

A photograph of two young boys, one slightly older than the other, both with short brown hair, looking intently at a tablet held by the older boy. They are in a room with soft lighting, and some toys are visible in the background.

2024

U.S. Age Assurance Is Beginning to Come of Age:

The Long Path Toward Protecting
Children Online and Safeguarding
Access to the Internet

U.S. Age Assurance Is Beginning to Come of Age: The Long Path Toward Protecting Children Online and Safeguarding Access to the Internet

By Ariel Fox Johnson

Special thanks and acknowledgement to Common Sense Media law student interns Evan Engel, Douglas Alfidi, Joshua Barclay, Veronica Chapman, and Ashley Leon, and Common Sense Media staff Amina Fazlullah, Holly Grosshans, and Danny Weiss, for their contributions to this paper.

September 30, 2024

Executive Summary

In the history of the internet, it has been difficult to determine how old users are online. Sites and services have thus far largely relied upon stated ages. This remains a concern for the safety and privacy of children and teens. The digital world was largely not created with young people in mind—and merely relying on a the checking of a box to attest to age leaves them unprotected. As harms pile up, and technology advances, policymakers across the globe are increasingly turning to more effective measures to assess age, in order to protect children and teens from addictive and unhealthy features, inappropriate purchases, adult content, and privacy risks. New laws mandate or encourage some form of age estimation, be it verification via ID, a technical age-flag signal, or some other "commercially reasonable" method.

In the U.S., much of this action is happening at the state level. And much of it is being challenged by a powerful tech lobby for allegedly violating the First Amendment. This paper assesses the current landscape of age assurance, technologically, legislatively, and in industry practice, and considers whether it is possible to develop age assurance practices that are privacy protective, proportionate, fair, and equitable—and that satisfy U.S. constitutional concerns. The paper concludes that there is clearly still work to be done, by industry, families and individual users, and policymakers, but it looks increasingly possible to achieve this goal.

This paper makes several recommendations. Technology companies must prioritize age assurance, with the same energy they focus on assessing age for marketing purposes. Families and teens should voice their preferences and concerns with respect to age assurance. And lawmakers must encourage innovation and flexibility in the age assurance space.

Introduction

There is an unprecedented and global focus on protecting children and teens online. In the United States, both in Congress and across the states, new laws and legislative efforts are coming from many political angles, and they vary in scope and focus, from bans on children using social media to requirements to build social media sites with youth's best interests in mind, to require privacy protections, and to prohibit children from accessing adult content. They are united, if at all, on a desire to protect youth—though what "protect youth" means is itself a point of disagreement that undergirds differences in approach.

Not everyone wants to enact laws to protect children and teens online. And opponents also come from a variety of perspectives. Many of these opponents are part of a Big Tech coalition that opposes any regulation of its industry at all. But opponents come from a civil liberties angle as well. They have found common ground over concerns that "protecting children" will turn into de facto universal ID requirements for adults that will threaten privacy and free speech. The idea behind age verification (i.e., checking IDs) is that to protect children online, platforms must have a definitive way to determine whether a user of their platform is underage. But not all age assessment is the same. Today there are many ways to assess age that do not place the same level of burden on users as the checking of IDs. The broad concept of assessing age is called "age assurance." It includes age verification, but it also includes other less certain concepts like age estimation.

This paper examines youth online protection and age assurance efforts in the U.S. It looks at the history of age assurance, considers current mechanisms of age assurance—those that exist as a possibility, and those that are currently employed by social media companies in the U.S.—and it considers what kids are experiencing on social

media platforms, as well as what lawmakers are motivated to fix. And because a number of other countries have taken more advanced steps on age assurance, this paper also looks at the international age assurance regulatory environment.

The paper raises several important questions. Is it possible for policymakers, technologists, and concerned advocates to work together to develop age assurance practices that are privacy protective, proportionate, fair, and equitable? And can age assurance satisfy U.S. constitutional concerns while also meeting the needs of children and their families? Though it will require continued efforts from everyone—tech companies, experts, and lawmakers—we think the answer to both questions is yes.

On the Internet, Nobody Knows You're a Kid – Historically Speaking

Concerns over children accessing adult content or experiences are not new, and date back to the nascency of the popular internet of the 1990s. In the midst of public fear over the dangers of the internet, particularly children being exposed to pornographic content online, Congress passed the Communications Decency Act (CDA) of 1996. The CDA criminalized transmitting obscene or indecent material to children, but offered a safe harbor if companies had "effective" age verification. The CDA was challenged, resulting in the Supreme Court decision *Reno v. American Civil Liberties Union*. In the decision, the court found that the law was vague and overbroad, and would burden adults' and children's access to constitutionally protected materials. The age verification safe harbor was not sufficient to address the overbreadth.¹ The court questioned whether there was any effective way to determine the age of users in newsgroups or chat rooms, and noted that the lower courts said the government had offered no evidence that there was "a reliable way to screen recipients and participants in such forums for age."² It also expressed that even if technology existed to block access to certain chat rooms related to indecent subjects, it would not be possible to block access to such material and not other materials. It expressed concerns that credit cards could as a technical matter only be used to screen age when associated with transactions. Ultimately, concerns about an "absence of viable age verification" helped lead the court to hold that two provisions of the CDA were unconstitutional.

Shortly thereafter, in 1998, in response to concerns over marketing and interactions with strangers online, the Children's Online Privacy Protection Act (COPPA) was passed, which requires websites to obtain parental consent before collecting personal information from children under the age of 13.³ COPPA did not require age verification. Early attempts at age assurance lacked the technological abilities to do much more than require self-reporting.⁴ Thus, many individuals in the U.S. experience age assurance online as simply checking a box that they are over 13.

¹ James Grimmelman, *The Return of Age Verification Laws*, 67 COMMS. OF THE ACM 34, 35 (2024), <https://james.grimmelman.net/files/articles/return-of-age-verification.pdf>.

² *Reno v. American Civil Liberties Union*, 521 U.S. 844, 855-56 (1997).

³ Ariel Fox Johnson, *13 Going On 30: An Exploration Of Expanding Coppa's Privacy Protections To Everyone*, SETON HALL J. OF LEG. AND PUB. POL. 419, 420 (2020), <https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1168&context=shlj>.

⁴ Lorna Cropper, *Age Assurance: A Modern Coming of Age Approach to Ensure the Safety of Children Online and an Age Appropriate Experience*, FIELD FISHER: INSIGHTS (Jan. 12, 2024), <https://www.fieldfisher.com/en/insights/age-assurance-a-modern-coming-of-age-approach-to-ensure-the-safety-of-children-online>.

Age Assurance Scenarios

The situations in which companies or lawmakers have sought age assurance vary. Primarily these situations fall into three categories: design, access, and privacy. As the reasons for seeking age assurance vary, so do the consequences of assurance procedures getting age wrong. (And so do the potential constitutional consequences, as discussed later.) As addressed in the table below, concerns about age assurance leading to privacy protections for everyone, or limiting addictive features for everyone, may be less concerning or problematic than if age assurance unwittingly cuts off access to an adult making a desired purchase or obtaining desired content. This is why one of the key considerations in determining which age assurance method is most viable in a given situation is whether the method chosen has the potential consequence of limiting access to products or content for adults, and what has been done to mitigate this issue.

Examples of when age assurance has been used or called for to protect minors.

Privacy	Product Design/Features		Access		
Data protections (avoidance of profiling, targeted ads, commercialization of data)	Addictive features (notifications, auto-scroll)	Unhealthy features (algorithmic targeting, plastic surgery filters)	Purchases (for adult products or for any online purchases)	Adult content (pornography, violence, gambling, contact with strangers)	Social media platforms

Modern Methods of Age Assurance

Age assurance is an umbrella term that encompasses everything from self-declaration to verification using government IDs.⁵ Methods vary in terms of ease, cost, accuracy, equity, and amount of information collected.

