The "Segregate-and-Suppress" Approach to Regulating Child Safety Online

Eric Goldman**

28 STAN. TECH. L. REV. 173 (2025)

ABSTRACT

In an effort to protect children online, regulators around the country and the world are enacting laws that compel Internet publishers to age-authenticate every reader (minors and adults alike) and then require publishers to restrict minors' access to online content or resources. This Article calls these measures "segregate-and-suppress" laws.

Legally mandating differential treatment between minors and adults superficially sounds like common sense, but implementing this principle online leads to surprising and counterproductive outcomes. Requiring readers to authenticate their age exposes minors (and adults) to significant privacy and security risks, and it dramatically reshapes the Internet's functioning to the detriment of almost everyone. Further, due to the inherent tradeoffs involved, segregate-and-suppress laws inevitably harm some minors.

In other words, segregate-and-suppress laws seek to protect minors online by harming minors online. To avoid this paradox, regulators should deprioritize segregate-and-suppress laws and, instead, develop a wider and more thoughtful toolkit of online child safety measures.

---

* Editors' Note**:** This Article was written and edited prior to the publication of the Supreme Court's opinion in Free Speech Coalition v. Paxton, 606 U.S. ___ (2025). The policy arguments set forth in the Article are largely unaffected by the decision and remain relevant to this area of law.

** Associate Dean for Research, Professor of Law, Co-Director of the High Tech Law Institute, and Co-Supervisor of the Privacy Law Certificate, Santa Clara University School of Law. Website: http://www.ericgoldman.org. Email: egoldman@gmail.com. Thanks to the participants in the Santa Clara Law Fall 2024 Faculty Retreat and the Fall 2024 Stanford Law, Technology, and Science Colloquium, and Michael Asimow, Ashutosh Bhagwat, Alison Boden, Mary Rose Finnigan, Dina Goldman, Lisa Goldman, Yvette Joy Liebesman, Vance Lockton, Jess Miers, Irina Raicu, Pam Samuelson, Morgan Stevens, Kate Tummarello, and Shoshana Weissmann, for their feedback on this project. This article generally reflects developments through March 18, 2025.

TABLE OF CONTENTS

I. INTRODUCTION

It's one of the most pressing empirical questions of the digital age: does the Internet harm or benefit minors?[1] Psychology researchers are fiercely debating the topic, with no definitive resolution yet.[2]

Regulators aren't waiting for clear answers to this question. Instead, governments around the nation and the world are restricting and blocking minors' access to a wide range of Internet websites and apps that publish online content or provide online services (the Article calls these entities "publishers").[3] This regulatory urge to restrict minors' engagement with online publishers isn't new; Congress first passed such a law in 1996.[4] However, fueled by post-pandemic fears about children's heavy usage of and purported "addiction" to

---

[1] This Article uses the terms "child" and "minor" interchangeably. The legal definition of "child" varies by jurisdiction and by statute. While minors are often defined as children under eighteen, *cf.* KIDS ONLINE HEALTH AND SAFETY TASK FORCE, ONLINE HEALTH AND SAFETY FOR CHILDREN AND YOUTH: BEST PRACTICES FOR FAMILIES AND GUIDANCE FOR INDUSTRY 6 (2024) [hereinafter NTIA Report], https://perma.cc/6AJK-NHHJ ("various terms are used in reference to youth, including children, kids, teens, boys, girls, LGBTQI+ youth, and minors"), the Children's Online Privacy Protection Act (COPPA) applies only to children under thirteen. 15 U.S.C. § 6501(1). For simplicity, this Article uses "minor" or "child" to mean a person younger than whatever age cutoff is established in a segregate-and-suppress law.

[2] *Compare*, *e.g.*, AM. PSYCH. ASS'N, HEALTH ADVISORY ON SOCIAL MEDIA USE IN ADOLESCENCE 3 (2023) [hereinafter APA Advisory], https://perma.cc/66W3-VT54 (noting that "causal associations are rare" and "associations between adolescents' social media use and long-term outcomes . . . are largely unknown"), *and* Christopher J. Ferguson, *Do Social Media Experiments Prove a Link with Mental Health: A Methodological and Meta-Analytic Review*, 14 PSYCH. POPULAR MEDIA 201, 205 (2024) ("Currently, experimental studies should not be used to support the conclusion that social media use is associated with mental health . . . this undermines causal claims by some scholars (e.g., Haidt, 2020; Twenge, 2020) that reductions in social media time would improve adolescent mental health"), *with* JONATHAN HAIDT, THE ANXIOUS GENERATION (2024), PETER ETCHELLS, UNLOCKED (2024), Candice L. Odgers & Michaeline R. Jensen, *Annual Research Review: Adolescent Mental Health in the Digital Age: Facts, Fears, and Future Directions*, 61 J. CHILD PSYCH. & PSYCHIATRY 336, 336 (2020), *and* Mike Males, *Why the Latest CDC Teen Mental Health Report Is a Politically Inconvenient Bombshell for Crusading California Pols*, S.F. CHRON. (Dec. 18, 2024), https://perma.cc/N3D7-X6LY.

[3] The term "publisher" is the most accurate descriptor because the entities publish content (either their own content or third-party content) or services targeted by the suppression obligation. It also highlights the speech interests at risk. *See* Moody v. NetChoice, LLC, 603 U.S. 707, 710–11 (2024) (stating that social media services engage in expressive activities). Regulatory distinctions among publishers could exacerbate the regulation's constitutional problems. *See* NetChoice, LLC v. Bonta, No. 22-CV-08861, 2025 WL 807961, at *11 (N.D. Cal. Mar. 13, 2025) ("[W]here a statute's gateway coverage definition divides the universe into covered and uncovered business based on the type of content they publish, those statutes are content-based and subject to strict scrutiny.").

[4] The Communications Decency Act (CDA) was enacted as Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

the Internet, regulators have promulgated many new laws that claim to protect children online.[5]

The details of these regulations differ in big and small ways. There is no consistency in how the laws define minors, how the entities are supposed to determine who is a minor, what entities the laws regulate, and how the laws require those entities to restrict minors. To give a sense of this regulatory diversity, here are three examples of recently enacted laws[6]:

- Texas required websites to determine their readers' ages if one-third or more of their content databases consist of items that are "harmful to minors," such as pornography, and then restrict minors from accessing that material;[7]
- California made it illegal for "an addictive internet-based service or application to provide an addictive feed to a" minor;[8] and
- Australia categorically banned minors' use of social media.[9]

Despite this policy diversity, many child safety laws share two fundamental design attributes: (1) the laws require online publishers to distinguish minor readers[10] from adult readers (the "segregation"), and (2) the law then restricts

---

[5] *E.g.*, ERIC N. HOLMES, CONG. RSCH. SERV., LSB11020, ONLINE AGE VERIFICATION (PART I): CURRENT CONTEXT 1 (2023) [hereinafter CRS Report Part 1] ("One legislative response that has been particularly popular over the decades involves enacting laws that require or encourage website operators to ascertain the ages of their websites' users before letting them access content."); ANDY PHIPPEN, POLICY AND RIGHTS CHALLENGES IN CHILDREN'S ONLINE BEHAVIOUR AND SAFETY, 2017-2023 151 (2025) ("[T]here seems to be a legislative arms race to see who will 'ban' smartphones for young people with most rapidity."); Free Speech Coal., Inc. v. Skrmetti, No. 2:24-cv-02933, 2024 U.S. Dist. LEXIS 234100, at *3 (W.D. Tenn. Dec. 30, 2024) (referring to "the tidal wave of internet regulations sweeping across the country").

[6] More recent proposals intend to impose age authentication requirements for the sale of skin cream and dieting products. *See* Rindala Alajaji, *First Porn, Now Skin Cream? 'Age Verification' Bills Are Out of Control*, ELEC. FREEDOM FOUND. (Mar. 7, 2025), https://perma.cc/W2XE-CFY6.

[7] H.B. 1181, 88th Leg., Reg. Sess. (Tex. 2023). The Supreme Court granted certiorari for a constitutional challenge to the law in July 2024 and, in January 2025, heard oral arguments in the case. Free Speech Coal., Inc., v. Paxton, 95 F.4th 263 (5th Cir. 2024), *cert. granted*, 144 S. Ct. 2714 (2024). However, the Supreme Court's review hasn't dissuaded other state legislatures. In 2024, eleven states passed bills similar to that of Texas. *2024 Age-Verification Legislative Scorecard*, FREE SPEECH COAL., https://perma.cc/EVY6-ESHY (archived May 4, 2025).

[8] CAL. HEALTH & SAFETY CODE § 27001(a) (West 2025), enacted in the Protecting Our Kids from Social Media Addiction Act of 2024.

[9] *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) (Austl.) https://perma.cc/4S3E-LSGY (archived May 4, 2025).

[10] This Article refers to "readers" of online publishers' content. However, when the online

minors' access to the publishers' online resources or services (the "suppression"). Because this regulatory genre lacks a well-accepted name,[11] this Article refers to such measures as "segregate-and-suppress" laws.

Superficially, online segregate-and-suppress laws resemble the venerable offline laws that make distinctions between minors and adults. However, perhaps counterintuitively, translating those offline principles to the Internet is not simple or straightforward.[12]

Instead, compared to the often benign process of authenticating age offline, doing age authentication online (the segregation requirement) imposes substantial harms on everyone—including, counterproductively, the minors that the laws are intended to protect.[13] Online age authentication exposes minors (and adults) to heightened privacy and security risks. Furthermore, the online authentication process acts as a technical barrier to reader access that will dissuade readers from navigating around the Internet. This reduced traffic will affect publishers' revenues and force them to bear higher authentication costs. Collectively, these economic forces will drive some publishers offline, making less content and fewer services available to readers (minors and adults alike), and the remaining publishers will erect more paywalls, exacerbating digital divides. Most insidiously, online age authentication builds an infrastructure that facilitates government surveillance of and control over the public.

These harms are not present with offline age authentication; they are unique to online age authentication. This is an example of Internet "exceptionalism," where offline rules should not extend to online activities because electronic mediation creates qualitatively different outcomes.[14]

---

publisher permits readers to post their own content, these "readers" are also "authors" whose rights to speak are restricted.

[11] Because standardized terminology doesn't exist, synonyms may include "restrictions" and "paternalistic" interventions. *See, e.g.*, Jinkyung Katie Park et al., *It's Still Complicated: From Privacy-Invasive Parental Control to Teen-Centric Solutions for Digital Resilience*, 22 IEEE SEC. & PRIV. 52, 53 (2024).

[12] SCOTT BABWAH BRENNAN & MATT PERAULT, CTR. FOR GROWTH & OPPORTUNITY AT UTAH ST. UNIV., KEEPING KIDS SAFE ONLINE: HOW SHOULD POLICYMAKERS APPROACH AGE VERIFICATION? 1 (2023) [hereinafter CGO Report], https://perma.cc/BHC7-L2EJ ("There is nothing simple or straightforward about determining the age of internet users.").

[13] ANDY PHIPPEN, POLICY AND RIGHTS CHALLENGES IN CHILDREN'S ONLINE BEHAVIOUR AND SAFETY 2 (2017) (discussing the regulatory "online safeguarding dystopia," the ironic process by which regulators require minors to give up rights to protect minors' rights).

[14] See *generally, e.g.*, Mark Tushnet, *Internet Exceptionalism: An Overview from General Constitutional Law*, 56 WM. & MARY L. REV. 1637 (2015).

Furthermore, in many cases, due to the heterogeneity of minors' needs, suppression regulations may benefit some portion of the affected population—but at the expense of other minor subpopulations. This is another way that laws claiming to protect all children actually harm many of them.

This Article thus raises a conundrum: In light of the ways that segregate-and-suppress laws harm minors, why do they remain so popular? In a well-functioning governance system, the answer would be that regulators thoughtfully concluded that the benefits of segregate-and-suppress laws justify the many harms they create. Unfortunately, this is not the world we live in. Without a solid basis to conclude that the benefits of segregate-and-suppress laws outweigh the harms, the laws put minors—along with adults and the Internet generally—at grave risk. This should raise red flags about the ongoing regulatory embrace of segregate-and-suppress laws.

This Article proceeds in four parts. Part I defines the segregate-and-suppress policy approach. Part II explains how the segregation process harms minors, adults, and the Internet. Part III explains how suppression requirements inevitably harm subpopulations of minors. Part IV explores several better policy approaches. The Article's conclusion considers why regulators keep making problematic policy choices.

II. AN INTRODUCTION TO SEGREGATE-AND-SUPPRESS LAWS

Regulators have a virtually limitless range of policy options to address child safety online, but regulators routinely prioritize the segregate-and-suppress approach. This Part explains how segregate-and-suppress laws work, including their key design features. This Part also references some policy problems raised by the laws, a topic Part II will address in more detail.

A. Stage 1: The Segregation

A typical Internet publisher serves a mixed reader population consisting of both adult and minor readers. Unless and until the Internet publisher takes some action to ascertain readers' ages, the publisher doesn't know which readers are adults and which are minors.[15] A segregation requirement compels

[15] If a publisher caters exclusively (or nearly so) to minors, it might not do age authentication at all. Instead, it could assume that all of its readers are underage. In that case, a segregate-and-suppress law would compel the publisher to subject every reader to the required suppression. For example, publisher offerings that are considered "directed to children"

publishers to affirmatively make this age determination. Because the publisher must put all readers through the authentication process (to identify the minors), age authentication mandates affect minors and adults alike.[16]

1. What Is Age Authentication?

Definition. This Article uses the term "age authentication" to describe the category of all processes used to determine readers' ages. Like almost everything in this field, the category descriptor is not standardized.[17] An authentication process can achieve different levels of precision about a reader's age:

- "Age assurance" means that a reader is confirmed as an adult and not a minor, without any further precision about the person's age.[18]
- "Age estimation" means that the reader's age is estimated within a margin of error, e.g., within a range of plus or minus two years.[19] The term "age assessment" is sometimes used.
- "Age verification" means that a reader's exact age is determined.[20]

---

must comply with the Children's Online Privacy Protection Act (COPPA), regardless of the publishers' knowledge about their readers' ages. *See* 16 C.F.R. pt. 312.2 (2017).

[16] Letter from Hayley Tsukayama, Assoc. Dir. of Legis. Activism, Elec. Frontier Found. (E.F.F.), to Leticia James, N.Y. Att'y Gen. (Sept. 30, 2024) regarding the Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 1500 et seq [hereinafter EFF Letter], https://perma.cc/7ECN-8Q8M ("Age verification requirements don't just impact young people."); SARAH FORLAND ET AL., OPEN TECH. INST., AGE VERIFICATION: THE COMPLICATED EFFORT TO PROTECT YOUTH ONLINE (2024) [hereinafter OTI Report], https://perma.cc/5967-JMAV ("[A]ge verification laws impact all users, not just youth.").

[17] The nomenclature in this area is confusing and used inconsistently. As the Congressional Research Service observed, "[t]here are no universally recognized legal definitions for these various terms . . . the use of these terms is not uniform." CRS Report Part 1, *supra* note 5, at 2.

[18] In Europe, the term "age assurance" is sometimes used to describe the category of "age authentication" options. *See, e.g.*, MARTIN SAS & JAN TOBIAS MÜHLBERG, GREENS/EFA IN THE EUROPEAN PARLIAMENT, TRUSTWORTHY AGE ASSURANCE? A RISK BASED EVALUATION OF AVAILABLE AND UPCOMING AGE ASSURANCE TECHNOLOGIES FROM A FUNDAMENTAL RIGHTS PERSPECTIVE 14 (2024) [hereinafter Greens Report], https://perma.cc/PU5Y-2HYD ("Age assurance is an umbrella term for both age verification and age estimation solutions," which is how the term is used in the UK Online Safety Act 2023); *see also* CGO Report, *supra* note 12, at 3 (adopting this approach).

[19] An error rate of +/- 2 years might sound precise, but it still produces many false positives and negatives. *See* Free Speech Coal., Inc., v. Rokita, 738 F. Supp. 3d 1041, 1066 n.21 (S.D. Ind. 2024) (discussing how a 1.5-year mean error may "pose too high an error rate").

[20] Sometimes "age verification" is used to describe the category instead of "age authentication." *See* CRS Report Part 1, *supra* note 5, at 2 ("[A]ge verification" refers to "methods for estimating or determining a user's age with varying levels of certainty.").

This Article doesn't further distinguish between these age authentication types because they all create the harms discussed in Subpart II.A.[21]

Instead of authenticating readers' ages, publishers can voluntarily ask readers to self-report their ages so that they can deny access to minors,[22] a process sometimes called "age-gating," "self declaration," "age declaration," or "self attestation."[23] Without further verification, reader self-reporting isn't credible evidence of the reader's age because minors are willing, and have incentives, to misreport.[24] As a result, self-reporting does not satisfy any age authentication mandate. As one U.K. government official said, "Self-declaration of a child's age is clearly completely insufficient."[25]

Constructive Knowledge About Age. Instead of compelling publishers to affirmatively authenticate age, regulators can reach the same result by imposing suppression obligations if the publisher has sufficient awareness that a reader is a minor.[26]

---

[21] Still, publishers care a lot about the degree of accuracy required by regulators, the consequences of making (inevitable) authentication mistakes, and each option's implementation costs.

[22] For example, online liquor vendors may voluntarily impose self-reporting interstitial screens to access their websites to signal that they do not welcome underage visitors. *E.g.*, Adam E. Barry et al., *Characteristics and Effectiveness of Alcohol Website Age Gates Preventing Underage User Access*, 56 ALCOHOL & ALCOHOLISM 82, 82 (2021); FED. TRADE COMM'N, SELF-REGULATION IN THE ALCOHOL INDUSTRY ii (2014), https://perma.cc/F5A2-MRVT. An online alcohol retailer will do more rigorous age authentication before actually delivering any ordered alcohol, such as requiring the delivery service to verify the recipient's adult status before completing the delivery.

[23] Greens Report, *supra* note 18, at 15 ("'Age declaration' refers to measures requesting users to confirm their age by declaring how old they are, but without providing further evidence of their claim.").

[24] danah boyd et al., *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act'*, 16 FIRST MONDAY 2 (2011), https://perma.cc/86GS-B99D; Liv McMahon et al., *'It's So Easy to Lie': A Fifth of Children Use Fake Age on Social Media*, BBC (Nov. 27, 2024), https://perma.cc/TN5Z-TTZ7 ("22% of eight to 17 year olds lie that they are 18 or over on social media apps.").

