference, Queen Mary, University of London, April 2003) at 3.

[15] *Ibid* at 2.

[16] Ekstrand, *supra* note 3 at 4,30.

[17] Rowland, *supra* note 14 at 6.

[18] Ekstrand, *supra* note 3 at 31.

[19] *See,* e.g., *R. v. Bykovets,* 2024 SCC.

a profound impact on how digital speech works for internet users of all ages, particularly by requiring adults to authenticate their ages.[20] Conditioning access to information on the surrender of identity creates a persistent digital trail that links specific online traffic directly to a real-world persona. By necessitating this link, age verification laws make it impossible to decouple a user's legal identity from their digital inquiries. Canada's Office of the Privacy Commissioner has flagged that linking identity to online activity can discourage people from "operating freely" online and can exclude users from encountering important information.[21] The potential for a chilling effect on speech is likely to be particularly sharp in the context of rising global authoritarianism, as well as parallel moves by governments around the world to enhance their authority to request user data from online platforms.

Traceable browsing can carry professional stigma, including for educators and clinicians, threats to physical safety, such as for people in abusive households, and community risk, such as for LGBTQ2S+ persons in hostile environments. For adults who create content such as sexual-health explainers, harm-reduction resources, or LGBTQ2S+ community supports, age verification compliance pressure can shift incentives toward self-censorship, de-indexing, or avoiding audiences in impacted jurisdictions altogether.

Age verification laws often cast a wider net than intended. For example, even when ostensibly targeted solely at sites offering adult content, their definitions can often bring in mixed use platforms or general purpose websites which feature content potentially subject to age gating alongside educational, artistic, health, and other user-generated expression. While some contemplated age verification laws carve out exceptions or defences for these legitimate purposes, legal uncertainty regarding case-by-case adjudication inevitably persists.[22] Even if exceptions for educational purposes exist, concern about the determination of what is protected and the cost of proving content falls within those bounds can still have a chilling effect on creators. Platforms are incentivised to over-comply with age verification laws to avoid exposing themselves to potential liability.

This is where children's and adults' expressive rights become interdependent. Youth are "listeners" in the informational ecosystem. If adults withdraw or platforms over-comply and purge grey-zone content, youth lose lawful information that supports health and development. A child-safety regime can thereby have outsized impacts beyond strict understandings of its scope, undercutting the notion that these laws will improve children' s online experiences and safety while leaving adults unaffected. The combined impact is the normalization of traceability as a prerequisite for participation. When users can no longer explore sensitive or controversial topics without generating an directly identifiable digital trail, anonymity ceases to function as a practical safeguard, and expressive freedom is chilled for those who cannot safely tolerate monitoring.

---

[20] Canadian Bar Association's Privacy and Access Section, *Re: Bill S-209 – An Act to restrict young persons' online access to pornographic material* (Dec 13 2025), online: https://cba.org/Our-Impact/Submissions/Bill-S-209-An-Act-to-restrict-young-persons-online-access-to-pornographic-material.

[21] Canada, Office of the Privacy Commissioner ("OPC"), *Consultation on age assurance – What We Heard* (2024), online: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-age/report_age_2025/.

[22] See Canada's Bill S-209, An Act to restrict young persons' online access to pornographic material, 1st Sess, 45th Parl, 2025, s 7(2).

4. Impacts on Racialized, Immigrant, and Low-Income People

The chilling effects of identity-based age verification are not felt equally across all demographics, as these systems inherently embed socioeconomic and racial inequality into access. Government ID ownership, stable addresses, private devices, and household privacy are not evenly accessed across society.[23] Neurodivergent individuals may be less likely to confirm to behavioural or motion-based estimation. Newcomer families may face language barriers and uneven digital literacy, increasing vulnerability to misunderstanding consent flows, misjudging risk, or falling victim to scams that exploit verification prompts.

Importantly, these burdens do not vanish because a system is marketed as being "for children". Adult newcomers may fear that identity-linked browsing could have reputational or immigration-adjacent consequences even when the browsing is lawful.[24] This risk is compounded for racialized individuals who may already feel targeted by state surveillance.