As noted above, in 1997, in *Reno v. ACLU*, the U.S. Supreme Court noted that there was no evidence that there was a reliable way to conduct age assurance. A year later, in 1998, when COPPA was passed, sites that were not directed to children could typically gain knowledge of a child user only if the child told them. But today, and as they have for some time, companies employ many ways to assess a user's age, whether because of legal obligations or financial self-interest.

1. Self-Attestation

Self-attestation is a basic form of age assurance in which an online service explicitly asks the user for their age and considers the response to be truthful. The responses available to the user may be specific ages and/or age ranges. This method is among the least data-intrusive, although it can include collecting a birth date. Many online services

⁵ See 5RIGHTS FOUNDATION, BUT HOW DO THEY KNOW IT IS A CHILD?: AGE ASSURANCE IN THE DIGITAL WORLD 24 (Oct. 2021), https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf.

already rely on self-attestation to comply with COPPA, which requires additional statutory privacy protections for children under the age of 13.⁶

Self-reporting of age also appears in parts of the internet designed for adults. This is the most common method of age verification used by alcohol retailers online. Although age gates for such websites are not legally mandated, they are required by manufacturers under the codes adopted by the Brewers Association, the Beer Institute, the Wine Institute, and the Distilled Spirits Council. The Federal Trade Commission's "Self-Regulation in the Alcohol Industry" reports for 2008 and 2014 include age-gate recommended practices.⁷ Many consumers are familiar with clicking "Yes/No" or inputting their birth date to indicate they are at least 21 years of age.

There is an obvious concern that self-attestation, while easy, is insufficient in terms of accuracy. Self-reporting of age is clearly very easy to circumvent, even for the single-digit crew. ("I just put in the year Mommy was born!"⁸). It may be appropriate in some situations, but it is clearly inadequate and inappropriate for use in high-risk situations. However, there is reason to believe that certain design features can enhance the effectiveness of self-attestation. For example, if online services framed self-attestation as a benefit rather than a barrier, response accuracy would increase.⁹ If users knew that the younger their self-reported age, the more privacy protections they would have in relation to the online service, they might be more likely to report accurately. Similarly, if users did not automatically assume that self-attestation in age assurance leads to blocking user access, they would be less likely to falsely report their age.

Another design feature that can increase the effectiveness of self-attestation is "friction."¹⁰ The Electronic Privacy Information Center, a public interest organization, uses the term *friction* to describe design elements that have the effect of slowing a process, which usually results in fewer reporting inaccuracies. For example, an online service may require a user to wait a certain amount of time before changing their birth date in an attempt to gain access to a site, rather than immediately allowing the user to do so after their account is created.

2. Estimation

a. Usage and Transactional Data

There are multiple ways for online services to accurately estimate a user's age. For example, for users who have been using a social media platform, transactional data—data that is accumulated through use—can be combined and corroborated to effectively confirm a user's given age range. Transactional data may also be assessed from

⁶ FED. TRADE COMM'N, *Complying with COPPA: Frequently Asked Questions*, Business Guidance Resources (July 2020), <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

⁷ BREWER'S LAW, *Are Age Gates Required For Beverage Manufacturer Websites?*, (last visited Sep. 25, 2024), <https://brewerslaw.com/are-age-gates-required-for-beverage-manufacturer-websites-sort-of/#:~:text=Age%20gates%20are%20not%20legally,Institute%2C%20and%20Distilled%20Spirits%20Council>.

⁸ An author's child, age 7.

⁹ See 5RIGHTS FOUNDATION, *supra* note 6, at 52.

https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf

¹⁰ Brief of the Electronic Privacy Information Center as *Amicus Curiae* in Support of Defendant-Appellant Supporting Reversal, *NetChoice LLC v. Rob Bonta*, Attorney General of the State of California, in his official capacity, No. 23-2969, 2023. <https://cdn.sanity.io/files/3tzzh18d/production/c567c26dc66cd9839ab87ec6db9b95975d80b1c4.pdf>.

bank or mobile records. The company Privo, for example, has a number of age assurance offerings, including using bank, mobile, and credit card data.¹¹

Using transactional data may seem to be the most data-intrusive method of age assurance. However, most social media services already gather the relevant data points for marketing purposes, and/or have access to public data points on their users.¹² In fact, attorneys general from nearly every state have filed suit against Meta Platforms, accusing the social media company of having "actual knowledge" that specific Instagram and Facebook users were under the age of 13 and yet continuing to allow these accounts to encounter content that is known to be harmful to children.¹³ Additionally, websites often use third-party platforms for security screenings or marketing analytics, which can easily be repurposed to include age assurance.¹⁴ If large web services can financially exploit users through knowledge of their age, the same web services could be forced to provide additional privacy or safety protections using already existing age assurance measures. Even web services that do not engage in such behavior can easily implement age assurance based on already available transactional data. For example, web services can generally estimate a user's age by "analyzing their online profile, activity, history, or facial data."¹⁵ While data-intensive, the goal is to not cause any additional data intrusions by using only what information is already provided by the user. It should be acknowledged, however, that assessing age based on transactional data—particularly if it is limited to a specific company's site or service—is a more limited option in the case of minors using a platform or online service for the first time.

A number of states have passed age assurance laws in the past year, and several make reference to transactional data. Idaho HB 498,¹⁶ Louisiana Act 440,¹⁷ Mississippi SB 2346,¹⁸ Montana SB 544,¹⁹ Texas HB 1181,²⁰ and Utah SB 287²¹ permit the use of public or private transactional data for age assurance purposes. This includes information that documents exchanges, agreements, or transfers that the individual has engaged in, including but not limited to mortgage, education, and employment records.

¹¹ PRIVO, By industry: Age Restricted Content & Products (last visited Sep. 27, 2024), <https://www.privo.com/by-industry-age-restricted-content-products>.

¹² Erica Finkle et al., *How Meta Uses AI To Better Understand People's Ages On Our Platforms*, META: Tech at Meta (June 22, 2022), <https://tech.facebook.com/artificial-intelligence/2022/06/adult-classifier/>.

¹³ Press Release, Matthew Plankin, Attorney General of the State of New Jersey, AG Platkin, 41 Other Attorneys General Sue Meta for Harms to Youth from Instagram, Facebook: Company Falsely Assured the Public That Features Were Safe for Young Users (Oct. 24, 2023), <https://www.njoag.gov/ag-platkin-41-other-attorneys-general-sue-meta-for-harms-to-youth-from-instagram-facebook/>.

¹⁴ Electronic Privacy Information Center, *supra* note 11.

¹⁵ Sarah Forland et al., *Age Verification: The Complicated Effort to Protect Youth Online Age, Assurance and Age Verification*, OPEN TECHNOLOGY INSTITUTE (Apr. 23, 2024), <https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/age-assurance-and-age-verification/>.

¹⁶ H.B. 498, 67th Leg., 2nd Sess. (Idaho 2024),

<https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2024/legislation/H0498.pdf>.

¹⁷ H.B. 142 (La. 2022), <https://legis.la.gov/legis/ViewDocument.aspx?d=1289498>.

¹⁸ S.B. 2346 (Miss. 2023), <https://billstatus.ls.state.ms.us/documents/2023/html/SB/2300-2399/SB2346IN.htm>.

¹⁹ S.B. 544 (Mont. 2023), <https://leg.mt.gov/bills/2023/billhtml/SB0544.htm>.

²⁰ H.B. 1181 (Tex. 2023), <https://capitol.texas.gov/tlodocs/88R/billtext/html/HB01181H.htm>.

²¹ S.B. 287 (Utah 2023), <https://le.utah.gov/~2023/bills/sbillenr/SB0287.pdf>.

b. Facial or Biometric Data

Another form of age estimation is face characterization. Using a facial image scan, online services can confirm age declaration. (This is different from facial recognition, because it does not require confirming or even guessing at identity—simply age.) People engage in such a method daily. If a 10-year-old boy were to tell you he was 50 years old, one look at him would confirm that he was lying. On the other hand, we would usually defer to someone who claims to be 33 and who looks the part. It would be impossible to tell the difference between 33 and 35, but it is also unnecessary.