[25] McMahon et al., *supra* note 24 (quoting Ian McCrae, Director of Market Intelligence of U.K.'s Ofcom); *see* OECD, TOWARDS DIGITAL SAFETY BY DESIGN FOR CHILDREN: OECD DIGITAL ECONOMY PAPERS NO. 363, at 31 (2024) [hereinafter OECD Report], https://perma.cc/QC4V-L6MM ("[M]ere self-declaration of age is often not regarded as an effective age assurance technique as it can be easily misused.").

[26] *See* TIM BERNARD, STAN. CYBER POL'Y CTR., LEGISLATIVE APPROACHES TO COMBATING ONLINE HARMS TO CHILDREN (2024), https://perma.cc/78X8-TFVT (enumerating ways legislatures have described publishers' scienter about minors' ages beyond "actual knowledge"); Molly Buckley, *Fighting Online ID Mandates: 2024 in Review*, ELEC. FREEDOM FOUND. (Dec. 31, 2024), https://perma.cc/73C9-LY25 ("We call these bills 'implicit age verification mandates' because, though they might expressly deny requiring age verification, they still force

For example, the Children's Online Privacy Protection Act (COPPA) applies to any publisher who "has actual knowledge that it is collecting personal information from a child."[27] When the legal standard is "actual knowledge" that a reader is a minor, publishers can manage their likelihood of knowing readers' ages, such as by not voluntarily asking readers to report their age or refusing to provide access to any reader who self-reports as a minor.

To prevent these countermoves, regulators can use a "constructive knowledge" standard for publishers' awareness about readers' age. For example, COPPA also applies to a "website or online service directed to children."[28] The law enumerates multiple factors that signal when a publisher is "directed to children."[29]

Constructive knowledge scienter standards affect a much wider range of publishers than an actual knowledge standard. This has not been a major issue with COPPA because COPPA only applies to minors "under 13."[30] Many mainstream publishers don't regularly cater to preteens, so they usually can disregard COPPA's obligations.

When a segregate-and-suppress law defines minors to include teens and imposes a constructive knowledge standard, the law dramatically expands the universe of potentially affected publishers. Most mainstream publishers have some teens in their audience even if their primary audience is older, so the constructive knowledge standard forces those publishers to comply with the law, even when the true number of minors in their audience is trivial.[31]

Imagine an enforcement action where a regulator claims that a publisher had constructive knowledge that some minors were in its audience. The regulator will marshal all evidence that was available, at least in theory, to the publisher about its readers' ages—even if the publisher disregarded the evidence (the regulator will counter that the publisher was "willfully blind"), and even if the evidence was inconclusive about readers' ages. This

---

platforms to either impose age verification measures or, worse, to censor whatever content or features deemed 'harmful to minors' for all users—not just young people—in order to avoid liability.").

[27] 15 U.S.C. § 6502(a)(1).

[28] *Id.*

[29] *Id.* § 6501(10).

[30] *Id.* § 6501(1).

[31] *See* ASHLEY JOHNSON, INFO. TECH. & INNOVATION FOUND., HOW TO ADDRESS CHILDREN'S ONLINE SAFETY IN THE UNITED STATES 9 (2024) [hereinafter ITIF Report], https://perma.cc/3LZ8-NXRR ("[S]witching from an actual knowledge standard to an implied knowledge standard would create a minefield of potential liability for online services.").

enforcement vector puts publishers in a bind, because they will essentially have to disprove their knowledge about having minors in their audience.

To avoid this legal exposure, some publishers will extend the suppression requirement to all readers, both minors and adults. Other publishers will deploy age authentication across their entire audience, so that they can be certain about readers' ages and avoid defending a charge that they had constructive knowledge of minors' ages. In this way, age authentication provides a de facto safe harbor to a constructive knowledge standard[32]—a safe harbor that many publishers don't want to deploy but will feel they need to.

This pressure on publishers to use age authentication as a safe harbor is one of the many ways that segregate-and-suppress laws lead to counterproductive outcomes. As discussed in Part II, rolling out age authentication drives many publishers to collect more personal information from minors than the publishers would voluntarily choose to collect, and those data collection efforts put minors at greater risk.[33]

2. Methods for Authenticating Readers' Ages Online

There are many ways to authenticate age online. Some laws mandate or prohibit specific approaches,[34] but most require publishers to figure it out themselves.[35] Giving publishers choices among multiple options ordinarily sounds like a positive situation—but not in this case, because all of the options are problematic. As the Electronic Frontier Foundation (EFF) explained:

---

[32] For example, age authentication was a safe harbor for the law restricting the sale of pornography to minors at issue in Ginsberg v. New York, 390 U.S. 629 (1968).

[33] Memorandum from Maureen Mahoney, Deputy Dir. Pol'y & Legis., Cal. Priv. Prot. Agency, to the Cal. Priv. Prot. Agency Bd. 7 (May 3, 2024) [hereinafter Mahoney Memo], https://perma.cc/AGT5-KNUY (noting that without an actual knowledge standard, "additional protections for children online could come at the expense of other Californians' privacy, by incentivizing additional data collection for all Californians to verify the user's age" and that "while the bill does not require businesses to collect additional information to verify age, by removing the actual knowledge standard, businesses will have strong incentives to do so"); *see also* NetChoice, LLC v. Bonta, No. 22-CV-08861, 2025 WL 807961, at *21 (N.D. Cal. Mar. 13, 2025) ("The State's argument is grounded in an assumption that greater data privacy for children means greater security and well-being. As NetChoice points out, however, the State ignores that the age estimation requirement will require businesses to collect private information that users may not wish to share.").

[34] For example, Australia's under-sixteen social media ban restricts social media from using government IDs to authenticate age. *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) para. 63DB(1)(a), https://perma.cc/4S3E-LSGY (archived May 4, 2025).

[35] CGO Report, *supra* note 12, at 2 ("[M]any of the new regulations . . . provide only minimal guidance about how platforms or apps should verify a user's age.").

> [Authentication] methods don't each fit somewhere on a spectrum of "more safe" and "less safe," or "more accurate" and "less accurate." Rather, they each fall on a spectrum of "dangerous in one way" to "dangerous in a different way." . . . [E]very solution has serious privacy, accuracy, or security problems.[36]

Thus, there is no "preferred" or "ideal" way to do online age authentication.[37] Among the problematic options for doing online age authentication, the most popular options today are document reviews and visual inspections.

a. Document Review

Governments issue IDs that authenticate the resident's personal information, such as their name, home address, and age. Offline retailers and others can, and routinely do, check government-issued IDs to authenticate the holder's age, such as when a liquor store checks a buyer's driver's license to confirm that the buyer is old enough to purchase alcohol.

To comply with segregate-and-suppress laws, online publishers can attempt to replicate this offline document review process by asking readers to present their government-issued IDs before permitting readers to access suppressed resources, so that the publisher can confirm each reader's age using the presented document.[38]

A document review authentication process immediately creates a major obstacle for the millions of U.S. adults who do not have government-issued IDs.[39] As one court said, making document review a prerequisite to online engagement acts like "a complete block to adults who wish to access adult

---

[36] EFF Letter, *supra* note 16, at 7.

[37] *See* CGO Report, *supra* note 12, at 1–2 ("In selecting a method to identify a child, platforms and regulators will always be forced to prioritize some criteria and deprioritize others . . . . Each method . . . involves some tradeoff between privacy, security, accuracy, usability, and legality . . . .").

[38] Subpart II.C further explains why online document review has different implications than offline document review.

[39] MICHAEL J. HANMER & SAMUEL B. NOVEY, UNIV. OF MD. CTR. FOR DEMOCRACY & CIVIC ENGAGEMENT, WHO LACKED PHOTO ID IN 2020?: AN EXPLORATION OF THE AMERICAN NATIONAL ELECTION STUDIES 3 (2023), https://perma.cc/V5M8-UPAS (observing that in 2020, "[n]early 29 million voting-age U.S. [c]itizens did not have a non-expired driver's license and over 7 million did not have any other form of non-expired government issued photo identification"); Michael Sivak, *Choosing Not to Drive: A Transient or a Permanent Phenomenon?*, GREEN CAR CONG. (Feb. 2, 2019), https://perma.cc/TRA3-9BYL (finding that in 2017, 38% of 18-year-olds did not have a driver's license).

material [online] but do not" have the necessary documents.[40] These barriers will disproportionately block access for minorities, young adults, and marginalized subpopulations.[41] As segregate-and-suppress laws proliferate, uncredentialed adults will become casualties of a digital divide exacerbated by age authentication mandates.

Some governments are rolling out digital IDs that function like traditional government-issued IDs but are stored on a computing device.[42] Segregate-and-suppress laws could designate digital IDs as a method of satisfying the age authentication requirement.[43] Digital IDs potentially reduce one privacy problem, because they can be configured to communicate only age information to publishers without sharing the other sensitive information customarily found on government-issued IDs.[44] However, digital IDs raise numerous other concerns. First, the infrastructure for their adoption and usage is still nascent. Second, some people won't adopt digital IDs if they have a choice (in response to privacy and security concerns, among others). Third, governments may be able to gather data about each constituent's online activities by monitoring which publishers access the digital ID and could weaponize this information against people based on culture wars (such as research into out-of-state abortions[45] or gender-affirming surgery)—another reason why people may be fearful about using digital IDs. As a result, it is not clear if and when digital IDs will solve any structural problems with age authentication.

---

[40] PSInet, Inc. v. Chapman, 362 F.3d 227, 237 (4th Cir. 2004); *see also* Am. Booksellers Found. v. Dean, 342 F.3d 96, 99 (2d Cir. 2003).

[41] EFF Letter, *supra* note 16, at 2; *see also* ALICE MARWICK ET AL., CTR. FOR INFO. TECH. POL'Y, CHILD ONLINE SAFETY LEGISLATION: A PRIMER 30 (2024), https://perma.cc/3XTF-CFUS ("[W]idespread age verification would negatively impact access to information for marginalized groups.").

[42] *E.g.*, Ash Johnson, *The Path to Digital Identity in the United States*, INFO. TECH. & INNOVATION FOUND. (ITIF) (Sept. 23, 2024), https://perma.cc/9M6H-HX79 ("Currently, 13 states offer mobile driver's licenses, a type of digital ID, and have faced challenges such as interoperability, accessibility, usability, and trust.").

[43] *See, e.g.*, La. Rev. Stat. § 9:2800.29(D)(8)(a).

[44] ID holders can use software, such as Apple's, that will further reduce the specificity of the information transferred to the authenticator. *See generally* APPLE, HELPING PROTECT KIDS ONLINE (2025), https://perma.cc/8KM3-YAWT.

[45] *See, e.g.*, Complaint, Texas v. U.S. Dep't of Health & Hum. Servs., No. 5:24-cv-00204 (N.D. Tex. Sept. 4, 2024) (in which Texas sought out-of-state medical records to see if Texas residents obtained legal abortions in other states).

b. Visual Inspection

Another way to determine a person's age is just by looking at them. People do this many times every day. It's a well-practiced skill that is second-nature to most people.

Offline entities routinely use visual inspections to authenticate age. For example, based solely on visual inspection, offline liquor retailers' sales clerks can quickly assess if potential buyers are clearly adults or clearly minors, and then conduct a secondary age authentication review (such as inspecting a government-issued ID) only for buyers who are neither.[46]

Online visual inspections attempt to replicate this everyday process.[47] For example, a reader could present their face to the online publisher's human representative who could conduct a real-time visual assessment, just like the liquor store clerk does. More likely, publishers will use machine learning to make automated determinations of a reader's age based on the reader's face or other physical attributes. If forced to age-authenticate, consumers may prefer visual inspections over other methodologies. Facebook said that when given a menu of age-authentication options, 81% of Facebook Dating users elected to provide a video selfie.[48]

Superficially, online visual inspection can make pretty good estimates of people's ages. [49] One digital identification vendor, Yoti, claims that its "technology is accurate for 6 to 12 year olds with a mean absolute error (MAE) of 1.36 years and of 1.52 years for 13 to 19 year olds."[50]

---

[46] *See* Lawrence Lessig, *The Law of the Horse: What Cyber Law Might Teach*, 113 HARV. L. REV. 501, 504 (1999) ("Age in real space is a self-authenticating fact"). For example, I haven't been "carded" in many, many years.

[47] However, digital codifications of human processes inevitably encounter some of the same challenges. *See* Zahra Stardust et al., *Mandatory Age Verification for Pornography Access: Why It Can't and Won't 'Save The Children'*, 11 BIG DATA & SOC'Y 1, 4 (2024),("Because age estimation by human beings is already unreliable, age estimation by algorithms is inevitably fraught").

[48] Erica Finkle, *Bringing Age Verification to Facebook Dating*, META NEWSROOM (Dec. 5, 2022), https://perma.cc/2GSR-N4GV; *see also* Iain Corby, *A Summary of the Achievements and Lessons Learned of the euCONSENT Project and What Comes Next*, EUCONSENT (Dec. 7, 2022), https://perma.cc/2MZQ-T3BT ("facial estimation was by far the most popular age verification option, preferred by 68% of all participants").

[49] KAYEE HANAOKA ET AL., FACE ANALYSIS TECHNOLOGY EVALUATION: AGE ESTIMATION AND VERIFICATION 2 (2024), https://perma.cc/KAZ3-3LVF.

[50] YOTI LTD., YOTI AGE ESTIMATION WHITE PAPER (2022), https://perma.cc/U82L-5YBZ. A 1.5-year error rate may sound fairly precise, but it produces many Type I/Type II errors where seventeen-year-olds are classified as nineteen and vice-versa.

As impressive as that may sound, the error rates are still problematic. For individuals around the age of majority, age authentication "algorithms are simply not very accurate" and "could result in an enormous number of inaccurate estimates—both false positives and false negatives—for users within several years of the required age of eighteen."[51] In other words, when the visual inspections are asked to make the hardest judgment calls between minors and adults, they are not up to the task.

Furthermore, inspection accuracy is affected by variables such as demographics (e.g., race and gender),[52] image quality, and whether the subject wears eyeglasses.[53] These biases raise further concerns about discriminatory online treatment and the potential for additional digital divides. Also, the visual inspection requirement can be another access barrier for visually impaired readers (who may find it hard to compose the required screen display) or readers who lack the required camera equipment.

Even if visual inspection error rates are low, every error creates significant problems for readers and publishers. Misclassifications can have dramatic consequences for readers and authors. For example, when an online authentication process misclassified an adult user with dwarfism as a minor, the publisher permanently deleted over 500 videos she had posted.[54] To mitigate these problems, publishers will need to offer a way to correct errors, such as providing a process for readers to "appeal" their classification. However, error correction mechanisms increase publishers' authentication costs (discussed more in Section II.A.4).

c. Some Other Age Authentication Methods

Document reviews and visual inspections are just two of the many possible methods for authenticating age online. However, the other options are structurally flawed, just like the leading options. Some other possibilities:[55]

---

[51] EFF Letter, *supra* note 16, at 11.

[52] *E.g.*, Vítor Albiero et al., *Gendered Differences in Face Recognition Accuracy Explained by Hairstyles, Makeup, and Facial Morphology*, 17 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 127 (2022), https://perma.cc/XC3C-WUCD; Stardust, *supra* note 47, at 7–8; Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://perma.cc/76YQ-9FSG.

[53] Hanaoka et al., *supra* note 49.

[54] *See* Drew Harwell, *A Booming Industry of AI Age Scanners, Aimed at Children's Faces*, WASH. POST (Aug. 7, 2024), https://perma.cc/H4CF-9YGJ.

[55] For a more comprehensive review of possible options, *see* OTI Report, *supra* note 16 ("Age Assurance and Age Verification" section).

Device Authentication. Instead of authenticating individual readers, a device can be authenticated at the time of purchase as being owned by an adult or minor.[56] Device authentication solves one problem, in that online publishers interacting with the device can rely upon the device's self-reported age status rather than conducting its own age authentication. At the same time, device authentication creates a host of new problems: the device seller still has to do the age authentication, with the attendant privacy and security risks outlined in Subpart II.A; multiple users—some adults, some minors—may share a device;[57] devices can be easily sold or traded to unauthenticated users; users may have other devices that are not similarly authenticated; and broadcasting the device user's indicator about age to publishers could increase the risk of privacy and security violations, especially when publishers (or their vendors) combine that information with other data about the user.

Capacity Testing. A publisher can ask readers to perform tasks, or demonstrate knowledge, that signal adulthood. This method does not account for differential development rates among people, and (unless combined with identity authentication) it can be easily gamed by having an older person to take the test on the minor's behalf.

Data Mining of Past Activities. A person's age can be estimated by reviewing their past online activities, on the theory that an adult's activities will look different than a minor's activities. For example, Google has said that, in 2025, it will "begin testing a machine learning-based age estimation model in the U.S."[58] According to one report:

---

[56] *See*, *e.g.*, *Statement on Age Verification*, INT'L CTR. FOR MISSING & EXPLOITED CHILD. (ICMEC) (June 27, 2024), https://perma.cc/DL89-65Z2.

[57] MICHAL LURIA & ALIYA BHATIA, CTR. FOR DEMOCRACY & TECH., THE KIDS ARE ONLINE: RESEARCH-DRIVEN INSIGHTS ON CHILD SAFETY POLICY 13 (2025), https://perma.cc/H6TN-JB4B [hereinafter CDT Report] ("35% of multi-person households shared a computer or a laptop and 10% of multi-person households shared a smartphone, with 58% of those sharing it at least once every day. Sometimes a device isn't shared per-se, but an adult (e.g., a parent) may give their own device to a child and by doing so grant them access to the internet").

[58] Jen Fitzpatrick, *New Digital Protections for Kids, Teens and Parents*, GOOGLE: THE KEYWORD (Feb. 12, 2025), https://perma.cc/2A58-EUCW. Meta has taken similar steps. According to one report, Meta "can now use AI to scan for signals that may indicate a user is under 18. For example, if a user says they're 18 when creating an account but someone on the app tells them 'Happy 14th birthday,' Instagram can use that to inform their real age." Emma Roth, *Instagram Is Putting Every Teen into a More Private and Restrictive New Account*, VERGE (Sept. 17, 2024), https://perma.cc/3UCW-DM66. This example raises obvious concerns; it is vulnerable to false positives (such as a friend's joke about age) and malicious brigading attacks (e.g., malefactors making a posting to fool the algorithm with the goal of restricting the targeted user's account).