5. Children's Rights and Access to Information

Age verification is not just a content rule, it operates as a control mechanism for online material. It establishes who can access lawful information, who feels safe enough to seek it, and which communities bear the risks of traceability, error, and exclusion. Depending on how it is implemented, it can introduce traceability and data-handling risks as well as exclusion and loss of access effects. The central question is not only whether age verification is well-intentioned but whether it is consistent with our rights, effective against the harms it claims to address, and equitable in practice.[25]

A rights-respecting regulatory approach must recognize that youth safety is inseparable from expressive freedom. This is particularly important within the sexual-health and identity context, where expressive freedom is often essential to safe development. Research has highlighted that digital tools can support learning and help-seeking, and that privacy and anonymity are often integral to whether young people will use these resources.[26]

As a consequence, age verification is properly understood as fostering a trade-off between its intended purpose of preventing minors' access to age inappropriate material, and its likely incidental impact restricting young people's opportunity to explore ideas, develop identity, and seek knowledge online.[27]

International instruments also reinforce and help to interpret the likely impact of age verification on children's rights. Article 13 of the *Convention on the Rights of the Child* protects children's right to "seek, receive and impart information and ideas of all kinds," and Article 17 commits states to ensure chil-

---

[23] Access Alliance, *The Current State and Impact of Digital Literacy and Equity Factors on Newcomers' Healthcare Access* (Sept 2024) at pp 8-9, online: https://accessalliance.ca/wp-content/uploads/2025/12/The-Current-State-and-Impact-of-Digital-Literacy-and-Equity-Factors-on-Newcomers-Healthcare-Access-2024.pdf.

[24] Peel Newcomer Strategy Group, *Exploring Digital Equity for Newcomer Services: Perspectives on Access and Challenges in Peel Region* (December 2024) at p 30, online: https://peelnewcomer.org/wp-content/uploads/2025/01/Digital-Equity-in-Settlement-Services-Report_Final.pdf.

[25] OPC, *supra* note 21.

[26] Meherali et al, "Digital knowledge translation tools for sexual and reproductive health information to adolescents: an evidence gap-map" (2024) Ther Adv Reprod Health, online: https://pubmed.ncbi.nlm.nih.gov/39703678/.

[27] OPC, *supra* note 21.

dren have access to information that promotes their well-being and development.[28] Article 19 of the *International Covenant on Civil and Political Rights* protects freedom of expression and access to information, allowing restrictions only when necessary and proportionate to legitimate aims.[29] The policy question is not whether children should be protected, but whether identity-based gating is a justified and minimally impairing way to pursue protection.

While children's expressive rights are often subject to greater restriction than those of adults, those expressive rights nonetheless exist. Section 2(b) of the *Canadian Charter of Rights and Freedoms* protects "everyone,"[30] and the Supreme Court of Canada has repeatedly emphasized that freedom of expression includes both the right to convey meaning and the right to receive information necessary for personal development and participation in society.[31] The Supreme Court of Canada has also cautioned about "protective" measures that create discriminatory and censorship effects through broad screening and enforcement strategies that do not reliably track actual harms.[32] Canadian jurisprudence has also rejected the idea that all sexually explicit material is equally harmful but rather looks at context and harm (not mere offensiveness), and it insists on careful consideration when expression is restricted in the name of protection.[33]

For children and adolescents, anonymity is frequently a basic condition of accessing lawful information and support, particularly in sensitive areas where disclosure carries a real risk of stigma or other consequences. Sexuality, contraception, consent, STI prevention, sexual orientation, gender identity, and abuse are areas where youth regularly report barriers to offline guidance.[34] The Canadian Paediatric Society has highlighted that adolescents are more likely to seek care and disclose sensitive information when confidentiality is assured.[35] Further, research has shown that many youth seek sexual health information online specifically for privacy reasons, with sexual minority youth particularly likely to do so when they feel they have no one they can ask offline.[36] Anonymity is therefore not merely a "preference," but functions as a harm-reduction feature of accessing information.

---

[28] Convention on the Rights of the Child ("CRC"), OHCHR", 20 November 1989, online: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[29] International Covenant on Civil and Political Rights ("ICCPR"), OHCHR, 16 December 1966, online: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[30] *Canadian Charter of Rights and Freedoms,* s 2, Part I of the *Constitution Act,* 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

[31] *Irwin Toy Ltd. v. Quebec (Attorney General),* 1989 CanLII 87 (SCC), [1989] 1 SCR 927.

[32] *Little Sisters Book and Art Emporium v. Canada (Minister of Justice),* 2000 SCC 69 (CanLII), [2000] 2 SCR 1120.

[33] *R. v. Butler,* 1992 CanLII 124 (SCC), [1992] 1 SCR 452.

[34] Isabelle Marie Flory & Eran Shor, "Porn is blunt [...] I had way more LGBTQ+ friendly education through porn": The experiences of LGBTQ+ individuals with online pornography, Sexualities 2025, Vol. 28(4) 1505–1525, online: https://www.mcgill.ca/sociology/files/sociology/2025_-_sexualities.pdf.