Face characterization is similar. It is "best used to place users in age bands" or "signal that a user meets an age threshold," such as under 13 or over 21. It is much less effective for distinguishing between two adjacent ages, such as 16 and 18.²² This can mean that face characterization's accuracy in distinguishing users at the edges is less than desired. Still, there is scientific support for its effectiveness in certain instances. For example, the service Yoti,²³ which is used by diverse clients such as Instagram, the U.K. Post Office, and Epic Games, as well as some financial institutions, claims that their facial recognition software accurately identifies 6- to 11-year-olds as under 13 years old 98.35% of the time.²⁴ Recent data published by the National Institute of Standards and Technology (NIST) raises questions about Yoti's accuracy, especially with 12-year-olds and teenagers, but it is undisputed that the accuracy of this technology in general continues to increase, as NIST itself reported on these gains.²⁵ The NIST report found that certain demographic groups were more likely to be misestimated than others, and that there is significant progress still to be made.

This type of age estimation can raise concerns about equity. NIST studies have indicated, for example, that women have higher false rates than men, and there are concerns that accuracy rises with the quality of a camera.^{26 27} The technology also raises privacy concerns. Biometric data necessary to use such a method may not otherwise be collected, is considered sensitive under a variety of laws, and has a stronger "creepy" factor for many Americans who may consider this type of data collection intrusive. Some of these concerns may be mitigated if providers do not save biometric data, and if they are simply doing an estimation of age, rather than any type of identification.

What's more, with respect to privacy being a barrier to implementing age assurance in general: It seems especially unfair for certain tech companies to abuse user trust, and then point to the lack of user trust as a reason for why they cannot implement age assurance and protect children. "Users' reluctance to provide personal information to tech companies, and their lack of trust in companies' data privacy and security practices, does not stem from age assurance alone but also from background market and regulatory forces: tech companies' relentless pursuit of surveillance capitalism and legislatures' failure to regulate this conduct. Companies should

²² Future of Privacy Forum, *Unpacking Age Assurance: Technologies and Tradeoffs* (June 2023), https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf.

²³ Yoti is a certified B Corporation based in the U.K.

²⁴ Yoti, *Facial Age Estimation Fact Sheet* (Oct. 2023), <https://www.yoti.com/wp-content/uploads/2023/10/Facial-age-estimation-fact-sheet.pdf>.

²⁵ See Kayee Hanaoka et al., *FACE ANALYSIS TECHNOLOGY EVALUATION: AGE ESTIMATION AND VERIFICATION*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 43 (2024), <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf> (noting 80% accuracy within 3 years of 12 year olds).

²⁶ National Institute of Standards and Technology, *NIST Reports First Results From Age Estimation Software Evaluation* (May 30, 2024), <https://www.nist.gov/news-events/news/2024/05/nist-reports-first-results-age-estimation-software-evaluation>.

²⁷ Hanaoka et al., *FACE ANALYSIS TECHNOLOGY EVALUATION: AGE ESTIMATION AND VERIFICATION*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (May 30, 2024), https://pages.nist.gov/frvt/reports/aev/fate_aev_report.pdf.

not be able to engage in monetization strategies that put users' privacy at risk and then turn around and use that fact to escape regulation."²⁸

3. Parental Attestation and Consent

Another form of age assurance used today is via parental attestation of a child's age, which can be part of or distinct from providing parental consent for a child's use of the product or service. Parents can indicate a child's age (either specifically, or within a range) through self-provided information. Parents' age may be determined from estimation or verification techniques, or they may self-attest their age. For example, parents can prove their age through some form of estimation—such as face characterization—and then afterward provide indication of a child's age. Bandio,²⁹ a relatively new actor in the age assurance field, offers this type of age assurance, which relies on assessment of the parent's age as being over a threshold, and then manges tokens that can be used on different sites and services to vouch for a child's age as being within a specific range.

For parental indication of age, similar to the child's attestation, methods can rely on device-level, user-level, or platform-level parental control settings.³⁰ Such controls are already available on all three of the most commonly used internet browsers: Chrome, Safari, and Firefox.³¹ These controls can also function as parental consent or approval for online sites and services. Data intrusion concerns are minimal with this method, as it does not require data collection beyond what parents have already provided through parental controls.³²

The New York Child Data Protection Act (SB S7695A), signed into law on June 20, 2024,³³ offers a parental age indication method dubbed "age flags," in which a parent or caregiver can set a child's device or browser to remember that the user is self-reporting as a minor. Under the law, online services will have to acknowledge and respect such reporting. The state attorney general is developing guidance for this method and will be empowered to enforce what it means to respect age flags.

Historically, parental consent has also effectively functioned as an indication of a child's age or age range. Under COPPA, if a parent provides consent—through an email, a phone call, a video chat, credit card use, or some other approved mechanism—that action also essentially attests to the age of the user for whom consent is provided, specifically that the age is under the threshold requiring parental consent. Under COPPA, the parent's age range may or may not be assessed—in a video call or phone call, it likely would be, or via use of a credit card. When COPPA permits email approval, as in lower risk situations, the parent's age would be effectively self-attested to. A related situation exists in the accounting reporting space as well. This has been implemented by online services such as WhatsApp and imo.im. Parents can request that their child's account be deleted if the user is under 13, but the process is a fairly onerous one that requires proof of the allegedly underage user's identity, age, and proof of parentage (usually with a birth certificate).

²⁸ Brief of Amicus Curiae Electronic Privacy Information Center in Support of Neither Party, *Free Speech Coalition, et al. v. Ken Paxton*, in his Official Capacity as Attorney general for the State of Texas (2024) (No. 23-1122), https://www.supremecourt.gov/DocketPDF/23/23-1122/326638/20240923144351707_23-1122%20Electronic%20Privacy%20Information%20Center%20Amicus%20Brief%20In%20Support%20of%20Neither%20Party.pdf.

²⁹ Bandio is a public benefit corporation created by Common Sense Media and Aleo Networks Foundation.

³⁰ Electronic Privacy Information Center, *supra* note 11.

³¹ Davis Neild, *How to Use Parental Controls in Your Google, Apple, and Microsoft Account*, WIRED (Nov. 8, 2020), <https://www.wired.com/story/parental-controls-google-apple-microsoft-account/>.

³² Electronic Privacy Information Center, *supra* note 11.

³³ S.B. S7695A (N.Y. 2023), <https://www.nysenate.gov/legislation/bills/2023/S7695/amendment/A>.

4. Verification and "Hard" Identifiers

On the far end of the age assurance spectrum, there is age verification. These are measures that not only estimate age or confirm an age range, but also seek to firmly verify the precise age of a user. A number of state bills include some form of age verification as a possible method of enforcement. Providing a digitized identification card, such as a digital scan of a driver's license or other government-issued identification, is the most common method of verification. Many age and identity verifiers—like Experian—assess hard identifiers like government IDs. While ID checks may risk circumvention—kids could get ahold of their parents' IDs, or even fake IDs—the technology is becoming more reliable at countering common circumvention tactics. For instance, Yoti's ID verification systems, employed by Instagram, incorporate face matching to confirm that the individual submitting the ID is indeed the person depicted on it. They also perform authenticity checks to verify the legitimacy of the ID, and utilize technology to counter deepfakes that attempt to make the user resemble the photo on the ID to bypass the verification process.³⁴

Providing government identification and submitting to biometric verification is a highly effective method of age assurance. However, it is also a financially costly method,³⁵ and raises a number of significant concerns. For one, it raises a concern about equity for individuals who may not have easy access to eligible forms of identification. That, and/or a lack of desire or mistrust in presenting a government identifier, can lead to additional barriers to accessing information or entering an online platform. Opponents also highlight higher risks to privacy—the data collection that is needed to employ such a system includes sensitive IDs or other types of data that are generally not currently provided by online users. For this reason, some proponents of age verification focus on high-risk or highly regulated services that would justify both such financial costs and the burden of sharing an ID.