> The age estimation model will use existing data about users, including the sites they visit, what kinds of videos they watch on YouTube, and how long they've had an account to determine their age. When it detects a user may be under 18, Google will notify them that it has changed some of their settings and will offer information about how users can verify their age with a selfie, credit card, or government ID.[59]

The data-mining approach has a number of obvious problems, including the difficulty making precise age estimates (especially for individuals right around the cutoff), the ability of minors to fool the test by injecting adult-like activities into the mined data, the heightened privacy and security risks from data mining, and the creepiness of the process.[60]

Third-Party Reporting. Instagram experimented with "social vouching," which "allows you to ask mutual followers to confirm how old you are," but abandoned the test after a few months.[61] Among other problems, this approach is vulnerable to coordinated brigading attacks where the users all agree to lie.

Credit Cards. The 1990s-era segregate-and-suppress statutes[62] treated the possession of a valid credit card number as proof of adult status.[63] That assumption is clearly outdated now. For example, one 2019 study found that 17% of minors aged 8-14 have valid credit card numbers.[64]

d. Who Does the Authentication?

Most publishers won't perform age authentication themselves. Building and operating a complex and error-prone function like age authentication won't be their core competency. Instead, many will outsource the process to a

---

[59] Emma Roth, *Google Will Use Machine Learning to Estimate a User's Age*, VERGE (Feb. 12, 2025), https://perma.cc/3FPY-LSEK.

[60] In response to TikTok testifying in Congress that it assessed users' ages by making inferences from their online activities, one Congressmember immediately responded "That's creepy!" Lisa Remillard (@lisaremillard), TIKTOK (Mar. 23, 2023), https://perma.cc/2CPS-GA89 (archived May 7, 2025).

[61] *Introducing New Ways to Verify Age on Instagram*, INSTAGRAM (June 23, 2022), https://perma.cc/6QJQ-UT93.

[62] *See* Free Speech Coalition, Inc. v. Rokita, 738 F. Supp. 3d 1041 n.21 (S.D. Ind. 2024) ("credit card verification is not effective at ensuring a user is over the age of 18").

[63] Communications Decency Act of 1996, Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, §§ 501–61, 110 Stat. 56, 133–43; Child Online Protection Act, Pub. L. 105-277, 112 Stat. 2681 (1998).

[64] Herb Weisbaum, *How Young is Too Young for a Kid to Have a Credit Card?*, NBC NEWS (Aug. 6, 2019), http://perma.cc/9QEA-793W.

third-party age authentication vendor.[65] Indeed, some laws may require publishers to outsource age authentication as a way of (superficially) abating some of the heightened privacy and security risks of publishers having direct access to their readers' authentication data that can be combined with other datasets.

As more jurisdictions enact segregate-and-suppress laws, it has fueled a burgeoning industry of specialist authentication vendors. An industry group, the Age Verification Providers Association (AVPA), lists 28 member organizations.[66] Authentication services could also be offered by offline enterprises that conduct in-person document review to authenticate age (similar to how notaries do in-person identity authentication) and issue some token or certification that readers can present to publishers about their age.[67]

Another potential source of authentication vendors are existing services that provide account login credentialing services to publishers (sometimes called "federated identity"),[68] such as the OAuth standard[69] that allows services to let their readers' login credentials function as logins at qualifying third-party services. These services could expand their credentialing offerings to include age authentication. For example, many Internet publishers already enable readers to log into a publisher's services using the reader's Facebook or Google credentials, and Facebook and Google (who already know many readers' ages) could include age authentication as part of the authorization. Apple is instituting a related concept: it will collect parent-reported ages for children and then make available age range information for those children to app developers (using Apple's "Declared Age Range API").[70]

Publishers' outsourcing of the age authentication process to a third-party vendor may keep the reader's authentication information out of the publishers' databases. That might be viewed as a pro-privacy outcome. On the other hand,

---

[65] ENGINE, MORE THAN JUST A NUMBER: HOW DETERMINING USER AGE IMPACTS STARTUPS 7 (2024) [hereinafter Engine Report], https://perma.cc/ELN5-3BRN ("no startup will create their own age-verification system, and will instead rely on third-party providers. Building a reliable in-house system would require the same resources as they've invested developing their actual product."). As an analogy, laws requiring websites to provide readers with choices about cookie settings has spawned an industry of third-party cookie consent management vendors.

[66] *Members*, AGE VERIFICATION PROVIDERS ASSO., https://perma.cc/M555-PMVC (archived May 7, 2025); *see also Best Age Verification Software of 2025*, SLASHDOT, https://perma.cc/CS8Z-ABLJ (archived May 27, 2025).

[67] *See*, *e.g.*, Commission Nationale Informatique & Libertés, *Age Verification by a Trusted Third Party* (illustration), https://perma.cc/57LA-2MEY.

[68] *Federated Identity,* WIKIPEDIA, https://perma.cc/A2VP-FJPS (archived May 7, 2025).

[69] OAUTH, https://perma.cc/9M4M-M38H (archived May 7, 2025).

[70] APPLE, *supra* note 44.

the outsourcing potentially creates new privacy and security risks. For example, an outsourced vendor will have lots of information about readers' online destinations (based on which publishers request authentication for that reader). The vendor that could use that data to build highly valuable consumer profiles that would jeopardize readers' privacy.

App stores also could function as authentication providers by authenticating their customers' ages and blocking certain app downloads by minors. Superficially, app store age authentication could ensure that all people installing restricted app from that app store will be confirmed as adults, permitting the app publishers to avoid any segregation obligations. Some advocates, including some publishers, have been pushing regulators to adopt this approach rather than placing the authentication burden on individual publishers. [71] Regulators are embracing mandatory app store age authentication as well.[72]

Unfortunately, app store age authentication doesn't really solve any problems discussed in this Article.[73] First, it doesn't solve the shared device problem when the device is used by both minors and adults. Second, minors can install apps from sources other than app stores, thus bypassing the app store authentication process. Third, minors have access to devices, like desktop and laptop computers, that don't get their software from app stores, also bypassing the app store authentication process. Fourth, many of the content or services that regulators seek to suppress can be accessed via the web without installing the publisher's app, and that direct access wouldn't be affected by the app store age authentication mandate. Fifth, the app stores as authenticators (or their vendors) create all of the privacy and security risks discussed in Part II.[74] On top of all that, to reduce their legal risk, app stores will interpret their

---

[71] Antigone Davis, *Parenting in a Digital World Is Hard. Congress Can Make It Easier.*, META (Nov. 15, 2023), https://perma.cc/B9CU-UZRK; Cristiano Lima-Strong & Cat Zakrzewski, *Meta Gains Steam in Its Push to Make Apple, Google Verify Users' Ages*, WASH. POST (Nov. 21, 2024), https://perma.cc/FU7X-ZBDX; Shannon Sollitt, *'Unideal Situations With Social Media': Utah Kids Lobby to Require App Stores to Verify Age.*, SALT LAKE TRIB. (Jan. 29, 2025), https://perma.cc/2GSQ-JAC6.

[72] *See*, *e.g.*, S. 142, 2025 Leg., Gen. Sess. (Utah 2025).

[73] Josh Withrow & Shoshana Weissmann, *No, Conscripting the App Stores Doesn't Solve the Problems with Age Verification*, R STREET (Jan. 29, 2025), https://perma.cc/P349-FDRA.

[74] In addition, the transfer of age authentication information to app developers creates the potential for developer misuse. *See* Kareem Ghanem, *Google's Legislative Proposal for Keeping Kids Safe Online*, GOOGLE: THE KEYWORD (Mar. 12, 2025), https://perma.cc/TYS7-RZXZ (the Utah App Store Accountability Act "requires app stores to share if a user is a kid or teenager with all app developers . . . without parental consent or rules on how the

suppression obligation to minimize their liability, leading to overblocking of minors' access to apps.

A variation on this theme is device-level authentication, or imposing the age authentication mandate on every Internet-enabled device manufacturer and provider of operating systems for those devices.[75] This approach would reach more devices than an app store authentication requirement—indeed, it may be overinclusive because so many devices are now Internet-enabled—but it otherwise suffers from all of the same problems.

3. The Relationship Between Age Authentication and Identity Authentication

Age authentication can be done without authenticating the person's identity. For example, if an authenticator is using online face scans to authenticate age, the authenticator doesn't necessarily need to know whose face it is reviewing; it simply needs to decide if the reader being assessed meets the age cutoff before allowing them to access the restricted resources.

Despite this, authenticators will routinely couple age authentication with identity authentication. Without doing simultaneous identity authentication, many age authentication processes will be too error-prone or easy to fool, trick, or game.[76] For example, without doing identity verification, a visual inspection

---

information is used. That raises real privacy and safety risks, like the potential for bad actors to sell the data or use it for other nefarious purposes"). As with the privacy and security risks of age authentication, any legal restrictions on what app developers do with the age data would be hard to enforce, especially with respect to any malefactor developers.

[75] Device-level age authentication is the preferred approach of the adult entertainment industry, because it takes them out of the age authentication equation. *See FSC Supports North Dakota Age-Verification Bill*, FREE SPEECH COAL. (Jan. 28, 2025), https://perma.cc/FA2M-UH7R.

[76] Harwell, *supra* note 54 ("users have shared tips on how to print out fake IDs, buy other people's selfie videos or apply makeup that might make them look sufficiently adult"). Linking identity authentication with age authentication doesn't ensure accuracy of either authentication. *See* Brief for The Center for Democracy & Technology et al. as Amici Curiae Supporting Petitioners, Free Speech Coal., Inc. v. Paxton, U.S. Sup. Ct., No. 23-1122, 2024 WL 4290487 (filed Sept. 20, 2024), at 10-11. Like all forms of authentication, identity authentication is gamable. *See*, *e.g.*, Joseph Cox, *Inside the Face Fraud Factory*, 404 MEDIA (July 15, 2024), https://perma.cc/DQ7M-XJQK (for $30, the author bought 80 photos and 4 videos depicting a third party that, after some customization by the buyer, would satisfy identity authentication screens); Kaja Andric & Corey Kilgannon, *A New Generation of 'Unbeatable' Fake IDs Is Bedeviling Bouncers*, N.Y. TIMES (Feb. 13, 2025), https://perma.cc/7668-ESUG; Lauren Smiley, *Priscila, Queen of the Rideshare Mafia*, WIRED (July 10, 2024), https://perma.cc/43QN-QLRS.

cannot confirm that the person being assessed is the same person who will have access to the restricted resources.[77]

To reduce this spoofing risk, authenticators could combine real-time visual inspection with document review for identity verification (i.e., requiring the reader to simultaneously present a government-issued ID with their face). Or if age authentications are done offline, any authentication "token" issued by the authenticator must be tied to the assessed person's identity to prevent the token from being purchased by an adult and transferred to a minor.

Because authenticators will feel pressure to connect the age authentication to a specific person to boost the reliability of their authentications, an age authentication mandate is highly likely to increase the prevalence of identity authentication (even if a segregate requirement says nothing about identity authentication). The proliferation of identity authentication adds further privacy and security risks.

For efficiency purposes, age authentication mandates will motivate publishers to ask readers to register and create an account with the publisher and create a persistent identity across that reader's visits to the publisher. By doing this, the publisher can age-authenticate each reader only once,[78] rather than making repeat visitors go through the annoying and time-consuming authentication process each time they visit. (This also saves authentication costs for the publisher). To facilitate readers' creation of persistent identities, publishers will erect more login barriers (sometimes called "registration walls")[79] that readers must navigate before they can access the publishers' resources. Registration walls will reduce publishers' audience and revenues (see *infra* Section II.A.3). Furthermore, the age authentication mandate will drive publishers to collect more information from readers than they would choose to collect, and it will make it easier for publishers to track the reader's activities for data mining purposes. Each of these outcomes will put readers' privacy and security at greater risk—including minors.[80]

---

[77] *Cf.* Kimberley Chandler, *Milk, Eggs and Now Bullets for Sale in Handful of US Grocery Stores with Ammo Vending Machines*, ASSOC. PRESS (July 9, 2024), https://perma.cc/5LB8-V2NL (offline vending machines that sell gun ammunition verify both identity and age).

[78] However, a segregate-and-suppress law might prevent the publisher from using persistent online identities to bypass repetitive age authentications. *See* S. 1792, 113th Gen. Assemb., Reg. Sess. (Tenn. 2024) (requiring publishers to reauthenticate readers' ages every sixty minutes).

[79] *Registration Wall,* WIKIPEDIA, https://perma.cc/VJD8-5D37 (archived May 7, 2025).

[80] Harwell, *supra* note 54 (quoting Brenda Leong as saying that "the more [publishers] learn about [children], the more their privacy is at risk").

The increased prevalence of persistent online identities will reduce readers' ability to consume content anonymously or pseudonymously.[81] However, unattributable content consumption is essential for people's uninhibited exploration of their intellectual interests.[82] This is why privacy laws protect content consumption histories.[83]

Persistent identities also make it harder for authors to share their content anonymously or pseudonymously.[84] This will degrade the information ecosystem.[85] Efforts to hold powerful entities accountable, such as whistleblowing and political activism, are sometimes possible only when authors can be assured of anonymity or pseudonymity.[86] Mandatory online age authentication will reduce these socially vital activities.

B. Stage 2: The Suppression

The prior subpart described the "segregation" stage of the segregate-and-suppress approach. This subpart now describes the "suppression" stage, in which regulators compel publishers to restrict minors' access to online content or resources. Many laws require the restriction of material that is purportedly "harmful to minors," a codeword for online pornography that can be interpreted more expansively to facilitate greater content restrictions.[87] However, segregate-and-suppress laws are not just anti-pornography laws. The laws target any type of activity that regulators disfavor, including a wide range of socially beneficial and constitutionally protected content and activities. In

---

[81] MARWICK ET AL., *supra* note 41, at 27 ("wide scale implementation of mandatory age verification would have devastating consequences for internet privacy, making it more or less impossible to browse the web anonymously").

[82] *See* CDT Report*, supra* note 57, at 14 (discussing how minors use multiple accounts for exploration and safety purposes).

[83] For example, the federal Video Privacy Protection Act, 18 U.S.C. § 2710, restricts the disclosures of people's video-watching histories, and California's Reader Privacy Act, CAL. CIV. CODE § 1798.90, restricts book services' disclosure of personal information about book buyers or readers.

[84] EFF Letter, *supra* note 16.

[85] *See* JEFF KOSSEFF, THE UNITED STATES OF ANONYMOUS (2022).

[86] Greens Report, *supra* note 18, at 34. For example, the Federalist Papers were written pseudonymously. *See*, *e.g.*, *Pseudonyms and the Debate over the Constitution*, CTR. FOR THE STUDY OF THE AM. CONST. AT UW–MADISON (July 22, 2022), https://perma.cc/2DH7-YX8B.

[87] *See*, *e.g.*, Paige Collings & Rindala Alajaji, *The Impact of Age Verification Measures Goes Beyond Porn Sites*, ELEC. FREEDOM FOUND. (Jan. 23, 2025), https://perma.cc/9TSQ-HE2F (discussing an Oklahoma statute that "requires a site to verify someone's age before showing them content about homosexuality").

other words, "suppression" is a synonym for government-compelled "censorship," which should make all such efforts constitutionally suspect.[88]

1. Suppression Methods

Suppression obligations can be structured in a variety of ways, including categorical access restrictions ("bans"), conditional access restrictions, and obligations to satisfy a duty of care.

Categorical Access Restrictions. Lawmakers can categorically ban minors from accessing certain types of online content or resources. For example, regulators can restrict minors' ability to access a specific category of content (such as online pornography)[89] or block an entire speech venue (such as Australia's ban of minors' access to social media).

Conditional Access Restrictions. Instead of a categorical ban, lawmakers can impose conditions on minors' ability to access online content or resources.[90] In the following examples (all of these restrictions are contained in the New York SAFE for Kids Act),[91] minors can access desired content and resources, but not necessarily in the manner preferred by the reader or publisher:

- The law can ban content auto-play or "infinite scrolling" where an online "page" has no end.
- The law can restrict the time of day when a minor can access the publication (e.g., not during typical sleeping hours) or the total number of hours that a minor may access the publication during a single day.
- The law can dictate how algorithms present content, such as requiring that content be presented using reverse chronological order or not be prioritized based on personalized algorithms.

---

[88] MARWICK ET AL., *supra* note 41, at 33 ("There is a long history of internet legislation requiring age verification that has been struck down because of the First Amendment."). The two leading Supreme Court segregate-and-suppress decisions are Reno v. ACLU, 521 U.S. 844 (1997) and ACLU v. Ashcroft, 542 U.S. 656 (2004). The Supreme Court has granted review of Texas H.B. 1181, Free Speech Coal., Inc., v. Paxton, 95 F.4th 263 (5th Cir. 2024), *cert. granted*, 144 S. Ct. 2714 (2024).

[89] As discussed above, the law may use a euphemism like "material that is harmful to minors."

[90] This is conceptually similar to "time, place, and manner" speech restrictions, but applied to private actors' editorial decisions, not as restrictions on government action.

[91] S. 7694A, 2023 Leg., Reg. Sess. (N.Y. 2024).

As discussed below, a parental consent requirement is also typically a conditional access restriction.

Duty of Care. Instead of enumerating specific restrictions, lawmakers can require publishers to satisfy a duty of care to treat minors "better" than adults, prioritize the best interests of minors, or otherwise subvert their corporate interests in favor of minors' interests.[92]

This approach nominally gives publishers more editorial and operational flexibility to satisfy the duty than they would have in the face of categorical bans or detailed conditional restrictions. Nevertheless, a "duty of care" suppression obligation creates several unsolvable problems for publishers.[93]

First, publishers cannot satisfy a duty of care towards minors because they are ill-positioned to determine what is in the best interests of minors as a whole or with respect to any specific child. Regarding minors as a whole, the needs of minor subpopulations routinely conflict with each other as described in Part III. As a result, no matter what editorial or design choices the publisher makes, some minor subpopulations are likely to be disadvantaged. Regulators will point to those disadvantaged subpopulations as prima facie evidence that the publisher failed to satisfy its duty of care towards them. Regarding individual minors, publishers have very limited insights into each minor's life, making it impossible for publishers to anticipate how their choices will impact each individual.[94] Thus, no matter how the duty of care is styled, publishers will routinely breach it—a no-win situation for publishers.

Second, unless the law spells out the duty of care in detail, the duty will be defined via the common law. That process will create long-term legal uncertainty about what publishers can and cannot do, and publishers will incur high legal defense costs to define the rules and defend their practices—all in the face of substantial, if not business-ending, legal risks if the courts say the publishers got it wrong. The defense costs and legal risks will prompt publishers to "self-censor" their editorial choices or exit the industry entirely.

Third, partisan regulators can easily weaponize a duty of care standard to advance partisan goals or the culture wars. For example, regulators can claim

---

[92] *See* PHIPPEN, *supra* note 5, ch. 2 (discussing the duty of care in the U.K. Online Safety Act).