[35] Holly Agostino MD & Alene Toulany MD, "Considerations for privacy and confidentiality in adolescent health care service delivery", online: https://cps.ca/en/documents/position/privacy-and-confidentiality-in-adolescent-health-care.

[36] Kimberly J Mitchell, "Accessing sexual health information online: use, motivations and consequences for youth with different sexual orientations" Health Educ Res 2014 Feb;29(1):147-57, online: https://pubmed.ncbi.nlm.nih.gov/23861481/.

6. Children's Capacity and Marginalized Youth

Another policy issue associated with existing age verification proposals are that they tend to treat childhood as a single, binary status. The vast majority of legislation targeting adult content around the world draws a hard 18+ line for access. In reality, adolescents' capacity, vulnerability, and information needs vary significantly across ages and contexts. The UN *Committee on the Rights of the Child* (CRC) has cautioned that generic, one-size-fits-all policies often fail to address adolescents "in all their diversity," and emphasizes respect for adolescents' dignity, agency, and evolving capacities.[37] This is important as adolescence is a developmental period where identity formation and participation are increasingly impacted through the digital environment. Further, the CRC specifically links adolescents' rights to "seek, receive and impart information and ideas" with a requirement that protective approaches not displace those expressive rights.[38] The *Convention on the Rights of Persons with Disabilities* also reinforces the expectation of equal access to information and non-discrimination in digital contexts.[39] In Canada, section 15 of the *Charter of Rights and Freedoms*' equality guarantee makes it difficult to defend systems that predictably exclude disabled users unless strong mitigation, accessible remedies, and alternative access paths exist.

Regulators have often treated the tendency of age verification measures to impact lawful expression and information seeking as a proportionality or design problem. The European Data Protection Board (EDPB) stresses that the necessity and proportionality of age assurance must be demonstrated through a risk-based assessment and that children's views and their evolving capacities should be considered.[40] The EDPB further warned that requiring age checks for all users across all content would fail to meet appropriate standards of necessity and proportionality.[41]

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.[42] For LGBTQ2S+ youth, research has highlighted that online spaces can be essential for identity development, support, and access to affirming sexual-health information where formal systems are lacking.[43] In that context, overly broad age verification categories can restrict access not only to explicit adult content, but also to lawful resources that are educational, health-oriented, or identity-affirming – raising a heightened risk of over-blocking information that is closely tied to youth wellbeing and participation in public life. LGBTQ2S+ content is also disproportionately likely to be classed as age inappropriate, or otherwise subject to politically motivated restrictions.[44]

For youth who are more likely to be misclassified by verification systems, the rules can function as a barrier rather than a safety measure. As noted in chapter 4, many age verification systems suffer ongo-

---

[37] CRC, *supra* note 28.

[38] *Ibid.*

[39] Convention on the Rights of Persons with Disabilities ("CRPD"), UNCRPD, 12 December 2006, online: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities.

[40] European Data Protection Board ("EDPB"), *Statement 1/2025 on Age Assurance,* at para 12, online: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf.

[41] *Ibid* at para 14.

[42] OPC, *supra* note 21.

[43] Egale, *Learning From Queer and Trans Sexual Joy: Cultivating Just, Pleasurable, and Affirming Sexual Cultures,* online: https://indd.adobe.com/view/publication/42fb9e0e-e509-4b38-bf49-d302bb71c510/1/publication-web-resources/pdf/Queer_Sexual_Joy_Report_V_01.pdf.

[44] *See, e.g.,* Little Sisters Book and Art Emporium v Canada (Minister of Justice) [2000] 2 S.C.R. 1120, 2000 SCC 69.

ing performance differences across demographics – creating predictable outcomes for false rejection and exclusion.[45] This risk of exclusion is particularly important for disabled youth and other youth whose features or presentation may not be properly handled by models trained on limited datasets. This means that marginalized youth may be blocked from accessing lawful material with little recourse available.

A rights-respecting regulatory approach should recognize that youth safety is inseparable from expressive freedom. Policies that deny children the ability to seek information anonymously do not protect development, they constrain it.

7. Lessons for Regulators

Although age verification proposals are primarily emerging within democratic nations, the rapid erosion of rights even in stable societies cautions against complacency. Expansions of digital surveillance that undermine anonymity are particularly concerning in light of rising global authoritarianism and broader challenges against democracy and human rights principles around the world, particularly in the context of backsliding by established democracies.