Age assurance is a challenging balancing act. Some state laws have attempted to reduce the "costs"—the amount of data that is required to be provided, or the number of parties with whom it is shared—of hard age verification. One approach is to offer alternative methods of verification. For example, Florida³⁶ and Indiana³⁷ permit third-party verification, discussed below. Another data minimization effort involves clear prohibitory rules. Although the language is slightly different across states, the majority of state laws enacted in this space prohibit any commercial entity, including third parties that perform the required age verification on behalf of the commercial entity, from retaining any identifying information of the individual after access has been granted to the service. Requiring on-device processing is another mechanism to minimize data and limit risk.³⁸

³⁴ Amba Karsondas, *Effective Age Verification: Going beyond reading a date of birth on an ID*, Yoti (July 11, 2023), <https://www.yoti.com/blog/effective-age-verification-going-beyond-reading-date-of-birth-on-id/>.

³⁵ Sarah Forland et al., *Age Verification: The Complicated Effort to Protect Youth Online Age, Assurance and Age Verification*, OPEN TECHNOLOGY INSTITUTE (Apr. 23, 2024), <https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/age-assurance-and-age-verification/>.

³⁶ H.B. 3 (Fla. 2024), <https://www.flsenate.gov/Session/Bill/2024/3/BillText/er/PDF>.

³⁷ S. B. 17, 123rd Gen. Assemb., 2nd Reg. Sess. (Ind. 2024), <https://iga.in.gov/pdf-documents/123/2024/senate/bills/SB0017/SB0017.05.ENRH.pdf>.

³⁸ FUTURE OF PRIVACY FORUM, *Unpacking Age Assurance: Technologies and Tradeoffs* (June 2023), https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf (See "Risk Management Tools").

5. Use of Third Parties

One popular approach—which typically incorporates some form of the above described methods for assessing age—involves a third-party verifier. This is a way to limit the number of times a user or a parent has to address age assurance, which parents in particular may appreciate. Third-party verifiers can pass information on to the site or service that requires age assurance—this information may be very limited, including through "zero knowledge proofs" that do not do anything other than indicate whether a user is or is not a certain age.³⁹ While research is still developing in regard to preferences and attitudes toward age assurance, one study showed that parents reported "that their most ideal method for setting age assurance on apps and services would be on a per account basis—the point at which they are downloaded from an app store." (That said, they next preferred providing assurance per app, versus per device.)⁴⁰

Additionally, a third-party verifier can limit the number of entities that hold age information (which could be simply a number, or which could be ID), and this could presumably mean that data collected is held by fewer—and possibly more trustworthy—hands. That said, third-party verifiers may themselves be ripe targets for hacking, which is an important concern to address. At the same time, it is possible that this method could be designed to delete information once age has been ascertained. A third party could be:

- A private entity, a state or federal entity, or an independent, quasi-governmental, or nonprofit organization established for this purpose.
- A device or app store that has received an attestation of age. One such device-based offering is offered by the company Aylo.⁴¹
- A cellular phone company or internet service provider, which may possess more data than attestation of the account holder's age; they may have their ID or credit card, including data from an in-person visit.
- Offline-to-online verification. Readers are already familiar with the various forms of offline age verification, such as in-person encounters. In physical stores that already require age verification, such as a liquor store or pharmacy, tokens or "scratch cards" could be purchased and then registered online.⁴² This method, while still highly effective, presents fewer privacy concerns because tokenization results in little identifying information being saved online.⁴³

³⁹ Kathie Jurek, *Zero-Knowledge Proof*, ALEO (Oct. 5, 2023), <https://aleo.org/post/what-is-a-zero-knowledge-proof/>. "A zero-knowledge proof (often abbreviated as "ZKP") is a cryptographic protocol that can improve data privacy. It allows one party, known as the prover, to assure another party, the verifier, that a statement is true without revealing any extra information."

⁴⁰ KANTAR, *MAKING SENSE OF AGE ASSURANCE: ENABLING SAFER ONLINE EXPERIENCES*, FAMILY ONLINE SAFETY INSTITUTE (Finding 10) (2022), https://cdn.prod.website-files.com/5f47b99bcd1b0e76b7a78b88/636d0df804bd2d7c849f4e50_MAKING%20SENSE%20OF%20AGE%20ASSURANCE%20EXEC%20SUMMARY%20-%20FOSI%202022.pdf.

⁴¹ AYLO, *Age Verification + Device-Based Solution: Fact Sheet* (Apr. 2024), https://www.aylo.com/assets/files/age_verification_fact_sheet.pdf.

⁴² Sarvesh Mathi, *What Are The Different Age Verification Methods Available And Why Are They Problematic?*, MEDIANAMA (Jan. 11, 2023), <https://www.medianama.com/2023/01/223-online-age-verification-solutions-privacy-issues/>.

⁴³ CNIL, *Online age verification: balancing privacy and the protection of minors* (Sept. 22, 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

Age Assurance Used by High Impact Social Media Companies

Currently, companies in the U.S. are largely left on their own to figure out age assurance—or to ignore it—and which methods they choose.

The largest social media companies operate under a diverse set of user age requirements. Companies based in or operating in the U.S. and the European Union, for example, must determine which users are under 13 years old. Despite these mandates, we see that when companies are not explicitly required to employ age assurance systems, they do not do so—at least in terms of assessing age to provide protections. Instead, most major social media platforms rely primarily on users to self-identify their age, without any kind of verification.

There are a variety of age assurance systems used by the largest social media companies with significant user bases in the United States, both in their structure and effectiveness.

Facebook, owned by Meta, is the largest social media company by far, with just over 3 billion monthly active users.⁴⁴ It is also one of the few social media platforms that purports to implement some version of age assurance other than just relying on attestation. Facebook's policy requires users to be at least 13 years old to sign up for an account.⁴⁵ Prospective users must attest to their age to the platform when they sign up, and they will be locked out of making an account if they do not attest to being at least 13.⁴⁶ Once a user is on the platform, Facebook uses artificial intelligence systems that draw on "multiple signals," including things like birthday messages from friends and the kinds of content the user searches for on the platform, to verify that the user is actually as old as they identified themselves to be.⁴⁷ (Facebook claims to use this for keeping people on or off its apps; as noted above, however, per court documents it has historically seemed to rely on only the self-provided age for "legal purposes" and has used the signals from user activity for marketing and other purposes.⁴⁸) Finally, Facebook also uses human content moderation. If an account is flagged as a terms of service violation (normally, these flags are unrelated to the account's age, e.g., an account is flagged for hate speech or doxing), then the human content moderator assigned to investigate the activity also reviews the account to ensure it is properly of age.⁴⁹ The assessment of the effectiveness of this system is mixed. On the one hand, Facebook has been applauded for taking a voluntary "first step" in age assurance.⁵⁰ On the other hand, serious questions have been raised about the efficacy of these systems; in fact, the European Commission recently launched a probe that includes an investigation into the efficacy and proportionality of Facebook's age assurance methods.⁵¹

Instagram, also owned by Meta, is not the next largest social media platform, but it is the next largest platform that relies on a unique age assurance method. Like Facebook, users must be at least 13 years old to create an account on Instagram.⁵² And also like Facebook, Instagram initially relies on users self-reporting their age at signup. However, if a user seeks to change the age on their account from under age 18 to 18 or older, the user

⁴⁴ Stacey Jo Dixon, *Number of Monthly Active Facebook Users Worldwide as of 4th quarter 2023*, STATISTA (Feb. 2024).

⁴⁵ Pavni Diwanji, *How Do We Know Someone Is Old Enough to Use Our Apps?*, META (July 27, 2021).

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ Complaint for Injunctive and Other Relief, *State of Arizona et al. v. Meta Platforms, Inc. et al.* (N.D. Cal Oct. 24, 2023).

⁴⁹ *Id.*

⁵⁰ Peter Suci, *Meta Testing New Age Verification Tools – Experts Explain Why They Won't Work*, FORBES (July 1, 2022).