[93] *See* Maria P. Angel & danah boyd, *Techno-Legal Solutionism: Regulating Children's Online Safety in the United States*, CSLAW'24: 3rd ACM Computer Science and Law Symposium 9 (Mar. 12–13, 2024), https://perma.cc/9KLH-NL6P (in response to duty of care obligations, "tech companies will be required by law to design their systems for social outcomes they cannot possibly control").

[94] *See infra* Part III. Reminder: it does not benefit minors to motivate publishers to collect more sensitive information from minors.

(illegitimately) that making available truthful information on a culture war topic harms minors and thus violates the duty of care.[95] Thus, an amorphous legal standard makes it easier for partisan regulators to target content that benefits marginalized communities, such as the LGBTQ+ community, for suppression.[96] Some publishers will stand up to these regulatory attacks, but many others will acquiesce to the regulatory threats.

Privacy Laws Can Be Segregate-and-Suppress Laws

Segregate-and-suppress laws can be framed as privacy laws, but that doesn't change their nature or effect. For example, the California Age-Appropriate Design Code (AADC),[97] styled as a privacy law, obligates many commercial online publishers to identify minors through age authentication (the segregation). It then requires publishers to provide purportedly heightened "privacy" protections (including duty-of-care obligations)[98] to minors, including restricting minor access to online content and services (the suppression). Thus, like other segregate-and-suppress laws, the AADC advances censorship by blocking the publication of content to minors as well as the ability

---

[95] MARWICK ET AL., *supra* note 41, at 32 ("In a polarized social context where the definition of 'harmful' is highly subjective and deeply influenced by politics, allowing the government to decide which content is considered 'harmful' opens up a serious vector for abuse"); *see also* danah boyd, *Risks vs. Harms: Youth & Social Media*, DATA: MADE NOT FOUND (BY DANAH) (Oct. 8, 2024), https://perma.cc/PN3G-NSUJ.

[96] For example, the segregate-and-suppress bill Kids Online Safety Act (KOSA) contained a duty of care, which Senator Blackburn hoped would help with "protecting minor children from the transgender in this culture." https://perma.cc/879P-CKFP; *see also* https://perma.cc/9DW6-W3A4 (the Heritage Foundation supported KOSA because "Keeping trans content away from children is protecting kids"); ALBERT FOX CAHN ET AL., SURVEILLANCE TECH. OVERSIGHT PROJECT (STOP), THE KIDS WON'T BE ALRIGHT 9 (Sept. 23, 2023), https://perma.cc/B8VX-346Z [hereinafter STOP Report] (segregate-and-suppress laws can effectuate "a digital erasure of access to information for and about LGBTQIA+ youth"); Shae Gardner, *Logged Out, Left Out*, LGBT TECH (Apr. 8, 2024), https://perma.cc/X7HP-RTVN [hereinafter LGBT Tech Report] ("vague criteria around 'harm to children' can be weaponized to suppress LGBTQ+ voices online").

[97] Cal. A.B. 2273 (2021-22). *See generally* Stacy-Ann Elvy, *Age-Appropriate Design Code Mandates*, 45 U. PA. J. INT'L L. 953 (2024) (comparing the California AADC with the U.K. Age-Appropriate Design Code).

[98] For example, the AADC prohibits publishers from using "the personal information of any child in a way that the business knows or has reason to know the online service, product, or feature more likely than not causes or contributes to a more than de minimis risk of harm to the physical health, mental health, or well-being of a child." CAL. CIV. CODE § 1798.99.31(b)(1) (West 2025).

of minors to author their own content.[99] This Article applies to segregate-and-suppress laws however they are characterized, including as "privacy" laws.

2. The Special Circumstances of Parental Consent Requirements

In many circumstances, it's better if parents[100] make decisions about their children's Internet usage instead of the government imposing one-size-fits-all restrictions or expecting third-party publishers to divine individual children's idiosyncratic needs. Compared to all other players in the ecosystem, typically parents best understand their children's needs and are best positioned to help their children use the Internet appropriately.

Based on this premise, regulators are routinely creating parental consent requirements for minors' access to online content or resources. These requirements act like conditional access restrictions, meaning that minors can access the resources, but only after the publisher and minor obtain parental consent.

Unfortunately, parental consent requirements are highly problematic. First, the literature suggests that such requirements may counterproductively undermine the parent/child relationship.[101] Second, the requirements raise several difficult conceptual and operational issues:

Who Can Consent? Regulators often assume a paradigm that families are run by two married parents who are co-parenting. When this assumption isn't true, the parental consent requirement becomes potentially problematic.

For example, divorced parents with joint custody may disagree about their desired online access for their child. What should a publisher do if one parent consents and the other parent withdraws the consent? Such conflicting instructions are inevitable among parents who are separated, divorced, or living apart, especially when the parents disagree about what's in the best interests of the child (or worse, are using the child as a pawn in disputes between them).

---

[99] NetChoice, LLC v. Bonta, 113 F.4th 1101 (9th Cir. 2024); Eric Goldman, *Will California Eliminate Anonymous Web Browsing? (Comments on CA AB 2273, The Age-Appropriate Design Code Act)*, TECH & MKTG. L. BLOG (June 27, 2022), https://perma.cc/QAH3-ABVG.

[100] "Parents" include guardians, custodians, and anyone else who has the legal rights and responsibilities of parents.

[101] *E.g.*, Mariya Stoilova et al., *Do Parental Control Tools Fulfil Family Expectations for Child Protection? A Rapid Evidence Review of the Contexts and Outcomes of Use*, J. CHILDREN & MEDIA (Oct. 29, 2023), https://perma.cc/AWV2-WXWK.

Parental consent also may not be feasible for minors in foster care and unemancipated minors who are not in touch with their parents (in some cases for good reasons, such as because they fled an abusive home environment).

Unless the laws specify how publishers can navigate non-paradigmatic parent-child relationships, a parental consent requirement turns into a categorical ban for the affected minors.

Authenticating Parental Status. Publishers do not have any good way of confirming that the person "consenting" for a minor is actually the minor's parent.[102] As the Irish Data Protection Commission has said, "there aren't yet many ways of checking parental consent which are accurate, proportionate and that actually work in practice."[103]

Authenticating parental status online is not a new problem, but it remains a completely unsolved one. For example, for a quarter-century, COPPA has required that publishers "obtain verifiable parental consent before any collection, use, or disclosure of personal information from children."[104] The FTC's regulation purportedly clarifies what "verifiable" means: "[a]ny method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[105]

In other words, after decades of trying, the FTC still has no idea how to authenticate parental status. As further evidence that the problem remains unsolved, the FTC's regulation enumerates several modalities for "parents" to communicate their consent, but the regulations mostly ignore the authentication challenge:[106]

Modality to Communicate Parental Consent	**Steps Publisher Must Take to Confirm Parental Status**
Consent form submitted via mail, fax, or email scan	Apparently self-authenticating

[102] *See* NetChoice, LLC v. Griffin, No. 5:23-CV-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023) (discussing the problems of authenticating parental status).

[103] *Children's Data and Parental Consent*, IRELAND DATA PROTECTION COMM'N (Apr. 2023), https://perma.cc/3BW3-JCQ.

[104] 16 C.F.R. Part 312.5(a)(1). A reminder that COPPA defines "children" as minors under thirteen.

[105] *Id.* Part 312.5(b)(1).

[106] *Id.* Part 312.5(b)(2).

Credit card or other payment "that provides notification of each discrete transaction to the primary account holder"	Apparently self-authenticating[107]
Telephone	Staffers must be trained
Video-conference	Staffers must be trained
"Verifying a parent's identity by checking a form of government-issued identification against databases of such information"	Apparently identity authentication is sufficient?[108]
Email consent	"Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call"

If regulators really wanted to ensure that the person providing COPPA consent is the minor's parent, this list of options is wholly inadequate. With almost all of these techniques, minors easily can overcome the requirements by self-consenting or having a non-parent third party consent for them. The fact that the COPPA regulations have been in effect for nearly twenty-five years, and yet still rely on obviously deficient methods of authenticating parental status, shows how hard the parental-status authentication challenge is to solve.

If regulators were really serious about properly authenticating parental status, the regulators would require authenticators to do four layers of authentication: (1) the reader's status as a minor, (2) the minor's identity, (3) the parent's identity, and (4) the legal parent-child status between the two. When stacked together like this, the gauntlet of required authentications is virtually impossible for minors, parents, or publishers to navigate for several reasons.

---

[107] This remains an authentication option despite the fact that many minors possess credit cards. *See supra* note 64.

[108] Perhaps the FTC expects publishers can assume parental status when the consenting individual and child share the same last name? That would be an imprecise proxy for parental status. *See*, *e.g.*, Claire Cain Miller, *Why Parents Give Their Children a Last Name Other Than the Father's*, N.Y. TIMES (Dec. 27, 2023), https://perma.cc/XNK7-S7W2.

First, unlike the information contained on government-issued IDs, parents rarely have a single document confirming their current status as a child's parent. Exactly what paperwork will sufficiently document the relationship?

Second, the disclosure of supporting paperwork creates another irony where efforts to protect minors counterproductively puts minors', and parents', privacy and security at greater risk. The invasive nature of the inquiry raises questions about whether the obligation comports with standard privacy law principles of data minimization[109] and proportionality.[110] This conflict is especially obvious when the parental consent obligation is imposed for circumstances where minors face a low level of privacy risk or other harms. The disclosures necessary to obtain parental consent might pose a much greater threat to the minor than does the restricted content or resource.

Third, the effort and time required for minors and parents to navigate four layers of authentication stacking acts like a nearly impenetrable barrier to access. Most minors will give up, a non-trivial number of parents—especially those from disadvantaged communities—will lack the digital skills or motivation to navigate these processes, and most publishers won't want to incur the costs.

Parents May Not Prioritize Their Children's Best Interests. While laws routinely and logically presume that parents act in the best interests of their children, any parental consent requirement must anticipate that some parents will act otherwise.[111] For example, a parental consent requirement gives abusive parents another way to abuse their children, such as by withholding consent when the child really needs online access, or by imposing conditions on the granting of consent to exercise greater leverage over the child.[112]

---

[109] The data minimization principle says that an entity should collect only the minimum amount of personal information necessary to accomplish the purpose. *E.g.*, General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) art. 5; *see* Shoshana Weissman, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R STREET (May 24, 2023), https://perma.cc/5X2X-XDST.

[110] *See*, *e.g.*, Treaty on European Union 2008/C 115/1, art. 5(4) ("the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties").

[111] *See* ITIF Report, *supra* note 31, at 5 ("not every child lives in a home with parents willing or able to look out for their best interests online.").

[112] One study estimated that over 12% of children experience some form of abuse over their childhood. Nancy Shute, *Odds of Abuse and Mistreatment Add Up over Children's Lives*, NPR (June 2, 2014), https://perma.cc/Z9GM-R6VH. That translates to many hundreds of thousands or millions of children at any time. *See* STOP Report, *supra* note 96, at 1 ("for countless kids, parents pose a threat . . . abusive parents can block all access to [support] resources by withholding consent").

Even in non-abusive situations, parents and children may strongly disagree about what's in a child's best interests online. For example, atheist parents may oppose their child's exploration of organized religion; parents may seek to deny or suppress a child's self-identification as part of the LGBTQ+ community; and parents may categorically reject abortion as an option even when a pregnant child needs an abortion to save their life.

These parent-child conflicts are often tragic and not easy to resolve. However, a parental consent requirement gives parents another tool to control what online content and resources are available to their children, and that gatekeeping can lead to life-changing and detrimental outcomes for minors. At minimum, parental restrictions can hinder their children's ability to understand and explore themselves, the world, and their options, which can have major implications for minor subpopulations like the LGBTQ+ community.[113]

Some parental consent requirements include the right to surveil their children's activities online—a supervisory power that doesn't really have an offline analogue. This threat of parental surveillance reduces children's privacy rights, which can inhibit developmentally appropriate exploratory behavior (especially when the views of parents and children diverge).[114]

---

[113] APA Advisory, *supra* note 2, at 4 ("Access to peers that allows LGBTQIA+ and questioning adolescents to provide support to and share accurate health information with one another can protect youth from negative psychological outcomes when experiencing stress"); STOP Report, *supra* note 96, at 1 ("For so many LGBTQ+ youth, online anonymity is the only thing that lets them access spaces where they can be themselves . . . Children and teenagers have relied on online communities as safe spaces and supportive lifelines for decades"); COMMON SENSE MEDIA & HOPELAB, A DOUBLE-EDGED SWORD: HOW DIVERSE COMMUNITIES OF YOUNG PEOPLE THINK ABOUT THE MULTIFACETED RELATIONSHIP BETWEEN SOCIAL MEDIA AND MENTAL HEALTH 12 (2024), https://perma.cc/FFL7-FG4M [hereinafter Common Sense & Hopelab Report] ("LGBTQ+ youth said that finding community in person was often fraught in a climate of increased restrictions and hate toward trans and queer youth, and that online communication often felt safer and more supportive . . . For many LGBTQ+ teens, online spaces create valued opportunities for connecting to content that is identity-affirming and supportive of LGBTQ+ people."); Jennifer Luu, *'Social Media Saved Me': Here's What Children Want You to Know About the Social Media Ban*, SBS NEWS (Nov. 29, 2024), https://perma.cc/4TY5-24ZP (quoting a queer teen as saying "[s]ocial media and the ability to spread positivity and spread my story has basically saved my life"); Claude Marks & Kathleen Murphy, *Bedoya Wants FTC to 'Reinvigorate' Robinson-Patman Act*, MLEX (Dec. 19, 2023), https://perma.cc/8WBP-SLT8 (FTC Commissioner Bedoya opposed regulations that "cut off the lifeline that social media is to kids in rural America, LGBT teens anywhere in the country who see social media as a place where they find community, they find resources, they find support").

[114] MARWICK ET AL., *supra* note 41, at 29 (a law "that allows parents to see the content of sites their children visit may make vulnerable minors more vulnerable . . . .If parental access now provides search history, comments, user activity, and even access to private messages to unsupportive parents, then queer youth will have their sexual privacy eroded, and be potentially subject to abusive responses."); STOP Report, *supra* note 96, at 9 ("If teens are

III. THE SEGREGATION PROCESS IS HARMFUL

Part I defined online age authentication and identified some problems with specific implementation options. This Part takes a closer look at additional problems endemic in every method of online age authentication.[115]

A. Structural Problems with the Segregation Process

This subpart describes five intrinsic problems caused by mandatory online age authentication.

1. Privacy Invasions

By definition, age authentication seeks to ascertain an important and immutable personal attribute of a person. Many people consider their age to be sensitive information,[116] and the process of figuring out a person's age inevitably involves the disclosure of additional private information beyond age, some of it highly sensitive. Thus, requiring minors to disclose their age always invades their privacy. As the California Privacy Protection Agency staff noted, "there is currently no privacy-protective way to determine whether a consumer is a child."[117]

The leading age authentication methods, document review and visual inspections, each require readers to disclose highly sensitive information beyond their age, namely the information displayed on a government ID or the

---

required to register their internet usage with parents, digital lifelines will become a potential threat that outs users to the very parents many are hiding from"). *See generally* Danielle Keats Citron & Ari Ezra Waldman, *Rethinking Youth Privacy*, __ VA. L. REV. __, at 4 (2025) ("Policymakers' go-to response—parental control—is a failure. While the parental control model was never well-suited to protect children's privacy, it cannot meet this moment").

[115] Efficacy is another concern: "age verification requirements are ineffective at preventing minors from viewing obscene content." Free Speech Coalition, Inc. v. Rokita, 738 F. Supp. 3d 1041 (S.D. Ind. 2024). Also, readers can route around geography-based segregate-and-suppress laws using VPNs. Rindala Alajaji & Paige Collings, *VPNs Are Not a Solution to Age Verification Laws*, ELECTRONIC FRONTIER FOUND. (Jan. 20, 2025), https://perma.cc/M7SU-R7LA. However, the problems identified in this Article would remain even if age authentication worked perfectly.

[116] *E.g.*, CAL. CIV. CODE § 1798.83.5 (enacted in Cal. AB 1687 (2016)) (prohibiting the publication of some people's ages by designated web publishers). The Ninth Circuit invalidated this law as unconstitutional in IMDb.com Inc. v. Becerra, 962 F.3d 1111 (9th Cir. 2020).

[117] Mahoney Memo, *supra* note 33, at 5. The memo adds, "age verification systems are likely not sufficiently advanced to ensure accurate age verification while protecting privacy." *Id.* at 7.

reader's appearance for biometric scanning.[118] These requirements are privacy-invasive: "66% of Americans are not comfortable sharing their identification documents or biometric information with online platforms."[119]

Rather than make unwanted disclosures, many readers confronted by a publisher's age authentication request will leave the publisher's service and not complete the authentication process. This U-turn is called a "bounce."[120] Readers' tendency to bounce will be worse for startup publishers who have not yet earned readers' trust.[121] Section II.A.3 will revisit the bounce issue.

Also, governments around the world want people to think twice before sharing sensitive biometric information due to the information's immutability if stolen. Mandatory age authentication teaches them the opposite lesson.

Given the stakes of providing the disclosures required to age-authenticate, the reader's choice of whether to authenticate or bounce is complicated and nuanced. Most minors are still developing the cognitive and analytical skills needed to make these decisions wisely. Yet, segregate-and-suppress laws will force minors to make these decisions constantly, with potentially significant negative consequences for making a bad choice. Thus, if the policy goal is to protect minors online because of their potential vulnerability, then forcing minors to constantly decide whether or not to share highly sensitive information with strangers online is a policy fail.

---

[118] Such information is highly protected by privacy law. *E.g.* General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) art. 9. In particular, biometric privacy laws may restrict or categorically ban age authentication based on some visual inspections. *See* Kuklinksi v. Binance Capital Mgmt. Co., No. 21-cv-001425, 2023 WL 2788654 (S.D. Ill. Apr. 4, 2023) (identity verification processes may violate the Illinois' Biometric Information Privacy Act, known as BIPA); Murphy v. Confirm ID, Inc., 2025 WL 603598 (E.D. Cal. Feb. 25, 2025) (addressing the same issue). If visual inspection-based age authentications are not legally permitted, compliance will become even more difficult and expensive for publishers and more burdensome for readers.

[119] Free Speech Coal., Inc. v. Rokita, 738 F. Supp. 3d 1041 (S.D. Ind. 2024) (cleaned up). "70% are uncomfortable with their children using such methods." *Id.*; *see also* Harwell, *supra* note 54 (discussing how South African parents viewed Yoti's face scanning with "extreme passionate fear" and "overwhelming" skepticism).