Measures that mandate identity disclosure or compromise anonymity create powerful infrastructure for surveillance and control. This infrastructure is inherently susceptible to being repurposed for governmental monitoring or silencing dissent, especially during times of political instability. In Brazil, the constitutional prohibition on anonymity led to the banning of apps like Secret (an anonymous communication app) and extensive monitoring during the 2014 World Cup protests.[46] Authorities tracked keywords such as "protest" to create databases of activists, violating rights to assembly and privacy, and fostering an environment where dissenters self-censor to evade investigations.[47] Similarly, South Korea's former real-name verification system for online postings, in place until ruled unconstitutional in 2012, amplified self-censorship, particularly on politically sensitive topics, as users feared prosecution or social repercussions.[48] In China, extensive surveillance has silenced dissent both at home and abroad. Pro-democracy students in Australia, for example, have altered their behaviour and self-censored online to avoid harassment from peers or authorities, with real-world reprisals including account closures and threats.[49]

Crucially, this dynamic poses a specific threat to the digital landscape. Mixed-use platforms face a binary choice: condition access on government-mandated verification, adding friction to the user experience, or simply eliminate the legal risk entirely. This dilemma extends far beyond social media

---

[45] Amnesty International, "Racial bias in facial recognition algorithms" (21 Mar 2023), online: https://amnesty.ca/features/racial-bias-in-facial-recognition-algorithms/.

[46] Cynthia Wong, "Too Many Secrets: Court Ruling Spells Bad News for Anonymous Speech in Brazil", Electronic Frontier Foundation (12 August 2014), online: https://www.eff.org/deeplinks/2014/08/too-many-secrets-court-ruling-spells-bad-news-anonymous-speech-brazil?language=tr.

[47] Carolina Rossini, Francisco Brito Cruz & Danilo Doneda, The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet (Paper Series No 19, Global Commission on Internet Governance, September 2015) at 19.

[48] Whon-il Park & Graham Greenleaf, "Korea Rolls Back 'Real Name' and ID Number Surveillance" (October 2012) Privacy Laws & Business International Report, No 119, 20–21, at 2, UNSW Law Research Paper No 2012-57.

[49] Human Rights Watch, "They Don't Understand the Fear We Have": How China's Long Reach of Repression Undermines Academic Freedom at Australia's Universities (30 June 2021), online: https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines.

giants like X or Reddit. It impacts private community hubs like Discord, non-profit archives like Archive of Our Own (AO3), and educational pillars like Wikipedia. All of these platforms host content that could fall into the "arguably explicit" grey area of many adult verification laws. Faced with strict liability, these platforms will likely choose to aggressively scrub their sites. To avoid the threat of heavy penalties, there will likely be a purge not just of explicit material but also everything that has a hint of connection to age gated content. This may include sex education resources, LGBTQ2S+ support groups, and artistic content. The likely result is the destruction of safer spaces for expression, with the potential to drive information-seeking youth towards darker and less regulated corners of the internet.

The chilling effect of mandatory identification is quantifiable through user behaviour metrics, revealing a consistent pattern of withdrawal and evasion across the internet. Empirical evidence demonstrates that when anonymity is conditioned on identity verification, a large number of users simply disengage. In the context of adult content, traffic to major platforms like Pornhub dropped by approximately 80% following the enactment of verification mandates in Louisiana.[50] This phenomenon is not unique to adult sites. In the realm of political discourse, South Korea's real name verification laws caused a massive drop in user participation on news portals, silencing the moderate majority while failing to stop malicious speech.[51] This confirms that for the average citizen, the cost of surrendering anonymity outweighs the value of digital participation.

This user withdrawal creates a dangerous paradox for safety. Verification laws do not stop consumption; they displace it. Data from the United States shows that alongside the traffic collapse in regulated states, searches for Virtual Private Networks (VPNs) surged by over 200%.[52] While many VPNs offer reputable services, others, including most free options, include significant safety and security trade-offs.

The spread of age verification laws is an enormously consequential change for the global public discourse. Although there are legitimate concerns about accountability in the digital age, the historical and constitutional weight of anonymous speech suggests it is still worth upholding. The ability to speak without fear of retribution remains a cornerstone of free expression, and surrendering it to solve specific harms risks undermining the very freedom that the internet was designed to foster.

---

[50] Justin Sherman, "Age Verification Laws Are a Privacy Nightmare—and VPNs Aren't a Simple Fix", Wired (12 September 2025), online: www.wired.com/story/vpns-and-age-verification-laws/.

[51] Daegon Cho & K Hazel Kwon, "The impacts of identity verification and disclosure of social cues on flaming in online user comments" (2015) 51:Part A Computers in Human Behavior 363 at 370.

[52] "VPN Demand Statistics", Top10VPN (last updated 10 December 2025), online: www.top10vpn.com/research/vpn-demand-statistics/.