⁵¹ Emma Woollacott, *European Commission Probes Meta Over Youth Social Media Addiction*, FORBES (May 16, 2024).

⁵² Diwanji, *supra* note 46.

must go through an age assurance system.⁵³ Instagram gives users three options to prove that they're over 18: First, a user can submit a digital version of an ID; second, users can upload a video of themselves speaking into a camera, which is then submitted to Yoti—a company that uses AI to determine age from facial and voice recognition; and third, social vouching, where users can get three other users they follow, who are all at least 18 years old, to "vouch" that the user who is seeking to change their account to 18+ is actually over 18.⁵⁴ There is reason to believe that the first two verification methods—ID checking and facial recognition—are fairly effective. While ID checking is at risk of some circumvention, the technology is becoming more reliable and more able to counter common circumvention tactics. For example, Yoti's ID checking systems, used by Instagram, include face matching to ensure that the person submitting the ID is actually the person on the ID, authenticity checking to ensure that the ID is legitimate, and technology that counters deepfakes that are designed to make the user look like the photo on the ID to circumvent the check.⁵⁵ In addition to using age assurance when young people attempt to create adult-age accounts, Instagram also announced in September 2024 that it is "building technology to proactively find accounts belonging to teens, even if the account lists an adult birthday" and that such technology would be tested in the U.S. in early 2025.⁵⁶

The remaining major social media companies popular with young people in the U.S.—YouTube, TikTok, WhatsApp, Telegram, Snapchat, X/Twitter, Reddit, Pinterest, Threads, and others—implement almost no age assurance. By virtue of operating in the U.S., they all have requirements within their terms of service that users must be at least age 13 to create an account on their sites. However, all of these platforms, and other ones of equivalent size, rely entirely on self-reporting by users to determine age. That means that on the vast majority of social media platforms, users of any age can sign up simply by saying they're older than 13, or can access adult-only content on the platform simply by saying they're 18 or older. Some platforms implement remedial measures; companies like TikTok, YouTube, and Pinterest implement human content moderation systems similar to Facebook and Instagram, where accounts that are flagged for a community guideline violation are also evaluated for age. And some other sites—WhatsApp and imo.im—implement a system where a parent can request that their child's account be deleted if the child is under 13, but the process is a fairly onerous one.

Age Assurance and Lawmakers' Efforts to Protect Children from Online Harm

The status quo of assessing (or ignoring) age is not working for youth. Children and teens are not adequately protected online and are being exposed to a wide variety of harms. These include: privacy harms; addictive and unhealthy design features that drive kids to unwanted places or actions; sexual exploitation; difficulty disconnecting; and mental health harms. These harms occur in a variety of ways, including via data collection and sharing, platform design choices, and algorithmic targeting.

Of course, companies could choose to limit data processing, make supportive design choices, and prevent harmful algorithmic targeting for all audiences. Typically, though, they resist such choices for all audiences across the board because these features lead to higher user engagement and more profits. The multi-state lawsuit against

⁵³ Instagram, *How does video selfie age verification work on Instagram?*, Help Center, https://help.instagram.com/292521846402382/?helpref=uf_share.

⁵⁴ Instagram, *Introducing New Ways to Verify Age on Instagram*, (June 23, 2022), <https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram>.

⁵⁵ Amba Karsondas, *Effective Age Verification: Going Beyond Reading a Date of Birth on an ID*, Yoti (July 11, 2023), <https://www.yoti.com/blog/effective-age-verification-going-beyond-reading-date-of-birth-on-id/>.

⁵⁶ Instagram, *Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents* (Sep. 17, 2024), <https://about.instagram.com/blog/announcements/instagram-teen-accounts>.

Meta reveals that Facebook and Instagram both moved to algorithmic feeds after they learned through their own internal research that this type of feed would engage users for longer periods of time.⁵⁷ However, at the same time, many industry leaders purport to want to offer stronger protections for children. For example, when testifying in the Senate in early 2024, Meta CEO Mark Zuckerberg touted Instagram and its more private and restricted accounts for under-15 users. In the same hearing, TikTok CEO Shou Chew told lawmakers that, "TikTok is vigilant about enforcing its 13-and-up age policy and offers an experience for teens that is much more restrictive than you and I would have as adults."⁵⁸ Unfortunately, in practice, children do not receive these protections. For example, Meta has been exposed for collecting information about, and then categorizing, children under 18 into adult-type interests such as gambling or alcoholic beverages.⁵⁹ Common Sense Media's own research has detailed how social media sites are both a source of accidental exposure to pornography and a way to intentionally access it for teens.⁶⁰ The report also details how smartphones allow access to many age-inappropriate experiences, with 68% of children under 13 saying they access "teen"-rated apps and social media apps, and almost 45% saying they use apps with mature (17+) or adult (18+) ratings, including pornography sites, Reddit, casino games, and violent games like Call of Duty.⁶¹ TikTok has been accused by a state attorney general of offering a virtual strip club of underage girls.⁶²

Because most companies, like social media companies, are resistant to offering across-the-board protections for adults—and because in more limited situations, like adult content, it is necessary to distinguish between adults and children—age assurance is increasingly necessary. And parents and caregivers want more action from companies and government: Nearly seven in 10 parents in the U.S. believe industry and government should be more involved in protecting children online.⁶³

Lawmakers at the federal and state levels and in both major political parties are increasingly focused on changing the status quo to protect children—though, as noted, what that means and how to accomplish it varies.

A. Federal Efforts

Some of the highest-profile federal proposals to protect children do not require age assurance, such as updates to COPPA, through the Children and Teens Online Privacy Protection Act, and new guardrails, through the Kids Online Safety Act (both of which were overwhelmingly approved by the Senate in July 2024 under a combined bill, the Kids Online Safety & Privacy Act⁶⁴ and which were also passed through a key House committee as

⁵⁷ Complaint for Injunctive and Other Relief, *State of Arizona et al. v. Meta Platforms, Inc. et al.* (N.D. Cal Oct. 24, 2023).

⁵⁸ Big Tech and the Online Child Sexual Exploitation Crisis Hearing Before the S. Comm. on the Jud., 119th Cong. (Jan. 31, 2024),

<https://www.judiciary.senate.gov/committee-activity/hearings/big-tech-and-the-online-child-sexual-exploitation-crisis>.

⁵⁹ Katie Joseff, *Behavioral Advertising Harms: Kids and Teens*, COMMON SENSE MEDIA (2022),

https://www.common sense media.org/sites/default/files/featured-content/files/behavioral_surveillance-advertising-brief.pdf.

⁶⁰ Michael B. Robb and Supreet Mann, *Teens and Pornography*, COMMON SENSE MEDIA (2023),

<https://www.common sense media.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf>.

⁶¹ Jenny S. Radesky et al., *Constant Companion: A Week in the life of a Young Person's Smartphone Use*, COMMON SENSE MEDIA and UNIVERSITY OF MICHIGAN MEDICAL SCHOOL (2023),

https://www.common sense media.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.

⁶² Complaint for Violations of the Consumer Sales Practices Act, *Utah Division of Consumer Protection v. TikTok Inc.* (2024),

<https://s3.documentcloud.org/documents/24725018/utah-division-of-consumer-protection-v-tiktok.pdf>.

⁶³ KANTAR, *supra* note 40, at Finding 4.

⁶⁴ S. 2073, 118th Cong. (2024).

separate, slightly different bills in September 2024⁶⁵). As written today, the House KOSA bill would require companies to protect youth in situations where the companies have knowledge that the user is a minor, however the knowledge standard differs based on the size of the company, while the knowledge standard in the Senate-passed bill and House COPPA 2.0 is "actual knowledge or knowledge fairly implied on the basis of objective circumstances" that a user is a minor. The House KOSA bill that passed the Energy & Commerce Committee would hold Big Tech to the knowledge standard that they "knew or should have known" a user is a child or a minor, and smaller companies to either "actual knowledge or willful disregard" or, for the smallest, "actual knowledge." All of these standards are an improvement over current law (COPPA), which allows companies to ignore information they have about a user's age. And in practice, the language in these two bills effectively means that companies are free to impose no age assurance whatsoever. However, if they are assessing information about age—either through age gates, or because they are collecting information on users for age-related marketing or targeting segments—then they will have to treat youth users as youth.