[120] Yun Fei, *Study on Factors Associated with Bounce Rates on Consumer Product Websites*, *in* BUSINESS ANALYTICS PROGRESS ON APPLICATIONS IN ASIA PACIFIC 526 (Jorge L. C. Sanz ed., World Scientific Publishing Co. Pte. Ltd. 2016).

[121] Engine Report, *supra* note 65, at 6 ("A startup that requires users to submit their drivers licenses as part of signing up for a service has to worry about whether users feel comfortable handing that sensitive information over, or whether they'll seek out an alternative offered by a larger, more established company").

2. Security Risks

The disclosure of highly sensitive authentication data exposes readers—including minors—to substantial information security risks, including identity theft, extortion and blackmail, financial fraud, more tailored commercial pitches, and data profiling.[122]

Regulators can mitigate the information security risks by compelling age authenticators to minimize their data collection (e.g., disregarding other data incidentally disclosed in the process, such as non-age information on a government-issued ID) and to promptly delete any highly sensitive information disclosed to them in the age authentication process.[123] Even if the law doesn't impose such mandates, age authenticators will likely voluntarily represent to readers that they will follow good data minimization and data deletion practices to boost reader confidence and trust.

Readers will have good reasons to assume that their data nevertheless will be collected or retained, regardless of what the law or the authenticator says.[124] Authenticators need to demonstrate the accuracy of their authentications if they are challenged, and they may need to retain records evidencing this.[125] Some authenticators will negligently retain authentication data due to incompetence or oversight. Other authenticators might intentionally disregard any minimization or deletion obligations because violations may be hard to detect. Even if these fears are overstated, skepticism about the security of their authentication data will increase readers' bounce rate from publishers' services.[126]

---

[122] Greens Report, *supra* note 18, at 35 ("unauthorised access can open the door to various forms of misuse, potentially resulting in significant harm to individuals").

[123] OECD Report, *supra* note 25, at 31 ("To mitigate privacy risks, age assurance solutions should incorporate robust privacy protections, such as principles of data minimisation to collect and retain the minimal amount of data required").

[124] *See* Free Speech Coal., Inc. v. Colmenero, 689 F. Supp. 3d 373 (W.D. Tex. 2023), *rev'd*, Free Speech Coal., Inc. v. Paxton, 95 F.4th 263 (5th Cir. 2024), *cert. granted*, 2024 WL 3259690 (July 2, 2024) (the premise that readers will "trust that companies will actually delete" their authentication data is "dubious"). "It is the threat of a leak that causes the First Amendment injury, regardless of whether a leak ends up occurring." *Id.*

[125] MARWICK ET AL., *supra* note 41, at 28 ("If information is deleted immediately following verification, then those systems are substantially less auditable because there would be no concrete record of the information provided for verification"). Other legal obligations may compel authenticators to retain authentication data, such as litigation holds, record retention laws, and law enforcement demands.

[126] "Requiring Internet users to provide . . . personally identifiable information to access a Web site would significantly deter many users from entering the site, because Internet users are concerned about security on the Internet and . . . afraid of fraud and identity theft[.]"

If authentication data is retained, it poses a major information security risk to minors (and adults).[127] In particular, the data will attract malefactors due to the high value of sensitive authentication data.[128] Inevitably, malefactors will find weak spots in authenticators' security and exfiltrate the authentication data; and some authenticators will mishandle the data and accidentally expose it publicly. Unsurprisingly, numerous authenticators have suffered major data security failures that put authenticated individuals at grave risk.[129]

Malefactors can also build legitimate-looking but bogus websites or apps designed to collect and expropriate readers' authentication data.[130] By the time readers realize they have been duped, their data will already be gone.[131] All

---

ACLU v. Gonzales, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007), *aff'd sub nom*., ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008); *see also* PSINet, Inc. v. Chapman, 167 F. Supp. 2d 878, 889 (W.D. Va. 2001), *aff'd*, 362 F.3d 227 (4th Cir. 2004) ("Fear that cyber-criminals may access their [identifying information] . . . . may chill the willingness of some adults to participate in the 'marketplace of ideas' which adult Web site operators provide.")

[127] Even if readers' authentication data is never retained, it will be an attractive target for real-time interception.

[128] *E.g.*, Taryn Plumb, *Face off: Attackers Are Stealing Biometrics to Access Victims' Bank Accounts*, VENTUREBEAT (Feb. 21, 2024), https://perma.cc/UP27-NQT7; Harwell, *supra* note 54 (quoting Jason Kelley of the E.F.F. as saying "All these extremely sensitive pieces of information, linked to people's faces?... [For a hacker,] that's the best [treasure trove] I can imagine"). Data that attracts exfiltrators is often called a "honeypot."

[129] *E.g.*, Joseph Cox, *ID Verification Service for TikTok, Uber, X Exposed Driver Licenses*, 404 MEDIA (June 26, 2024), https://perma.cc/XF2A-CKEB (describing security vulnerabilities of authentication service provider AU10TIX); Jessica Kidd, Isobel Roe & Jesse Hyland, *Cybercrime Detectives Arrest Man Following Alleged Data Breach Involving More Than 1 Million NSW Clubs Customer Records*, ABC NEWS (May 1, 2024), https://perma.cc/P3ST-KU38 (Australian bars must authenticate patrons before entry and retain the records; an authentication service provider Outabox suffered a security breach that exposed those records); *Notice of Data Security Incident*, NEXTSTEPS.LA.GOV, https://perma.cc/Q573-QWJK (archived Apr. 29, 2025) (Progress Software Corp., a third-party vendor that the Louisiana Office of Motor Vehicle uses to assist with driver's license information, experienced a data security breach of authentication data due to a cyberattack); Zack Whittaker, *Online Gift Card Store Exposed Hundreds of Thousands of People's Identity Documents*, TECHCRUNCH (Jan. 3, 2025), https://perma.cc/5PQP-MQE8 (MyGiftCardSupply publicly exposed consumers' government-issued IDs it had collected to comply with government "know your customer" (KYC) obligations); Jagmeet Singh & Manish Singh, *Indian Online ID Verification Firm Signzy Confirms Security Incident*, TECHCRUNCH (Dec. 2, 2024), https://perma.cc/S854-EZUW; Manish Singh, *Mobikwik Investigating Data Breach After 100M User Records Found Online*, TECHCRUNCH (Mar. 30, 2021), https://perma.cc/JD3Q-BPAZ (data breach of KYC materials); Zack Whittaker, *Hackers Are Threatening to Leak World-Check, a Huge Sanctions and Financial Crimes Watchlist*, TECHCRUNCH (Apr. 18, 2024), https://perma.cc/UNP4-M99S (data breach of KYC materials).

[130] Eric Goldman, *Amicus Brief on the Constitutionality of the California Age-Appropriate Design Code's Age Assurance Requirement* (NetChoice v. Bonta) (February 24, 2023). Santa Clara Univ. Legal Studies Research Paper No. 4369900.

[131] EFF Letter, *supra* note 16, at 11 ("If a third-party company acting in bad faith collected biometric faceprints of users, it would be impossible for users to know").

readers will be desensitized to this risk because disclosing authentication data to strangers online will be an everyday occurrence, boosted by the halo of legitimacy that comes from the government's compulsion of such disclosures. Because their judgment is still developing, minors will be especially vulnerable to schemes like this.

As the information security maxim goes, if you want to keep data safer, don't disclose it to third parties. Mandatory age authentication requirements contravene this longstanding and simple best-practices guidance.

3. Authentication Walls

Age authentication processes act like a virtual "wall" interposed between readers and the content and resources they hope to access. As discussed, many readers will bounce when they encounter authentication walls because of the complex privacy and security issues created by the age authentication request.

Other readers will bounce because they lack the digital skills to complete the authentication process. For example, one study tasked consumers with navigating three different authentication processes; only 63% were able to complete all three.[132]

Yet other readers will bounce because they don't want to invest the time or mental energy to navigate the authentication process, even if they could do so successfully. Online readers are highly sensitive to barriers or "speed bumps"—even modest ones—that delay their arrival at their desired online destination. Age authentication is such a speed bump.

Unlike other speed bumps, such as "cookie" walls,[133] authentication walls will force readers to navigate one or more "interstitial" screens interposed between them and their desired destination. Interstitial screens always increase bounce rates, even when they can be easily ignored. For example,

---

[132] Corby, *supra* note 48.

[133] A "cookie wall" is another form of access barrier. It refers to the annoying cookie- and privacy-related disclosures presented to readers who access an Internet publisher's service. *E.g.* Nurullah Demir et al., *A Large-Scale Study of Cookie Banner Interaction Tools and Their Impact on Users' Privacy*, PROC. ON PRIV. ENHANCING TECHS. (2024); Oksana Kulyk et al., *Has the GDPR Hype Affected Users' Reaction to Cookie Disclaimers?*, 6 J. CYBERSECURITY tyaa022 (2020). Unlike authentication walls, readers can often just ignore those disclosures, which is what most readers do. *See* Joe Nocera, *How Cookie Banners Backfired*, N.Y. TIMES (Jan. 29, 2022), https://perma.cc/66KJ-L4SJ.

Google+ used an interstitial screen to promote its mobile app before users could access the service on a mobile device. This caused a 69% bounce rate.[134]

Reader bounce rates are also affected by "latency," the time between a reader's request for content and its delivery.[135] "Research shows that sites lose up to 10% of potential visitors for every additional second a site takes to load, and that 53% of visitors will simply navigate away from a page that takes longer than three seconds to load."[136] Another study showed that a latency increase from one to three seconds increased the bounce probability by 32%, and an increase from one to five seconds increased the bounce probability by 90%.[137]

In the future, it is theoretically possible that age authentication procedures will become so automated that readers will not encounter interstitial screens.[138] Even then, the authentication process will increase latency due to the time required to establish the necessary data transfers and verification.

Unless and until fully automated authentication procedures become viable, age authentication processes will require some human effort by readers or publishers or both, and these activities will cause significant time delays. For example, the age authentication vendor Yoti claims it can do visual inspections in only eight seconds.[139] That may sound quick, but it feels like an eternity to a reader trying to quickly reach their desired destination. Any Internet publisher adding an eight second delay to their readers' experiences will increase their bounce rates significantly.

The technical and operational affordances of age authentication walls are likely to change how readers navigate the Internet. As segregate-and-suppress laws extend across the Internet and eventually apply to most publishers, readers will likely encounter age authentication walls many times a day. Each

---

[134] *See* David Morell, *Google+: A Case Study on App Download Interstitials*, GOOGLE SEARCH CENTRAL BLOG (July 23, 2015), https://perma.cc/D32G-WU3R.

[135] Will Co. v. Lee, 47 F.4th 917, 924 (9th Cir. 2022).

[136] *Id.* at 924–25 (footnote omitted).

[137] Daniel An, *Find Out How You Stack Up to New Industry Benchmarks for Mobile Page Speed*, THINK WITH GOOGLE (Feb. 2018), https://perma.cc/8WHP-T44D.

[138] *See* NetChoice v. Bonta, No. 5:24-cv-07885, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024) (conjecturing that "many companies now collect extensive data about users' activity throughout the internet that allow them to develop comprehensive profiles of each user for targeted advertising" and, mining that data, age authentication could 'run in the background' without requiring any affirmative steps from readers to complete the authentication).

[139] https://perma.cc/8VXL-7JUT (last visited Feb. 1, 2024). This claim may be a best-case scenario. A new Yoti user had to navigate 52 different steps to complete the authentication, a process that took over five minutes. *See* Samantha Cole, *Accessing Porn in Utah Is Now a Complicated Process That Requires a Picture of Your Face*, MOTHERBOARD (May 3, 2023), https://perma.cc/FPY5-KEDA.

time a reader encounters the age authentication wall, the reader must spend time and mental energy making the initial decision of whether or not to proceed; and proceeding with the age authentication process will demand more time and mental energy. These time and energy investments will be hard for many readers to justify,[140] especially when the reader can't easily determine the value of the content or resource behind the authentication wall. Imagine, for example, a reader clicks on a link to take them to see a single content item on an unknown website. Today, readers casually follow links on the web to explore single content items on unknown websites. Will readers be as willing to click on those links if they know an age authentication wall, and the concomitant time and mental energy demands, awaits them?

Indeed, readers will factor the likelihood of encountering an age authentication wall when deciding whether they should click on a link to visit a publisher. Knowing in advance that they will probably U-turn if the publisher requires age authentication, readers will choose not to click at all.[141]

Readers' click-inhibition will broadly impact the Internet ecosystem. It will result in fewer overall clicks, and those clicks will be directed towards a smaller number of publishers. What is today a dynamic, organic information ecosystem will (d)evolve into a more static environment where readers consume less content from fewer sources.

For publishers, the financial stakes are enormous. Latency increases, even small ones, will hurt publishers' revenues. "Amazon recently found that every 100 milliseconds of latency cost it 1% in sales."[142] Another study showed that for online retailers, the "difference in e-commerce conversion rate between blazing fast sites and modestly quick sites is sizable. A site that loads in 1 second has an e-commerce conversion rate 2.5x higher than a site that loads in 5 seconds."[143]

Whether due to increased latency or other reasons (such as privacy and security concerns), higher reader bounce rates will shrink publishers'

---

[140] This is one reason why online age authentication mandates are constitutionally problematic: "Requiring adult users to produce state-approved documentation to prove their age and/or submit to biometric age-verification testing imposes significant burdens on adult access to constitutionally protected speech." NetChoice, LLC v. Griffin, No. 5:23-CV-05105, 2023 WL 5660155, at *17 (W.D. Ark. Aug. 31, 2023).

[141] Alternatively, readers may gravitate towards publishers who aren't required to authenticate age or disregard their obligations to authenticate, which could take readers (including minors) into more dangerous corners of the Internet.

[142] Will Co. v. Lee, 47 F.4th 917, 925 (9th Cir. 2022).

[143] Michael Wiegand, *Site Speed Is (Still) Impacting Your Conversion Rate*, PORTENT (Apr. 20, 2022), https://perma.cc/9CZU-84AR.

audiences[144]—and the associated revenues. For one publisher, "the imposition of age verification requirements will reduce traffic to impacted websites by approximately 80%."[145]

As this discussion indicates, age authentication mandates have wide-ranging effects on the entire Internet ecosystem, including effects far beyond the purported concerns of protecting minors online. The inevitable changes in readers' behavior affect what readers consume and from whom. This, in turn, has potential second-order effects on educating consumers and citizens to help them make more informed choices. We will all feel the effects of an information-poorer society.

4. Publishers' Costs

Age authentication mandates cost publishers money—potentially a lot of money. One estimate indicated that authenticating 5 million readers per month "can cost upward of $7 million."[146] For publishers that cater to minors only incidentally, these authentication costs will hit particularly hard. For example, if a publisher's reader base is only 1% minors, the publisher will incur the costs to age-authenticate the other 99% of its readers who are adults. This lack of regulatory proportionality drains the financial resources of publishers who pose little or no risk of harming minors.

---

[144] *Cf. NetChoice, LLC*, 2023 WL 5660155 at *17 ("many adults who otherwise would be interested in becoming account holders on regulated social media platforms will be deterred—and their speech chilled—as a result of the age-verification requirements").

[145] Free Speech Coal., Inc. v. Rokita, 738 F. Supp. 3d 1041, 1062 n.16 (S.D. Ind. 2024); *see* Michael Hoffman, *House Bill 3: Florida Residents Will Have to Verify Their Age to Access Adult Sites Starting Jan. 1, 2025*, WPTV (Dec. 26, 2024), https://perma.cc/V9CM-9DWN (Pornhub says its traffic dropped 80% in Louisiana when it imposed mandatory age authentication); David Cooke & Sarah Bain, *Brief Submitted to Standing Committee on Public Safety and National Security*, AYLO & ETHICAL CAPITAL PARTNERS (Apr. 18, 2024), https://perma.cc/MY7S-786R ("over 99% of users subjected to a verification requirement did not verify their age"). These bounce rates may reflect heightened privacy and security concerns of pornography consumers.

[146] *Free Speech Coal., Inc.*, 738 F. Supp. 3d at 1049, n.4 ("Pornhub receives 115 million visits per day, which would cost $13.8 million a day to verify at 12 cents a user."). A different source reported that Yoti charges 10–25 cents per face. Harwell, *supra* note 54. "Plaintiffs' complaint includes several commercial verification services, showing that they cost, at minimum, $40,000.00 per 100,000 verifications." Free Speech Coal., Inc. v. Colmenero, 689 F. Supp. 3d 373, 385–86 (W.D. Tex. 2023), *rev'd,* Free Speech Coal., Inc. v. Paxton, 95 F.4th 263 (5th Cir. Mar. 7, 2024), *cert. granted*, 2024 WL 3259690 (July 2, 2024). Another report estimated authentication costs at 65 cents per verification. *See* Marc Novicoff, *A Simple Law Is Doing the Impossible. It's Making the Online Porn Industry Retreat.*, POLITICO (Aug. 8, 2023), https://perma.cc/Z9F2-TTEX (citing Mike Stabile, director of public affairs for the Free Speech Coalition).

Some publishers will treat the authentication costs as a cost of doing business. Other publishers—especially small or non-commercial publishers—will change their practices in response to the costs. If publishers can pass the authentication costs along to readers, then readers will pay more for access to the restricted resource—but the publisher will also see increased bounce rates due to the increased costs. If publishers cannot pass the costs to readers, the increased costs will make some publishers unprofitable and drive them out of the industry entirely.[147]

As with the disruption due to authentication walls, authentication costs—combined with the reduced revenue caused by the authentication walls and increased legal risk from the suppression obligation—will wreak havoc on the Internet ecosystem. Some of the likely effects: publishers will impose more paywalls to cover the age authentication costs; readers will be priced out of access to content and services they used to enjoy for free, which deepens digital divides; paywalls will increase the data that publishers collect from readers, increasing privacy and security risks; publisher profits will be eroded, which will drive some publishers and their constitutionally protected speech out of industry; reduced competition among publishers (because there are fewer remaining and startups can't afford the enter the industry) will drive up prices and reduce quantity; and the publishers' departures from the industry will leave gaps in the content and services available to readers that will not be backfilled by new entrants. Segregate-and-suppress laws *always* shrink the Internet for everyone, both minors and adults. In other words, an age-authenticated Internet will look quite different from the Internet as we know it today—and will be a worse place for almost every constituency.

These negative effects have already started. In the United Kingdom, the U.K. Online Safety Act (a segregate-and-suppress law) drove publishers out of the industry.[148] In the U.S., "nearly 139 million U.S. residents live in states with

---

[147] Engine Report, *supra* note 65, at 3 ("The direct and indirect costs of determining user age . . . will make it harder for startups to compete"); OTI Report, *supra* note 16 ("Age verification mandates would impose costly barriers to entry for start-ups and smaller operators. Such costs could unintentionally bias the market toward larger, more established companies that are better positioned to implement age verification and undertake the associated costs.").

[148] *E.g.*, Matthew Sparkes, *Hundreds of Small Websites May Shut Down Due to UK's Online Safety Act*, NEW SCIENTIST (Dec. 20, 2024), https://perma.cc/84NC-82BV; James Titcomb, *Hundreds of Websites to Shut Down Under UK's 'Chilling' Internet Laws*, TELEGRAPH (Dec. 17, 2024), https://perma.cc/AL4X-F2FJ. *See generally* PHIPPEN, supra note 5, ch. 2.

age verification laws on the books" targeting harmful to minors materials.[149] In response, Pornhub has blocked readers in those states,[150] essentially exiting those markets. This block dramatically affected reader behavior. In the aftermath of Louisiana's age authentication mandate, searchers shifted their searches away from Pornhub and towards its European competitor, Xvideo, who doesn't require age authentication.[151] This shift in reader preferences highlights the difficulty legislatures face when imposing geography-limited bans, but also shows that behavioral changes make marketplace winners and losers with important content access and distributional effects.

5. Building a Surveillance Infrastructure

By enacting age authentication mandates, the government sends a clear message to Internet readers: they must "pay" for the privilege of enjoying online content and services by sharing their highly sensitive personal information with online strangers.[152] What lessons might people—especially minors who are developing their intellectual identities—internalize from having this message repeated to them many times a day and stamped with the government's imprimatur? Widespread age authentication mandates will inevitably change people's attitudes towards privacy,[153] such as degrading their reluctance to share personal information in unrelated circumstances and increasing their overall long-term stress about the privacy and security of their sensitive information.

As age authentication becomes widely deployed across the Internet, governments will inevitably coopt the process to increase their control over their constituents.[154] This risk is heightened by any efforts, voluntary or

---

[149] Michael McGrady, *41 Percent of Americans Live Under Age Verification Laws Targeting Porn*, TECHDIRT (Dec. 30, 2024), https://perma.cc/LL57-H24V.

[150] *Id.*

[151] David Lang et al., *Do Age-Verification Bills Change Search Behavior? A Pre-Registered Synthetic Control Multiverse*, OSF (Mar. 9, 2025), https://perma.cc/6DLN-T8D7 ("Over the three months after the age verification law was passed, [Pornhub] lost more than half their search traffic (51%). [Xvideo] saw relatively large magnitude gains in their search volume (48.1%)"). There was also a boost in searches for VPNs, a tool readers can use to bypass geography-based blocks. *Id.*

[152] *See* ACLU v. Mukasey, 534 F.3d 181, 197 (3d Cir. 2008) (age authentication requirements force readers to "relinquish their anonymity to access protected speech").

[153] Greens Report, *supra* note 18, at 33 ("widespread adoption of age assurance in the online realm could cultivate a societal habituation to being identified and tracked online").

[154] *See* Stardust, *supra* note 47, at 3 ("We can understand the enthusiasm for age verification

mandatory, to couple age authentication with identity authentication. With a widely adopted identity authentication process, governments can create blocklists that age authenticators must enforce as part of their authentication process. Such blocklists can be easily weaponized to punish governments' enemies and entrench government incumbents' power.[155]

Even if publishers don't voluntarily link age authentication with identity authentication, regulators may compel the linkage as part of a broader "Know Your Customer" (KYC) push.[156] KYC originated in the financial sector but is propagating beyond those roots. In the context of content regulation, KYC is a euphemism for mandatory identity authentication. Imposing KYC obligations on publishers would end the possibility of user-authors publishing unattributed content and will accelerate the proliferation of partisanized blocklists.

B. Can Technological Ingenuity Mitigate the Problems with Age Authentication?

In 1997, the Supreme Court held that online age authentication mandates violated the First Amendment.[157] At that time, credit cards were lawmakers' primary age authentication solution. Over the past quarter-century, age authentication technology has evolved a lot. Does that mean technologists have solved the problems with age authentication?

The short answer is no.[158] Technologists can possibly improve certain aspects of age authentication technology, such as reducing the confidence

---

(biometric age estimation in particular) as part of a broader trend towards population-level surveillance"); Greens Report, *supra* note 18, at 35 ("The extensive implementation of age assurance systems may heighten the risk of state surveillance, particularly impacting marginalised communities and minorities"); Alex Stamos, THREADS.NET (July 5, 2024), https://perma.cc/LS37-AXC5 (saying that some age authentication services are an "authoritarian nightmare"); Harwell, *supra* note 54 (saying that even supporters of age authentication "acknowledge that age checks could fuel a profound expansion in government oversight of online life").

[155] For example, various government entities in China use social credit systems that can block or prioritize citizens' access to important social resources depending on their compliance with government rules and moral values. *See* Zeyi Yang, *China Just Announced a New Social Credit Law. Here's What It Means*., MIT TECH. REV. (Nov. 22, 2022), https://perma.cc/F695-JZMA. *See generally Know Your Customer,* WIKIPEDIA, https://perma.cc/5LQB-ANZP (archived May 4, 2025).

[156] *Know Your Customer,* WIKIPEDIA, https://perma.cc/J56U-GDDW (archived May 27, 2025).

[157] Reno v. ACLU, 521 U.S. 844 (1997).

[158] *See* Free Speech Coal., Inc. v. Colmenero, 689 F. Supp. 3d 373, 398–99 (W.D. Tex. 2023), *rev'd* Free Speech Coal., Inc. v. Paxton, 95 F.4th 263 (5th Cir. 2024), *cert. granted*, 2024 WL 3259690 (July 2, 2024) ("Despite changes to the internet in the past two decades, the Court comes to the same conclusion regarding the efficacy and intrusiveness of age verification as the ACLU courts did in the early 2000s.").

intervals when making automated age estimates using visual inspections,[159] reducing the speed or intrusiveness of the age authentication requests, or improving information security practices to reduce the likelihood of exfiltration. None of these developments will fix the underlying problems with online age authentication.

For example, every age authentication process inherently implicates sensitive personal information. The process always requires enough information to determine a person's age and then link that information to the person being authenticated. Making this determination doesn't necessarily require something as sensitive as government-issued IDs, but it cannot be done without some person or machine having access to highly sensitive information about the authenticated person.

Some proposals try to mask this fundamental truth by shifting the authenticator's identity. In those alternatives, there's still an authenticator, it's just not the publisher or a third-party vendor. For example, device-level authentication can speed up the authentication process by requiring it only once, but someone still has to authenticate the device. Similarly, with "zero-knowledge proofs,"[160] a third-party authenticator doesn't communicate the authenticated individual's identity to publishers. However, there always will be some authenticator with more than "zero knowledge" about the authenticated individual. In each case, the authenticator—whoever it is—becomes a potential weak link in the information security chain that creates the privacy and security risks discussed in Subpart II.A above.[161]

More generally, treating the online age authentication challenges as purely technological encourages the unsupportable belief that its problems can be solved if technologists "nerd harder."[162] This reductionist thinking is a categorical error. Age authentication is fundamentally an information problem,

---

[159] *But see* Stardust, *supra* note 47, at 2 ("While it remains a common refrain in computer science that such systems simply require better training data, more sophisticated algorithms or other incremental improvement, our meta-analysis indicates that age estimation solutions from facial scans cannot ever be expected to achieve acceptable levels of accuracy.").

[160] *Online Age Verification: Balancing Privacy and the Protection of Minors*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) (Sept. 22, 2022), https://perma.cc/6RKE-KTWA.

[161] *Colmenero*, 689 F. Supp. 3d at 399 ("Whatever changes have been made to the internet since 2004, these privacy concerns [with age authentication] have not gone away, and indeed have amplified").

[162] The phrase "nerd harder" is commonly attributed to Julian Sanchez. (@normative), X (Jan. 29, 2016, 04:34 PT), https://perma.cc/WK4H-E6FH; *see* Mike Masnick, *Nerd Harder: the T-Shirt*, TECHDIRT (May 20, 2016), https://perma.cc/KD9V-7S8P.

not a technology problem. Technology can help improve information accuracy and quality, but it cannot unilaterally solve information challenges.

For these reasons, it is a red herring to note that age authentication technologies may be more accurate or cheaper than the technologies at issue in the Supreme Court battles from the 1990s.[163] Even if an age authentication achieved perfect accuracy at zero financial cost to the publisher, the other problems discussed in this Part would still remain.

C. Analogies to Offline Age Authentication Are Misguided[164]

Offline age authentication occurs all of the time. Some entities are required by law to do it, such as retailers of items like cigarettes and alcohol. Other entities check age voluntarily, such as 21-and-over dance clubs that confirm patrons' ages prior to entry regardless of whether the patron will consume age-restricted items.

Because offline age authentication is so common and routine, it's tempting to assume that online age authentication is similarly common and routine. It's not. All of the problems with online age authentication outlined in Subpart II.A are more severe than in the offline world.

For example, online age authentication has marginal costs not present with offline age authentication. A retailer selling a restricted item must divert some worker capacity to age-authenticate buyers at the point of sale, but usually the retailer won't add more staff or incur other marginal costs to complete this task. In contrast, online publishers incur marginal costs both for system implementation and per-authentication.

Also, in offline authentication, an authenticator can make an age determination by visually inspecting the person and their documents without making or keeping copies of anything.[165] For example, a liquor store clerk age-

---

[163] ERIC N. HOLMES, CONG. RSCH. SERV., LSB11022, ONLINE AGE VERIFICATION (PART III): SELECT CONSTITUTIONAL ISSUES 4 (2023) [hereinafter CRS Report Part 3] (arguing—incorrectly in my opinion—that if "age verification technology has grown more effective, courts may be more willing to accept that requiring age verification can further a government interest in protecting minors. Likewise, if age verification solutions have become cheaper and more widely available, adopting such solutions may place less of a burden on website operators").

[164] For additional discussion of this issue, *see* Brief of Internet Law Professors Zachary Catanzaro, et al. as Amici Curiae in Support of Petitioners, Free Speech Coal., Inc. v. Paxton, 95 F.4th 263 (5th Cir. 2024), *cert. granted*, 2024 WL 3259690 (July 2, 2024) (No. 23-1122), https://perma.cc/9BYQ-Z6VM.

[165] *See* ITIF Report*, supra* note 31, at 11 ("because bars, casinos, and liquor stores do not store a copy of each customer's ID, these in-person ID checks pose lower privacy risks than do online ID checks").

authenticating a buyer can glance at the buyer's government-issued ID and confirm the buyer meets the age threshold. This evanescent visual inspection doesn't generate a paper trail or other records. In contrast, online authentications necessarily create electronic records of readers' data, at least temporarily. Simply by existing, those records expose the authenticated person to greater privacy and security risks.

Online age authentication also usually applies to more patrons than offline. When offline retailers are legally compelled to authenticate buyers' ages, the retailers typically can wait until the patron is ready to buy a restricted item like alcohol or cigarettes. For example, patrons of all ages can freely enter a liquor store; the law typically requires age authentication only when a buyer seeks to purchase a restricted item. In contrast, many segregate-and-suppress laws require publishers to authenticate every reader before they are allowed to enter the publisher's virtual premises, regardless of whether the reader will access a restricted resource.[166] As a result, online publishers incur higher authentication costs because they must authenticate readers before the publishers make any money from the reader, and even if the reader never needed to be authenticated (either because they were adults or because they weren't going to consume a restricted resource).

The requirement to authenticate online readers before allowing readers to enter the virtual premises differs substantially from offline content restrictions. Imagine, for example, if a bookstore[167] sells a mix of restricted and unrestricted items and a law required the bookstore to age-authenticate every patron before they could enter the store (so that the bookstore could block minors from entering). That kind of pre-transaction access barrier would impermissibly block minors from accessing constitutionally protected unrestricted materials; and it would dissuade adults from entering the premises to obtain materials (unrestricted and restricted) which they are legally entitled to obtain. Imposing that kind of pre-access screening online deviates from the offline world.[168]

---

[166] *See* Free Speech Coal., Inc. v. Rokita, 738 F. Supp. 3d 1041 (S.D. Ind. 2024). As a result, far more consumers are subjected to age authentication online compared to offline. *See Colmenero*, 689 F. Supp. 3d at 397.

[167] A bookstore is a good analogy to online publishers because restrictions of reader access to their venues has significant speech implications for both. This differs from other age-restricted offline venues, such as bars or casinos, where access restrictions typically have a minimal impact on the venue's speech. Like bookstores, physical space libraries are also targeted by offline segregate-and-suppress restrictions. *See*, *e.g.*, Fayetteville Pub. Libr. v. Crawford Cnty., 760 F. Supp. 3d 811 (W.D. Ark. 2024).

[168] *See Colmenero*, 689 F. Supp. 3d at 392 n.5 ("a more apt analogy would be that H.B. 1181

Lawmakers could take a narrower approach and require online age authentication only when a reader tries to access a restricted item or resource from the publisher.[169] This approach leaves the remainder of the publisher's offerings unburdened (in theory) by the age authentication mandate, but it is still problematic.[170] In addition to all of the other downsides of mandatory age authentication enumerated in Subpart II.A, the item-level authentication requirement would make publishers incur the costs of sorting through their catalogs to figure out which items are restricted; and to face legal consequences when they inevitably make classification errors. Many online publishers would balk at the imposition of those additional costs and legal risks; and publishers would mitigate the risks by overclassifying constitutionally protected items as restricted.

Finally, offline age authentication analogies often understate the speech impacts of online age authentication for both minors and adults.[171] The speech implications of requiring retailers to age-authenticate before selling liquor or cigarettes, or requiring casinos to age-authenticate gamblers, are minimal. In contrast, by imposing online age authentication mandates on publishers, the very thing being restricted is the publishers' speech (and, to the extent the reader also wants to be an online author, their authorship rights as well). Due to these differences in speech impacts, offline age authentication may be inherently less pernicious than online segregate-and-suppress laws.

---

forces movie theaters to catalog all movies that they show, and if at least one-third of those movies are R-rated, H.B. 1181 would require the movie theater to screen everyone at the main entrance for their 18+ identification, regardless of what movie they wanted to see").

[169] This is essentially the regulatory approach Congress took in the 1990s by passing the CDA and Child Online Protection Act (COPA), both of which ultimately were deemed unconstitutional.

[170] Among other concerns, "[c]reating segregated '18 or older' spaces in libraries and bookstores will powerfully stigmatize the materials placed therein, thus chilling adult access to this speech." *Fayetteville Pub. Libr.*, 760 F. Supp. 3d at 827.

[171] *See*, *e.g.*, Bobby Allyn, *How Will Australia's Under-16 Social Media Ban Work? We Asked the Law's Enforcer*, NPR (Dec. 19, 2024), https://perma.cc/JV9M-6GWC (Australia's eSafety Commissioner said "we should approach online safety the same way we have water safety," like requiring property owners to fence pools; but pool fencing minimally restricts speech, while implementing an online analog to "pool fencing" will be government censorship of speech).

IV. CONFLICTS BETWEEN MINOR SUBPOPULATIONS' NEEDS

Part II explained how the "segregate" part of segregate-and-suppress harms minors and adults. This Part now considers how the "suppression" part also harms minors.

Everyone acknowledges that minors have different needs from each other.[172] As one report explained, "different users will have different responses to the same platform—even when presented with the same content or experience . . . . Subgroups of social media users also have unique practices and vulnerabilities."[173]

Yet, there isn't any regulatory consensus about how to address the heterogeneity of minors' needs. The "suppression" obligation usually requires a publisher either to: (1) custom-tailor the suppression in response to each minor's idiosyncratic needs,[174] or (2) implement a one-size-fits-all approach for minors. Each option is problematic.

Idiosyncratic Suppression

---

[172] *See* Comm. on the Rts. of the Child, U.N. Convention on the Rts. of the Child, Gen. Comment No. 25 (2021) on Children's Rts. in Rel. to the Env't at 4, U.N. Doc. CRC/C/GC/25 (2021) [hereinafter UN Convention Committee Report] ("The risks and opportunities associated with children's engagement in the digital environment change depending on their age and stage of development"); Phippen, *supra* note 5, at 11 ("what is considered the 'best interests' can vary across cultures, individuals, and even within legal frameworks . . . [children have] multi-dimensional needs, encompassing physical, emotional, social, and developmental aspects."); CDT Report, *supra* note 57, at 29 ("young users experience online services and harms differently" and noting "the importance of understanding how harms manifested for different youth communities and how to tailor solutions to their unique challenges"); Ine Beyens et al., *The Effect of Social Media on Well-Being Differs from Adolescent to Adolescent*, 10 SCI. REPS. 10763, 10763 (2020), https://perma.cc/QW7V-KRP3 ("[P]erson-specific effects can no longer be ignored in research, as well as in prevention and intervention programs.").

[173] Common Sense & Hopelab Report, *supra* note 113, at 2.

[174] For example, the California AADC says "businesses should take into account the unique needs of different age ranges, including the following developmental stages: 0 to 5 years of age or 'preliterate and early literacy'; 6 to 9 years of age or 'core primary school years'; 10 to 12 years of age or 'transition years'; 13 to 15 years of age or 'early teens'; and 16 to 17 years of age or 'approaching adulthood.'" Cal. A.B. 2273 §1(a)(5) (2021-22). This age cohorting is obviously problematic for several reasons, including (1) age authentication processes may not yield sufficiently precise determinations; (2) the cohort schedule contemplates a typical maturation process, so it completely disregards minors who mature at non-typical rates; and (3) as discussed below, minors in the same age cohort will inevitably have conflicting informational needs.

Any idiosyncratic tailoring obligation isn't scalable. Any implementation that accounts for individual minors' needs must be fine-grained and artisanal. The associated implementation costs will be prohibitive for many publishers.

Regardless of costs, publishers are not well-positioned to accurately assess the needs of each individual minor.[175] Each publisher sees only a small slice of each minor's life, which means the publishers are functionally blind to that minor's needs.[176] That's true even for the minors most active on data-hungry social media. Publishers could attempt to gather more information about minors to make more nuanced determinations, but encouraging publishers to adopt more privacy-invasive practices isn't in the minors' interests either.