B. State Efforts

In general, states have gone further than Congress. States have actually enacted laws, and actually enacted laws that explicitly involve age assurance in the context of online safety and privacy. The state laws largely target services that are deemed to pose a particular threat to children. In many cases, the laws are focused on pornography sites—the laws apply to any commercial entity that knowingly and intentionally "publishes"⁶⁶ material considered harmful to minors, and sites that contain a substantial portion (defined as 33.3% of the site's content) of material that is considered harmful to minors.⁶⁷ Other laws particularly target "social media companies," "social media platforms,"⁶⁸ and "addictive feeds" of these platforms.⁶⁹ Still others apply only to companies that sell products or services that are illegal to sell to minors, such as alcohol, firearms, tobacco, marijuana, knives, and pornography.⁷⁰

One of the first state laws to protect minors from online harms addresses a broad set of privacy and safety concerns. The California Age Appropriate Design Code⁷¹ (CA AADC) required that sites and services likely to be used by children—including social media—must be designed with children's best interests in mind. It was based on the United Kingdom's Children's Code. Under the CA AADC, sites and services are required to "[e]stimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers." Age assurance is required to be proportionate to the risks and data practices of a service, and companies are prohibited from using any personally identifiable information for age estimation. An industry trade group sued the state of California over the CA AADC, and the law is currently stayed, pending outcome of the litigation.

Following the passage of the CA AADC, many state lawmakers focused more explicitly on concerns about pornography and social media, and specifically limiting youth access to such content. Arkansas' law, for example, specified that pornographic content is harmful to minors, and that age verification is necessary to prevent such

⁶⁵ H.R. 7890, 118th Cong. (2024). H.R. 7891, 118th Cong. (2024).

⁶⁶ "Publishes" means to communicate or make information available to another person or entity on a publicly available website. S.B. 66 (Ark. 2023).

⁶⁷ H.B. 3 (Fla. 2024), <https://www.flsenate.gov/Session/Bill/2024/3/BillText/er/PDF>.

⁶⁸ Ohio Rev. Code § 1349.09, <https://codes.ohio.gov/ohio-revised-code/section-1349.09>.

⁶⁹ S.B. 57694A (N.Y. 2023), <https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A>.

⁷⁰ A.B. 3080 (Cal. 2024), https://digitaldemocracy.calmatters.org/bills/ca_202320240ab3080.

⁷¹ A.B. 2273 (Cal. 2021), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=20210220AB2273.

harms.⁷² Lawmakers in Idaho,⁷³ Louisiana,⁷⁴ and Montana⁷⁵ are also concerned that online pornography is creating a public health crisis by fostering mental health problems and promoting risky behavior. Other states—and sometimes the same states—are also concerned about social media. Utah,⁷⁶ Florida,⁷⁷ and Arkansas⁷⁸ have passed laws with age verification requirements to address the harms related to social media. Arkansas' law mentions the dangers of bullying, exposure to predatory behaviors, mental health problems, and addiction associated with social media use by minors. Utah's and New York's laws seek to address the harms of excessive social media use by minors that impact sleep patterns, academic performance, and overall health.

Most of these state laws have employed similar language regarding permissible methods of determining a user's age. A digitized identification card, such as a digital scan of a driver's license or other government-issued identification, is usually listed first. However, many of the state laws also permit "any commercially reasonable age verification method." While user preferences for specific age assurance methods are still emerging, offering options seems preferable, as one study found that no one specific method was preferred by more than a third of parents.⁷⁹ Flexibility written into the law in determining appropriate methods is helpful, both to meet parent preferences and to allow technology to improve with time, and in general states can benefit from encouraging regulatory sandboxes in this technologically fast-moving space.⁸⁰ While some states do not go on to define with specificity such age assurance methods, Arkansas specifies that the verification method must meet Identity Assurance Level 2.⁸¹ Other states such as Florida⁸² and Indiana⁸³ permit age verification by independent third parties. Still others permit age verification that uses public or private "transactional data," data that has documented exchanges, agreements, or transfers that the individual has engaged in, including but not limited to mortgage, education, and employment records. Lastly, there are states, such as Ohio, that require different standards for children than for teens, and require parental consent under enumerated methods, but generally do not address or require specific forms of age verification. Ohio Section 1349.09, for example, requires that social media sites targeted at or likely to be accessed by children under 16 must obtain the parental consent required by law.⁸⁴

⁷² S.B. 66, 94th Gen. Assem., Reg. Sess. (Ark. 2023),

<https://www.arkleg.state.ar.us/Home/FTPDocument?path=%2FACTS%2F2023R%2FPublic%2FACT612.pdf>.

⁷³ H.B. 498, 67th Leg., 2nd Reg. Sess. (Idaho 2024),

<https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2024/legislation/H0498.pdf>.

⁷⁴ H.B. 142 (La. 2022), <https://legis.la.gov/legis/ViewDocument.aspx?d=1289498>.

⁷⁵ S.B. 544 (Mont. 2023), <https://leg.mt.gov/bills/2023/billhtml/SB0544.htm>.

⁷⁶ Utah Code §§ 13-71-101 to 401,

https://le.utah.gov/xcode/Title13/Chapter71/13-71-S101.html?v=C13-71-S101_2024100120240501.

⁷⁷ H.B. 3 (Fla. 2024), <https://www.flsenate.gov/Session/Bill/2024/3/BillText/er/PDF>.

⁷⁸ S.B. 689, 94th Gen. Assem., Reg. Sess. (Ark. 2023),

<https://www.arkleg.state.ar.us/Home/FTPDocument?path=%2FBills%2F2023R%2FPublic%2FSB396.pdf>.

⁷⁹ KANTAR, *supra* note 40, at Finding 7.

⁸⁰ Scott Babwah Brennen and Matt Perault, *Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?*, The Center for Growth and Opportunity and The University of North Carolina Center on Technology Policy, 20 (June 2023).

https://www.thecgo.org/wp-content/uploads/2023/06/Age-Assurance_02.pdf.

⁸¹ S.B. 66, 94th Gen. Assem., Reg. Sess. (Ark. 2023),

<https://www.arkleg.state.ar.us/Home/FTPDocument?path=%2FBills%2F2024F%2FPublic%2FSB66.pdf>.

⁸² H.B. 3 (Fla. 2024), <https://www.flsenate.gov/Session/Bill/2024/3/BillText/er/PDF>.

⁸³ S.B. 17, 123rd Gen. Assem., 2nd Reg. Sess. (Ind. 2024),

<https://iga.in.gov/pdf-documents/123/2024/senate/bills/SB0017/SB0017.05.ENRH.pdf>.

⁸⁴ Ohio Rev. Code § 1349.09, <https://codes.ohio.gov/ohio-revised-code/section-1349.09>.