The publishers' limited perspective about their minor readers differ from other procedures that seek to advance minors' interests, such as court proceedings. As one court explained:

> The State argues that 'best interests' of a child is a legal term of art that is well-established in family law . . . .Those are specialized proceedings, however, in which finite custodial or dependency options must be considered by the court as to a particular child, on a particular factual record. A state court's application of the 'best interest' standard in those specialized proceedings provides no useful guidance as to how a covered business should understand what the 'best interests of children' generally means as used in the CAADCA.[177]

In other words, a court proceeding to adjudicate a minor's best interests will involve adversarial proceedings and discovery, due process, and possibly guardians ad litem. Online publishers have none of those. Instead, trying to maximize scalability with only limited information about each minor, publishers will make their decisions using error-prone assumptions and stereotypes about minors' needs. Those errors aren't just potentially legally risky mistakes. The errors could actively make things worse for minors, such as denying access to a

---

[175] Phippen, *supra* note 5, at 12 ("it is difficult to see how ALL young people's best interests can be incorporated into global platforms").

[176] *See* APA Advisory, *supra* note 2, at 3 ("the effects of social media are dependent on adolescents' own personal and psychological characteristics and social circumstances—intersecting with the specific content, features, or functions that are afforded within many social media platforms.").

[177] NetChoice, LLC v. Bonta, No. 22-CV-08861, 2025 WL 807961 (N.D. Cal. Mar. 13, 2025); *see also* Phippen, *supra* note 5, at 10 ("The 'best interests of the child' is a widely recognized standard in both law and child welfare practice, but its application and understanding can vary significantly.").

resource that the publisher doesn't realize the minor needs to maintain their mental health.

As a result, unless the publisher has enough information to accurately understand each minor's needs—which never is true, nor would we want it to be true—requiring publishers to cater to minors' idiosyncratic needs does not work.

One-Size-Fits-All Suppression

Because idiosyncratic suppression doesn't work, it makes sense that segregate-and-suppress laws often impose a binary suppression obligation, i.e., minors of all ages get one outcome, adults get a different outcome. For example, laws restricting minors' access to "harmful to minors materials" (i.e., pornography) online may make such material categorically off-limits to all minors, regardless of the reader's age and regardless of the material's explicitness.

A one-size-fits-all approach inevitably over-restricts content by reducing the acceptability standards to the lowest possible level, such as restricting teens from accessing material that is age-appropriate for them but not age-appropriate for toddlers.[178]

Content overblocking often gets referenced as a constitutional defect of censorship, but that's a symptom of a bigger problem. Due to the heterogeneous needs of minors, one-size-fits-all rules inevitably create conflicts between minor subpopulations,[179] where the suppression may help some subpopulations and hurt others. In the content overblocking scenario, older teens are hurt by losing access to materials that would be appropriate for them.

The conflicts among minor subpopulations can manifest based on a wide variety of socio-economic and demographic attributes beyond age, including geography, gender, race, education, personality type, family structure, neurodivergence, and much more. This diversity of needs virtually guarantees

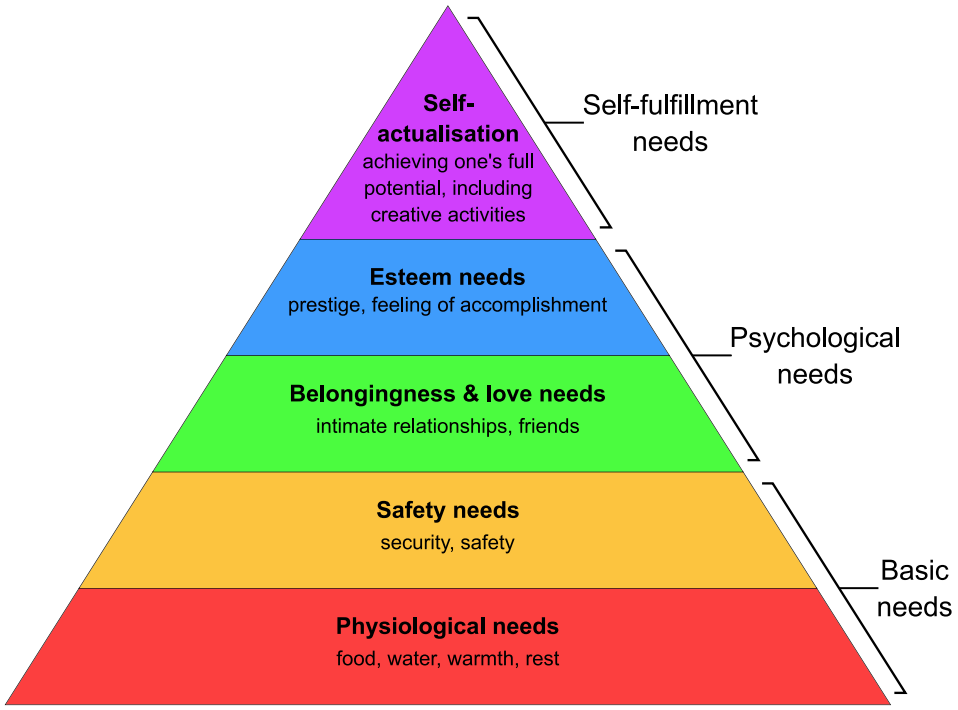
---

[178] A "website dedicated to sex education for high school seniors, for example, may have to implement age verification measures because that material is 'patently offensive' to young minors and lacks educational value for young minors." Free Speech Coal., Inc. v. Colmenero, 689 F. Supp. 3d 373, 394 (W.D. Tex. 2023), *rev'd* Free Speech Coal., Inc. v. Paxton, 95 F.4th 263 (5th Cir. Mar. 7, 2024), *cert. granted*, 2024 WL 3259690 (July 2, 2024); *see also* Stardust, *supra* note 47, at 2 (discussing how post-pubescent teens benefit from age-appropriate sexual information, which segregate-and-suppress laws may hinder).

[179] APA Advisory, *supra* note 2, at 3 ("Not all findings apply equally to all youth.").

that when one minor subpopulation benefits from a restriction, other minor subpopulations experience detriments. Given the inevitability that minor subpopulations have conflicting needs, many one-size-fits-all-minors segregate-and-suppress regulations cannot advance the best interests of *all* minors.[180]

Maslow's Hierarchy of Needs[181] helps explain why minor subpopulations routinely will have conflicting needs. The hierarchy arranges human needs into a pyramid, starting with basic physical needs for survival on the bottom and working up to higher-level cognitive and emotional accomplishments at the pyramid's top. This diagram[182] illustrates the hierarchy:



At lower levels of Maslow's hierarchy, minors' interests are likely to be homogeneous. Everyone needs air, food, water, sleep, and physical safety.

---

[180] Tonya Riley, *Children's Online Safety Bills Clear Senate Hurdle Despite Strong Civil Liberties Pushback*, CYBERSCOOP (July 27, 2023), https://perma.cc/HM2Q-EP32 (quoting Center for Democracy and Technology's Aliya Bhatia as saying that a segregate-and-suppress "bill just assumes what's good for some kids is good for all kids").

[181] Abraham H. Maslow, *A Theory of Human Motivation*, 50 PSYCH. REV. 370 (1943).

[182] By Androidmarsexpress - Own work, CC BY-SA 4.0, https://perma.cc/6H8B-CUQ4.

Regulatory interventions to promote those basic human needs typically will benefit all minors.[183]

Unlike those basic needs, people satisfy higher-level needs in diverse ways. Thus, as regulatory interventions target issues higher up in the pyramid, they are more likely to create conflicts among subpopulations.

For example, "friendship" is a middle band in the pyramid. Most of us aspire to have friendships, but people form, maintain, define, and express "friendship" in a variety of ways. A regulatory suppression of access to an online speech venue might boost friendships for some minors (i.e., by redirecting them away from toxic online environments and towards genuine offline connections) and degrade friendships for other minors (i.e., by depriving minors of connections with like-minded people they can find only online).[184] This intervention would have important—but divergent—effects on the psychological well-being of the affected subpopulations.

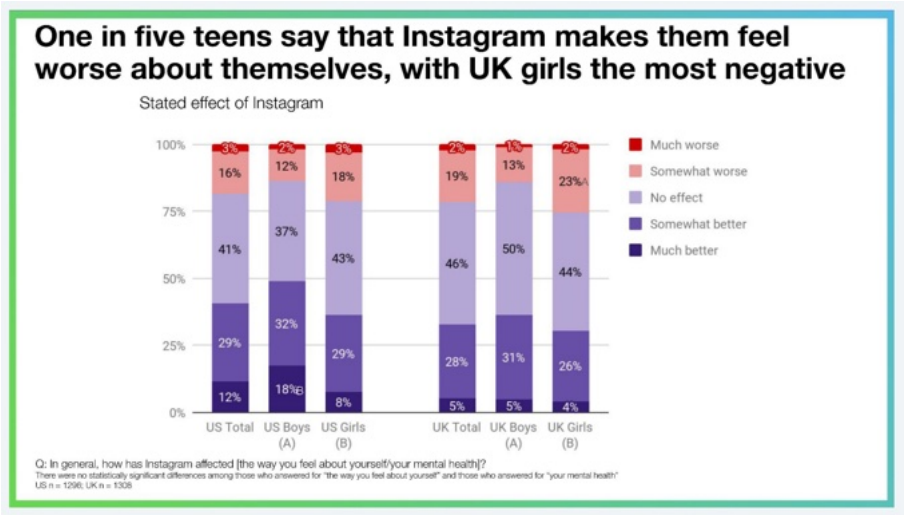
The following chart illustrates this divergence. It comes from an internal Facebook research report dated October 10, 2019, entitled "Teen Mental Health Deep Dive."[185] This chart has been referenced by lawmakers around the globe in support of their segregate-and-suppress laws.

---

[183] There will always be niche exceptions. For example, a program to promote a specific food item (e.g., peanuts) that provides healthy nutrition to a majority of people may simultaneously harm the minority of people allergic to that item.

[184] APA Advisory, *supra* note 2, at 4 ("[Y]ouths' psychological development may benefit from [specific types] of online social interaction, particularly during periods of social isolation, when experiencing stress, when seeking connection to peers with similar developmental and/or health conditions, and perhaps especially for youth who experience adversity or isolation in offline environments."); Jason Kelley, *Thousands of Young People Told Us Why the Kids Online Safety Act Will Be Harmful to Minors*, ELECTRONIC FRONTIER FOUND. (Mar. 15, 2024), https://perma.cc/3GRD-MVDQ ("Over and over again, young people told us that one of the most valuable parts of social media was learning that they were not alone in their troubles. Finding others in similar circumstances gave them a community, as well as ideas to improve their situations, and even opportunities to escape dangerous situations.").

[185] https://perma.cc/BT5G-SLNM (slide 21, which also provides additional context to interpret the data); *see generally* Pratiti Raychoudhury, *What Our Research Really Says About Teen Well-Being and Instagram*, META (Sept. 26, 2021), https://perma.cc/NLA3-K3EK (discussing Instagram's research findings in more detail).



It's easy to see why this chart caught lawmakers' attention. The headline is chilling: Instagram makes 20% of teens feel worse about themselves, with even higher numbers among teenage girls. The chart indicates that Instagram usage is distressing some minor subpopulations.

At the same time, the chart indicates that over 40% of U.S. teens said that Instagram made them feel *better* about themselves—more than twice as many as the U.S. teens who report that Instagram makes them feel worse about themselves.[186] Even with respect to U.S. girls, 37% say Instagram made them feel better about themselves compared to 21% who say it made them feel worse.

As a result, regulatory restrictions on Instagram access would likely benefit some minors, but at the cost of increasing the psychological or mental distress of other minors.[187] Any such regulatory intervention simply prioritizes some

---

[186] *See also* Beyens, *supra* note 172 ("Adolescents experienced an increase in well-being at moments when they had *passively* used Instagram"); *cf.* Common Sense & Hopelab Report, *supra* note 113, at 40 ("Of young people age 14 to 22 who use social media, 39% report that when they are feeling depressed, stressed, or anxious, using social media makes them feel better. On the other hand, 8% say it makes them feel worse . . . many young people mentioned that social media helps them focus on something positive, instead of mulling over negative concerns that might be out of their control.").

[187] *See* APA Advisory, *supra* note 2, at 4 ("Social media may be psychologically beneficial particularly among those experiencing mental health crises, or members of marginalized groups that have been disproportionately harmed in online contexts"); Common Sense & Hopelab Report, *supra* note 113, at 18 ("Teens and young adults who report elevated depressive symptoms are especially likely to say social media is an important resource for

minor subpopulations over others, which is the opposite of "protecting all children."

* * *

The fact that a law makes tradeoffs between subpopulation communities isn't unique to child safety laws. Virtually every new law makes policy winners and losers. Knowing this, legislatures are supposed to consider the needs of all affected constituents, assess the tradeoffs, and craft solutions that balance the competing interests as best as they can.

What's comparatively unique about the segregate-and-suppress laws is that legislatures do not publicly admit that their interventions will harm some minors. Such candor would be politically devastating.

Instead, legislatures pretend that their segregate-and-suppress laws categorically benefit all minors.[188] Segregate-and-suppress laws often include "legislative findings" that enumerate in detail the purported harms of the regulated technology, without any countervailing acknowledgement of how the technology benefits anyone.[189] Efforts like these perniciously erase disadvantaged subpopulations, invalidating their concerns *sub silento*. Legislative "findings" that assume all children will benefit from the regulation are not credible and deserve no judicial deference.

V. WHAT CAN POLICYMAKERS DO?

As this Article has made clear, segregate-and-suppress laws are riddled with problems. Fortunately, they are not the only tool in policymakers' regulatory toolkit to improve child safety online. This Part explores some other tools available to policymakers, as well as some suggested methodological improvements.

---

making themselves feel better and finding a range of support and advice when they need it . . . When compared with their peers, the role of social media in helping youth feel less alone is far more important for those who report depressive symptoms."); MARWICK ET AL., *supra* note 41, at 35 ("young people are not a monolith; content that empowers one teenager may make another anxious"). *See generally* DIGITAL TRUST & SAFETY P'SHIP, AGE ASSURANCE: GUIDING PRINCIPLES AND BEST PRACTICES 13 (Sept. 2023), https://perma.cc/C4RG-6ESQ ("Age assurance would be counterproductive if it had the effect of eliminating access to digital services for wide swaths of users for whom those services are appropriate.").

[188] *See*, *e.g.*, STOP Report, *supra* note 96, at 12 (explaining that segregate-and-suppress laws "claim to protect children and teens, [but] they fail to truly consider the needs of the diverse and vast group of people they cover").

[189] For example, the assembly bill enacted as California's AADC enumerates ten legislative findings about the Internet's problems, none of which reference the Internet's benefits. A.B. 2273, § 1, 2021-22 Cal. Assemb., Reg. Sess. (Cal. 2022).

A. Expanding the Policy Toolkit

There are no easy paths to protecting minors online, and no single policy intervention will magically make children safe online.[190] Making real progress on child safety online will require multiple overlapping and coordinated policy efforts.

Similarly, no single player in the ecosystem can unilaterally solve the problem.[191] As the expression goes, it takes a village to raise a child.[192] To help minors stay safe—and to help them grow, learn, and self-actualize[193]—online will require cooperation and coordination among many stakeholders, including children, parents, other family members, other community members, teachers and the school system, the publishers, outsourcing vendors, civil society advocates, the government, and others.[194] In contrast, segregate-and-suppress laws try to force online publishers to magically solve a society-wide problem, even though the publishers lack the required expertise, resources, or

---

[190] CDT Report, *supra* note 57, at 6 ("No one-size-fits-all approach fixes current issues . . . most solutions raise thorny tradeoffs."); ITIF Report, *supra* note 31, at 4 ("Debates over how best to protect children, and what potential harms society needs to protect children from are much older than the Internet and encompass much more than online harms. Problems facing children in society have never been easy to solve, and solutions to those problems often raise similar concerns to many of the proposed solutions to online harms, such as free speech, privacy, and parents' rights.").

[191] CDT Report, *supra* note 57, at 6–7 (noting "the necessity of collective efforts that would involve parents, educators, platform designers, and policymakers. Collaboration across these groups was identified as crucial for reaching feasible and balanced actionable steps.").

[192] This phrase is probably an African proverb. Joel Goldberg, *It Takes a Village to Determine the Origins of an African Proverb*, NPR (July 30, 2016), https://perma.cc/P8ZH-TYM3.

[193] As the OECD observed, "Digital technologies have become central to children's well-being and development and the digital environment is an integral part of their lives, offering important opportunities for self-expression, learning, socialising, connecting with community and culture, and the enjoyment of their rights." OECD Report, *supra* note 25, at 7.

[194] Greens Report, *supra* note 18, at 88 ("[Policymakers] should conceive children online protection within a broad spectrum of non-invasive measures, both technical and non-technical, which include the involvement of parents, teachers and other educators, social workers, and caregivers as an important source of children support."), NTIA Report, *supra* note 1, at 47 ("[A]ddressing health, safety, and privacy concerns for youth online must involve an on-going, whole-of-society approach in which industry, parents and caregivers, schools, health providers, other community-based organizations, and policymakers play their roles . . ."); Park et al., *supra* note 11, at 61 ("[W]e call on a whole village of parents, caregivers, researchers, technology designers/developers, clinicians, educators, and policymakers to put efforts toward positive media parenting and resilience-based approaches to promote the digital well-being of adolescents."); Phippen, *supra* note 5, at 9 ("Adopting a holistic view of collaboration among stakeholders to support young people in online risk-taking and decision-making is more effective, as each stakeholder can contribute their expertise to the safeguarding role."). *See generally* URIE BRONFENBRENNER, THE ECOLOGY OF HUMAN DEVELOPMENT: EXPERIMENTS BY NATURE AND DESIGN (1979).

relationships.[195] Child safety online needs a whole-of-society response, not a delegate-and-pray approach like segregate-and-suppress.

With those caveats, this Part suggests a few options policymakers might explore instead of segregate-and-suppress laws:

Digital Literacy and Citizenship Education for Children. When minors mature into adults, they will need digital expertise to navigate social situations and succeed in the labor market. As a United Nations committee noted, children "reported that digital technologies were vital to their current lives and to their future."[196]

Suppression policies counterproductively leave minors ill-prepared for their future.[197] A European research group explained that segregate-and-suppress laws prevent minors "from learning and gradually developing online skills. Instead of abruptly granting access to new services at a specific age, a more effective approach involves providing supportive tools for children to build resilience and navigate online services safely."[198]

From a national perspective, segregate-and-suppress laws potentially put U.S. minors at a competitive disadvantage regarding the development of their digital skills compared to minors who grow up in countries with more progressive Internet policies.

To avoid these consequences, policymakers should ensure that minors develop the digital literacy and citizenship skills they need for their future personal and professional growth.[199] To help minors prepare for the digital-first

---

[195] Phippen, *supra* note 5, at 35 (describing this legislative approach as "platform scapegoating" and saying that "platforms cannot be to blame for everything that happens online, no matter how politically attractive it is to claim this"). Phippen also laments the "the global convergence towards a regulatory stance prioritizing punitive measures over multi-stakeholder involvement." *Id.* at 19.

[196] UN Convention Committee Report, *supra* note 172, at 1.

[197] *See* Tara García Mathewson, *Frustrated by School Web Filters, One Teenager Created His Own*, CALMATTERS (July 24, 2024), https://perma.cc/26B3-2RH7 (highlighting one high school student who "points out that schools' overly strict [web filtering] controls disappear as soon as kids graduate. 'That's a recipe for disaster,' he said. Kids, he contends, need to learn how to make good choices about how to use the internet safely when trusted adults are nearby so they are ready to make good decisions on their own later."). *Cf*. Jack Nicas, *The Internet's Final Frontier: Remote Amazon Tribes*, N.Y. TIMES (June 2, 2024), https://perma.cc/NJ98-27Z7(discussing some challenges the Amazon-based Marubo tribe experienced when it connected to the Internet via Starlink with limited training and preparation).

[198] Greens Report, *supra* note 18, at 38.

[199] APA Advisory, *supra* note 2, at 8 ("Adolescents' social media use should be preceded by training in social media literacy to ensure that users have developed psychologically-informed competencies and skills that will maximize the chances for balanced, safe, and meaningful social media use."). As one child said, "Kids don't need protection we need

future, governments should ensure that they learn how to navigate the Internet, become discerning content consumers, develop online resilience, and use the Internet as a tool to become more engaged and productive citizens[200]—rather than learn to fear or avoid it.[201] As danah boyd observed, "to raise children who can function in our complex world, we need to teach them how to cross the digital street safely."[202]

Train Parents to Become Better Teachers. As the expression goes, parents are their children's first teachers. However, parents don't have any specialized knowledge to share with their children about how to use the Internet safely and wisely. Policymakers should teach parents how to help and guide their children online. If governments provide more help to parents, then parents can become more effective teachers for their children's digital futures. Governments "should support parents and caregivers in acquiring digital literacy and awareness of the risks to children in order to help them to assist children in the

---

guidance. If you protect us you are making us weaker we don't go through all the trial and error necessary to learn what we need to survive on our own . . . don't fight our battles for us just give us assistance when we need it." Tanya Byron, *Safer Children in a Digital World: The Report of the Byron Review*, BYRON REV.: CHILD. & NEW TECH. (2008), https://perma.cc/2FL5-MJW2.

[200] *See* H.B. 1575, 2023 Gen. Assemb., Reg. Sess. (Va. 2023) (creating an Internet Safety Advisory Council "to establish model instructional content on certain student internet safety topics"); BERNARD, *supra* note 26 (discussing educational proposals to "improve children's safety online"); LGBT Tech Report, *supra* note 96 (advocating for digital literacy efforts in state legislatures); Phippen, *supra* note 5, at 151 (stating that regulators should move "beyond a narrow focus on preventing harm through bans and restrictions, towards empowering young people with the knowledge, resilience, and support they need to navigate the digital world safely"); *Be Internet Awesome in Central and Eastern Europe Second Impact Report School year 2023-2024*, BE AWESOME INTERNET (Oct. 2024), https://perma.cc/V95L-9S98 (discussing how digital literacy efforts benefited students).

[201] As one paper explained:

> In today's digitized world, one of the most important developmental tasks for adolescents is to acquire proficiency in managing online interactions and safeguarding themselves against digital risks . . . we fail to account for how our paternalism and protectionism hinders teens' ability to become informed, thoughtful, and engaged adults . . .
>
> taking a fear-based and controlling approach disproportionately focused on adolescent vulnerability does not prepare teens for future online adversity, nor does it productively advance the field.

Park et al., *supra* note 11 (quoting in part danah boyd, It's Complicated: The Social Lives of Networked Teens 28 (2014)).

[202] boyd, *supra* note 95. As an added benefit, minors can observe pro-social behaviors and model their own behavior accordingly. APA Advisory, *supra* note 2, at 4 ("Social media offers a powerful opportunity for socialization of specific attitudes and behaviors, encouraging adolescents to follow the opinions and prosocial acts of others. The discussion of healthy behaviors online can promote or reinforce positive offline activity and healthy outcomes.").

realization of their rights, including to protection, in relation to the digital environment."[203] As a British professor explained:

> Parents and guardians are often the first line of defence, providing guidance, setting boundaries, and monitoring their children's online activities. However, many parents feel ill-equipped to manage the complexities of the digital world, especially given the rapid pace of technological change. Providing parents with the necessary resources, education, and support to navigate these challenges is essential.[204]

Fund More Research.[205] There are many unanswered questions about how the Internet impacts minors (both positively and negatively), especially with respect to niche subpopulations.[206] The government could fund more research into these issues to lay a proper foundation for evidence-based policymaking.[207]

The government can also promote and highlight research findings that will help stakeholders learn from other stakeholders' experiences. What's working to improve children's safety online? What isn't? Government support can help best practices proliferate among Internet stakeholders.

---

[203] UN Convention Committee Report, *supra* note 172, at 4; *see also* Park et al., *supra* note 11, at 58 ("The landscape of adolescent online safety has shifted toward collaborative family-based approaches, fostering communication, privacy, and autonomy within digital family contexts.").

[204] Phippen, *supra* note 5, at 154.

[205] *See* NTIA Report, *supra* note 1 (laying out a detailed research agenda).

[206] APA Advisory, *supra* note 2, at 3 ("[R]elatively few studies have been conducted with marginalized populations of youth, including those from marginalized racial, ethnic, sexual, gender, socioeconomic backgrounds, those who are differently abled, and/or youth with chronic developmental or health conditions."); Park et al., *supra* note 11, at 60 ("[F]ew evidence-based interventions to empower foster youth self-regulation and online safety have been developed.").

[207] CDT Report, *supra* note 57, at 7 ("Most [researchers] agreed that improved access to data is vital to develop evidence-informed policy."); UN Convention Committee Report, *supra* note 172, at 5 ("Regularly updated data and research are crucial to understanding the implications of the digital environment for children's lives, evaluating its impact on their rights and assessing the effectiveness of State interventions. State parties should ensure the collection of robust, comprehensive data that is adequately resourced and that data are disaggregated by age, sex, disability, geographical location, ethnic and national origin and socioeconomic background."); Phippen, *supra* note 5, at 155 (claiming we need "a progressive, evidence-based approach to online safety that aligns with the lived experiences and needs of young people"); APA Advisory, *supra* note 2, at 8 ("A substantial investment in research funding is needed, including long-term longitudinal research, studies of younger children, and research on marginalized populations.").

The government could also support the (1) the collection and availability of data to facilitate studies;[208] (2) development and proliferation of content moderation and trust-and-safety tools that can improve the entire industry;[209] and (3) new tools that help consumers, including minors, better manage their online experiences.[210]

Implement Solutions for Everyone, Not Just Minors. If a policy idea would be good for minors, it might be a good idea for adults, too. If so, the policy should be extended to the entire population, not just minors. For example, if lawmakers are concerned about publishers' privacy practices towards minors, Congress should adopt a comprehensive federal reader privacy law that applies equally to both minors and adults.[211]

Enforce Existing Laws. Children face a wide range of threats online, but existing law already regulates many of those threats. We should ensure that we have enough law enforcement officers "walking the virtual beat" to proactively thwart (and deter) those threats and to appropriately prosecute violations.[212]

B. Use Better Policymaking Methodologies

Given the high stakes involved when protecting minors online, especially in light of the risks of harming minor subpopulations, regulators working on online child safety matters should use best practices for policymaking, such as:

Do Adequate Research. Policymakers should identify all of the minor subpopulations who will be affected by the proposal and explicitly acknowledge the likelihood that those subpopulations have conflicting interests.

---

[208] *See* APA Advisory, *supra* note 2, at 8 ("Access to data among independent scientists (including data from tech companies) to more thoroughly examine the associations between social media use and adolescent development is needed.").

[209] The industry has made some progress in this regard. *See, e.g.,* ROOST, https://perma.cc/A2LU-5NA8 (archived Apr. 14, 2025) ("ROOST develops, maintains, and distributes open source building blocks to safeguard global users and communities."). Government support could turbocharge these efforts.

[210] *See* Park et al., *supra* note 11, at 58 (discussing interventions that help teens become more intentional about their social media usage and "real-time nudges" to help teens avoid various online risks).

[211] *See* Tate Ryan-Mosley, *Child Online Safety Laws Will Actually Hurt Kids, Critics Say*, MIT TECH. REV. (Oct. 2, 2023), https://perma.cc/CG99-MS9G (quoting S.T.O.P. executive director Albert Fox Cahn as saying: "Rather than misguided efforts to track every user's age and identity, we need privacy protections for every American.").

[212] *See The Future of Online Safety for Kids: Legislative Changes on the Horizon*, CONGRESS. INTERNET CAUCUS (Mar. 13, 2025), https://perma.cc/7SCW-PF2R (including remarks from Maureen Flatley of Stop Child Predators).

Then, policymakers should speak with, and hear from, minors in each affected subpopulation.[213] As the OECD explained, "Children are active digital citizens and both service providers and policymakers should involve children in discussions about online safety, design processes, and policy formulation. By giving children a seat at the table, stakeholders can help to ensure that the digital environment is shaped with children's best interests at heart."[214] A United Nations committee reinforced the importance of treating children as vocal stakeholders, not silent targets of regulation:

> States parties should involve all children, listen to their needs and give due weight to their views . . .
>
> States parties are encouraged to utilize the digital environment to consult with children on relevant legislative, administrative and other measures and to ensure that their views are considered seriously . . .[215]

Respect Minors' Rights to Speak. Minors have First Amendment-protected rights to express themselves online,[216] and many segregate-and-suppress laws disrupt those rights when they restrict minors' access to online publication tools.[217] As the Supreme Court indicated, "While in the past there may have

---

[213] *See* OECD Report, *supra* note 25, at 40–41; *see also* Common Sense & Hopelab Report, *supra* note 113, at 1 ("To better understand youth mental health and its relationship to social media use, researchers have shown that it is critically important to listen to and honor the experiences of youth themselves."); NTIA Report, *supra* note 1, at 46 ("Young people are active participants in their own online safety and have crucial insights into their own experiences and those of their peers. Their voices should be incorporated into policymaking discussions at every level . . . ."); MARWICK ET AL., *supra* note 41, at 35 ("[W]e need to center young people. What is at the root of their struggles? What do young people need and want to feel empowered?"); Citron & Waldman, *supra* note 114, at 47 ("Any conversation and policymaking effort about children's privacy should begin with young people themselves . . . . The perspectives of youth from minoritized groups are especially important."). Currently, "[r]arely is there an organized effort to hear from children during the [policymaking] process." Stacey B. Steinberg, *The Myth of Children's Online Privacy Protection*, 77 SMU L. REV. 441, 470 (2024).

[214] OECD Report, *supra* note 25, at 6. *Cf*. Luu, *supra* note 113 (explaining how Australian lawmakers didn't give minors any opportunity to oppose the Australian ban on social media for under-16s).

[215] UN Convention Committee Report, *supra* note 172, at 3.

[216] CRS Report Part 3, *supra* note 163, at 3. Minors also have associational rights that may be disrupted by segregate-and-suppress laws. *See* UN Convention Committee Report, *supra* note 172, at 11 ("[T]he digital environment enables children, including children human rights defenders, as well as children in vulnerable situations, to communicate with each other, advocate for their rights and form associations.").

[217] ITIF Report, *supra* note 31, at 14 ("[M]uch of this debate treats children as completely

been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in particular."[218] Regulators should ensure that minors can raise their voices in the "most important places for the exchange of views."[219]

Don't Sidestep the Difficulties of Age Authentication. Regulators sometimes enact segregate-and-suppress laws without any clarity about how publishers will implement the age authentication mandate. For example, the California Age-Appropriate Design Code Act (AADC) imposed age authentication mandates,[220] but the California legislature didn't resolve how the regulated businesses would implement age authentication or show any appreciation for the associated risks the mandate posed to minors. The California legislature essentially admitted its ignorance in a subsequent segregate-and-suppress law,[221] which delegated rule-making about age authentication to the state Attorney General to do the work the legislature skipped when passing the AADC.

Similarly, Australia has categorically banned under-16 minors from using social media.[222] To effectuate the ban, the law requires social media services to take "reasonable steps" to determine their readers' ages. However, the Australian legislators didn't know what those reasonable steps would be.[223] Worse, a year prior to this enactment, the Australian government had explained

---

lacking these [free speech] rights."). The United States has not ratified the United Nations Convention on the Rights of the Child (UNCRC), but segregate-and-suppress policies likely violate several of its provisions. *See* Greens Report, *supra* note 18, at 28.

[218] Packingham v. North Carolina, 582 U.S. 98, 104 (2017). The court continued: "to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights." *Id.* at 108.

[219] *Id*. at 98; *see also* Rand Paul, *Censoring the Internet Won't Protect Kids*, REASON (Aug. 20, 2024), https://perma.cc/664X-P9TC ("KOSA [a segregate-and-suppress bill] is a Trojan horse. It purports to protect our children by claiming limitless ability to regulate speech and depriving them of the benefits of the internet, which include engaging with like-minded individuals, expressing themselves freely, as well as participating in debates among others with different opinions.").

[220] CAL. CIV. CODE § 1798.99.31(a)(5).

[221] Protecting Our Kids from Social Media Addiction Act, S.B. 976, Cal. S., Reg. Sess. (Cal. 2024), codified at CAL. HEALTH & SAFETY CODE § 27006(b).

[222] *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) (Austl.) https://perma.cc/4S3E-LSGY (archived May 4, 2025).

[223] Natasha Lomas, *As Australia Bans Social Media for Kids Under 16, Age-Assurance Tech is in the Spotlight*, TECHCRUNCH, https://perma.cc/VHA4-8P3G (Dec. 7, 2024) ("The legislation was passed before key details were defined — such as the definition of 'reasonable steps.'"); *see* Allyn, *supra* note 171 (indicating that, at the time, Australia's eSafety Commissioner wasn't sure what age authentication methodology will be used, but she was impressed by a service that claims to achieve 99% accuracy based on a reader's hand gestures).

that "each type of age verification or age assurance technology comes with its own privacy, security, effectiveness or implementation issues . . . . the age assurance market is, at this time, immature . . . a decision to mandate age assurance is not ready to be taken."[224] Did the government magically solve all of the known and troubling problems with age authentication in that year? Or did the Australian parliament pass and pray?

Passing a segregate-and-suppress law, without ensuring that publishers have reasonable and non-harmful ways of implementing the age authentication requirement, is irresponsible policymaking. If legislatures can't understand the authentication mechanics and properly account for its pitfalls, they aren't ready to impose the mandate.

VI. CONCLUSION

The Article has highlighted many flaws with segregate-and-suppress laws. That's a good reason for legislatures to rethink their affinity for those laws. This Conclusion now addresses the obvious follow-up question: if the laws are so bad, why do regulators keep pushing them?[225]

It's tempting to assume that proponents of segregate-and-suppress laws genuinely believe that the laws are the best way to protect children. The problem with this assumption is that regulators repeatedly demonstrate that they don't understand, or care about, the many downsides of segregate-and-suppress laws discussed in Parts I and II. Instead, regulators are embracing simplistic one-note solutions to complex, multifaceted social problems.[226] As a result, segregate-and-suppress laws are unlikely to accomplish their purported goals[227]—and are guaranteed to make the Internet worse for everyone, including minors.

---

[224] AUSTL. DEPT OF INFRASTRUCTURE, TRANSP., REG'L DEV., COMMC'NS & THE ARTS, GOVERNMENT RESPONSE TO THE ROADMAP FOR AGE VERIFICATION 2 (Aug. 2023), https://perma.cc/KEL7-TMZ4.

[225] Phippen offers some ideas, including regulatory "path dependence," isomorphism, regulators feeling that they must "do something," and moral panics. Phippen, *supra* note 5, chs. 2-3.

[226] *See, e.g.*, Technet Letter to Sens. Cantwell & Cruz, July 26, 2023, https://perma.cc/N6PN-EEQ5 (saying "each of these bills are well-intentioned in seeking to protect children online," and then going on to criticize them all); MARWICK ET AL., *supra* note 41, at 26 ("While acknowledging the well-intentioned nature of [child online safety legislation], critics have highlighted how these bills will" cause various harms).

[227] *See* Angel & boyd, *supra* note 93, at 92 ("As the history of technology repeatedly shows us, techno-deterministic and techno-solutionist approaches are unlikely to achieve their purported goals.").

Worse, some segregate-and-suppress proponents are intentionally using segregate-and-suppress laws to push their censorship agendas.[228] For example, Russell Vought, an architect of Project 2025 and President Trump's Director of the Office of Management and Budget, admitted that age authentication mandates would intentionally serve as a "back door" way to censor pornography.[229]

Segregate-and-suppress laws can be an excellent Trojan horse for regulators pushing for Internet censorship. A proposed law avoids a lot of critical scrutiny because it claims to protect children, but that enables regulators to cynically treat children as political props in their quest to obscure their censorship agenda. Because it can be hard to disentangle a legislature's true motives for embracing segregate-and-suppress, each proposal should be reviewed with high skepticism.

Instead of doubling down on segregate-and-suppress, regulators should be working to develop better alternatives.[230] Any real progress towards protecting minors online will only come from tedious and politically unrewarding work to understand and balance the many tradeoffs;[231] and any meaningful solution will require collaboration and coordination across many stakeholders. When we direct our limited policymaking capacity towards segregate-and-suppress laws, we're not making progress towards solutions that actually have a chance of protecting children online.[232]

---

[228] STOP Report, *supra* note 96, at 1 (calling the laws a "legislative wolf dressed in sheep's clothing"); Mike Masnick, *Heritage Foundation Admits KOSA Will Be Useful For Removing Pro-Abortion Content . . . If Trump Wins*, TECHDIRT (Sept. 16, 2024), https://perma.cc/N5JX-3R27.

[229] Michael McGrady, *Don't Forget That The Same People Banning Books Want To Ban Porn*, TECHDIRT (Sept. 24, 2024), https://perma.cc/F8NU-B8KV.

[230] Phippen, *supra* note 5.

[231] CGO Report, *supra* note 12, at 22 ("Age assurance policy is hard.").

[232] *E.g.*, Stardust, *supra* note 47, at 2 (positing that age authentication efforts "divert resourcing that could be spent on strategies that are proven to support healthy sexual development").