Many state laws require data minimization of information collected to assess age. Although the language varies, the majority of the laws prohibit any commercial entity, including third parties that perform the required age verification on behalf of the commercial entity, from retaining any identifying information of the individual after access has been granted. Many of the state laws, but not all, include a private right of action to sue for damages that result from possessing such information.⁸⁵ In most of the state laws, companies are liable only when they knowingly maintain such information.⁸⁶

New York is one of the most recent states to pass laws in this space, focusing on youth privacy and safety on social media but not seeking to cut off youth access to social media. In this way, New York's goals seem most similar to California's with the AADC. New York's Stop Addictive Feeds Exploitation (SAFE) for Kids Act⁸⁷ addresses concerns about social media, and the New York Child Data Protection Act establishes youth privacy protections. The SAFE for Kids Act prohibits social media companies from serving addictive feeds to children and teens without parental consent, prohibits social media companies from pushing notifications from addictive feeds to children and teens between midnight and 6 a.m. without parental consent, and prevents companies from retaliating against users who do not opt in to addictive feeds or overnight notifications.⁸⁸ The SAFE for Kids Act applies only to platforms that are providing an addictive feed to users. It does not apply to all social media platforms.⁸⁹ The act also does not mandate age verification or use of biometric information. Section 1501.1(a) requires only that operators of an addictive social media platform use "commercially reasonable methods to determine that the covered user is not a covered minor."⁹⁰ As stated earlier, there are a number of ways that platforms can, and already do, conduct this type of age assurance, such as through the thousands of data points that these platforms already collect on their users.⁹¹ Through preexisting anti-discrimination laws and to-be-drafted attorney general regulations, New York's law is intended to ensure that websites "will not use age verification methods that rely solely on biometrics or require government identification that many New Yorkers do not possess."⁹² The New York Child Data Protection Act requires a different method to be used to assure age: age flags, discussed above. It will be up to the attorney general to clarify what it means to respect age flags and develop guidance for this method.⁹³

⁸⁵ S.B. 17, 123rd Gen. Assem., 2nd Reg. Sess. (Ind. 2024),

<https://iga.in.gov/pdf-documents/123/2024/senate/bills/SB0017/SB0017.05.ENRH.pdf>.

⁸⁶ S.B. 544 (Mont. 2023), <https://leg.mt.gov/bills/2023/billhtml/SB0544.htm>.

⁸⁷ Press Release, Kathy Hochul, Governor of New York, Governor Hochul Joins Attorney General James and Bill Sponsors to Sign Nation-Leading Legislation to Restrict Addictive Social Media Feeds and Protect Kids Online (June 20, 2024),

<https://www.governor.ny.gov/news/governor-hochul-joins-attorney-general-james-and-bill-sponsors-sign-nation-leading-legislation#:~:text=This%20legislation%20will%20require%20social,any%20state%20across%20the%20nation>.

⁸⁸ Common Sense Media, *Setting the Record Straight: New York's SAFE For Kids Act* (2024),

<https://www.common sense media.org/sites/default/files/featured-content/files/csm-response-to-chamber-of-progress-claims.pdf>.

⁸⁹ *Id.*

⁹⁰ S.B. S7694A (N.Y. 2023), <https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A>.

⁹¹ Common Sense Media, *Setting the Record Straight: New York's SAFE For Kids Act* (2024),

<https://www.common sense media.org/sites/default/files/featured-content/files/csm-response-to-chamber-of-progress-claims.pdf>.

⁹² S.B. S7694A (N.Y. 2023), <https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A>.

⁹³ New York State office of the Attorney General, Legal Recruitment, Opportunity for Attorneys w/ Experience Leading Complex Rulemaking Efforts, https://ag.ny.gov/sites/default/files/2024-07/dej_nyc_sc_3705_web.pdf; New York State office of the Attorney General, Legal Recruitment, Opportunity for Attorneys w/ Complex Rulemaking Experience, https://ag.ny.gov/sites/default/files/2024-07/dej_nyc_rpa_3704_web.pdf.

The New York law also takes an interesting approach to the debate of actual vs. constructive knowledge. Historically, most significantly under COPPA, companies were liable when they had "actual knowledge" of children using their general audience sites. This incentivized some companies to pretend to avoid the issue altogether, and especially for legal purposes (though, as discussed above, companies did seek to understand children's ages for advertising purposes). The actual knowledge standard has long been criticized by child advocates. Increasingly, child safety and privacy laws include a more constructive knowledge standard: that the platform "knew or should have known" that the user is a minor, rather than actual knowledge. This constructive knowledge, or "knew or should have known," means that platforms cannot pretend that they do not have minors on their platforms when they have evidence that they do. In New York, lawmakers in some sense flip this typical "actual knowledge" standard on its head. In the SAFE for Kids Act,⁹⁴ the knowledge standard is "actual knowledge"—but not actual knowledge that the user is a minor, rather that the user is *not* a covered minor. Under the act, the use of a "commercially reasonable and technically feasible" method of age determination by the platform to determine that a user isn't a minor creates a "safe harbor" for the platform, thereby incentivizing the platform to use age assurance in their determination of whether a user is a minor covered by the law.

Constitutional Considerations

When companies choose to implement age assurance methods on their own, constitutional challenges are rarely raised. However, as discussed above, companies seem loath to implement more effective age assurance without prodding from lawmakers. And, when it is required, they often sue.

In the U.S., laws requiring age assurance have come under fire for violating First Amendment rights: sometimes of children, and sometimes of adults who may be deterred from visiting sites if there are age assurance mechanisms in place.⁹⁵ And sometimes—including when privacy and data are involved—concerns have involved companies' free speech rights.

While cases have involved age assurance in regard to design, access, and privacy (with the CA AADC being a major example of design and privacy), most of the cases have involved access—generally to content involving pornography or as may be found on social media. And they typically rely on *Reno* and its progeny, *Reno* involving access to content. Overreliance on *Reno* is questionable, and particularly inappropriate in situations involving design and privacy.⁹⁶

Companies' litigation strategy often relies upon a sweeping argument that essentially everything they do is protected by the First Amendment (it all involves data, and data is speech).⁹⁷ This argument, when taken to its

⁹⁴ S.B. S7694A (N.Y. 2023), <https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A>.

⁹⁵ See focus on challenges and first amendment concerns in Sarah Forland et al., *Age Verification: The Complicated Effort to Protect Youth Online Age, Challenges with Age Verification*, OPEN TECHNOLOGY INSTITUTE (Apr. 23, 2024), <https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/age-assurance-and-age-verification/>.

⁹⁶ As explained compellingly in EPIC's brief in support of neither party in *Free Speech Coalition v. Paxton*, the tech industry repeatedly uses *Reno* and related decisions "to attack content-neutral privacy and design laws that rely on age assurance." This is despite the fact that these decisions do not "squarely address[] the question of whether and when age assurance constitutes a burden for content-based laws.... Yet NetChoice claims that the cases ruled age assurance presumptively unconstitutional, even for *content-neutral* laws." See Electronic Privacy Information Center, *supra* note 29.

⁹⁷ See, e.g., Neil Richards, *Why Privacy Matters*, pp. 182-3 (2022) (Noting companies' arguments that: "If everything rests on data, and data is "speech," regulation of everything becomes censorship." And noting that if we accept this argument from companies, "we run the risk that American courts will one day accept these claims as *actual* fundamental rights, judgments

logical conclusion, as has been argued in the privacy context in particular,⁹⁸ would mean that there can be no regulations of technology and no responsibility for harm. This argument fails to recognize the evolution of digital technology in all of our lives. Ultimately, the Supreme Court will be forced to address technology's gambit, and will need to reach a conclusion as to whether technology companies bear any responsibility whatsoever to the billions of people from which they profit. In the meantime, the lower courts are starting to issue decisions.

One example of Big Tech using the First Amendment tactic is when the California AADC was enjoined on First Amendment concerns in September 2023, in *NetChoice v. Bonta*. The district court noted with respect to the age assurance provisions that "The age estimation and privacy provisions thus appear likely to impede the 'availability and use' of information and accordingly to regulate speech." And the court expressed concerns that "the steps a business would need to take to sufficiently estimate the age of child users would likely prevent both children and adults from accessing certain content."⁹⁹ Apart from the probable First Amendment concerns, the district court expressed concern that the age assurance provisions could also have a negative impact on privacy. They would require businesses to collect more data in an attempt to verify the ages of their users, including children. The court wondered whether this might increase privacy breaches in clear contravention of the state's stated objective of improving online privacy for children.

In the *NetChoice v. Bonta* appellate court opinion, the Ninth Circuit found that certain provisions of the CA AADC are likely to fail under the strict scrutiny standard of the First Amendment—primarily a data protection impact assessment. However, the court was precise in finding that "whether NetChoice is likely to succeed on its facial challenge as to the remaining challenges is less certain. For instance, most of those provisions, by their plain language, do not necessarily impact protected speech in all or even most of their applications."¹⁰⁰ The age assurance provision of the AADC was one of these provisions, which did not necessarily impact protected speech in all or most applications. This finding by the Ninth Circuit seemingly suggests that forms of age assurance that do not restrict access to content but rather limit harmful design features such as dark patterns are not a violation of the First Amendment.

On laws primarily addressing access, states have come to differing conclusions as to whether laws that required, directly or by implication, age assurance were in violation of the First Amendment (and also differing views on whose First Amendment rights may or may not be violated). Some distinctions may be attributed to the type of restriction at issue (e.g., social media, or obscenity, where courts have much more precedent to justify children from accessing) and whose speech might be restricted. For example, Ohio Sec. 1349.09, which would have required parental consent for children under 16 to access social media platforms targeted at youth or likely to be accessed by such youth, was enjoined seemingly largely due to First Amendment concerns that the law burdens platforms' ability to publish and distribute speech by minors, as well as that regulates minors' production of and receiving of speech.¹⁰¹ In Utah, age verification requirements for pornography sites have so far been upheld despite First Amendment challenges—being dismissed at the district court level in part because of the procedural

that would make meaningful information-age consumer protection by democratically elected legislatures all but impossible.").

⁹⁸ *Id.* at 183.

⁹⁹ *NetChoice v. Bonta*, No. 5:22-cv-08861-BLF (N.D. Cal. Sept. 18, 2023).

¹⁰⁰ *NetChoice v. Bonta*, No. 23-2969 (9th Cir. Aug. 16, 2024).

¹⁰¹ *NetChoice v. Yost*, No. 21-4077 (6th Cir. May 23, 2022).

enjoined early 2024 (Feb 12 or Jan 9). This was deemed a content-based restriction that was not narrowly tailored. The law was also found to be void for vagueness.

posture of the cases as being pre-enforcement challenges.¹⁰² In contrast, a law that primarily addresses age verification for access to social media—while also having some privacy and design requirements—was recently preliminarily enjoined, with the judge noting that it "imposes content-based restrictions on social media companies' speech."¹⁰³ In Texas, the Fifth Circuit upheld an age verification law—that required companies hosting a third or more of "harmful to minors" content to verify age but permitted them to choose among different commercially reasonable methods—despite First Amendment challenges. The Fifth Circuit noted that "regulation of the distribution to minors of speech obscene for minors is subject only to rational-basis review."¹⁰⁴ Opponents argue that the law imposes burdens on adults' access to content and that strict scrutiny should have been applied. This is now up for review at the Supreme Court in *Free Speech Coalition v. Paxton*.¹⁰⁵

It is true that in the late 1990s, in *Reno v. ACLU*, the Supreme Court questioned the feasibility of age estimation and assurance online. There were concerns that it would be impossible to prevent adults from accessing online content if children were denied access—even if such children could be denied access "in real life." But, among other points, this was over two decades ago. Technology has advanced. More of everyday life takes place over the internet, and children are deserving of protections there are much as they would be in brick and mortar spaces. While this is an open question, judges have good reason to recognize the technological advances made, and that it should be possible now—unlike 20 years ago—to distinguish between adults and children without infringing upon adults' rights to access content.

And secondarily, the *Reno* case involved access to content. It was not age assurance to protect children from harmful design features or privacy practices. While also an open question, in situations involving age assurance to make sure product design is appropriate, or that privacy protections are provided, the First Amendment should be even less of a factor. As indicated by the Ninth Circuit considering the California AADC, age assurance targeted at product features or privacy protections may not always impact protected speech. This view has led to courts distinguishing between conduct (including design features) and speech.¹⁰⁶ And courts should make this distinction. As explained by the Electronic Privacy Information Center in a brief supporting neither party in *Free Speech Coalition v. Paxton*, "Privacy and design regulations that use age assurance to give kids special protections are fundamentally different from laws that block kids from accessing content or services."¹⁰⁷

Ultimately, age assurance should be able to exist alongside the First Amendment rights of adults and of children as well.

¹⁰² Evan Stambaugh, *Challenge to Utah Age Verification Mandate for Online Porn Lands at 10th Circuit*, COURTHOUSE NEWS (Sep. 18, 2023),

<https://www.courthousenews.com/challenge-to-utah-age-verification-mandate-for-online-porn-lands-at-10th-circuit/>.

¹⁰³ SB 194, Decision from U.S. District Court for the District of Utah, Judge Shelby. (Sept. 11, 2024).

¹⁰⁴ *Free Speech Coalition et al. v. Ken Paxton* (No. 23-50627) (5th Cir. 2024),

<https://www.texasattorneygeneral.gov/sites/default/files/images/press/Age%20Verification%205th%20Circuit%20Opinion.pdf>.

¹⁰⁵ *Free Speech Coalition et al. v. Ken Paxton* (No. 23-1122), U.S. (2024),

<https://www.supremecourt.gov/docket/docketfiles/html/public/23-1122.html>.

¹⁰⁶ Social Media Cases, Case No JCCP 5255, Lead Case 22STCV21355, Superior Court of CA, County of LA, Carolyn Kuhl, Oct. 13, 2023 (negligence claims based on social media design features not barred by First Amendment), https://socialmediavictims.org/wp-content/uploads/2022/07/Complaint_File-TikTok-Smith-Arroyo-7_1_22.pdf.

¹⁰⁷ Electronic Privacy Information Center, *supra* note 29.

International Age Assurance Practices

Efforts in the U.S. may get a boost—at least in terms of demonstrating technological feasibility—from efforts abroad. While most major social media companies have yet to introduce age assurance systems, that is likely to change in the relatively near future. This is because several countries and the E.U. have either passed new laws or are considering legislation that would require certain age assurance measures to be taken by companies over the next few years. These countries admittedly have different judicial systems and legal frameworks, and, importantly, lack First Amendment speech protections that exist in the U.S. Whether or not the U.S. chooses to follow their examples, these laws will demonstrate the capabilities, and challenges, of tech companies to comply with age assurance requirements.

United Kingdom: The U.K. passed the Online Safety Act (OSA) into law in October 2023. Part 3 of the OSA creates duties for providers of user-to-user services (services, like social media, through which user generated content may be encountered by other users) that are deemed "likely to be accessed by children."¹⁰⁸ One such duty is to protect children from harm online.¹⁰⁹ In order to meet this, the OSA requires that user-to-user service providers prevent children—through use of age verification or estimation—from accessing "primary priority content that is harmful to children."¹¹⁰ This kind of content is defined as "pornographic content or content that encourages/promotes suicide, self-injury and eating disorders/behaviours."¹¹¹ Part 5 of the OSA will also require that online service providers that publish certain pornographic content online to use "highly effective age assurance" to ensure that children do not have access to that content.¹¹² Ofcom is considering that highly effective methods could include photo-ID matching, facial age estimation, and reusable digital identity services. It has stated that "age assurance methods that are not capable of being highly effective include payment methods which do not require the user to be over 18, self declaration of age, and general contractual restrictions on the use of the service by children."¹¹³ These provisions will be enforced by Ofcom likely starting in early 2025.¹¹⁴

European Union: The E.U.'s Digital Services Act was passed in 2022 and went into effect in August 2023. The act requires Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to implement design features that protect children online.¹¹⁵ While age assurance isn't specifically required by the act, it does establish a long list of design requirements, such as setting children's privacy settings to the most protective by default, that require some method of determining which users are children.¹¹⁶ As a result, the act certainly contemplates a requirement for companies to implement an age assurance system, and to that end, the European

¹⁰⁸ Cooley, *Decoding the UK Online Safety Act 2023: Latest Draft Guidance, Key Features and Insights* (Nov. 29, 2023), <https://www.cooley.com/news/insight/2023/2023-11-29-decoding-the-uk-online-safety-act-2023-latest-draft-guidance-key-features-and-insights>.

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ Megan Lukins, *The UK's Online Safety Act: The Online Safety Act and Children*, TaylorWessing (Nov. 2, 2023).

<https://www.taylorwessing.com/en/interface/2023/the-uks-online-safety-act/the-online-safety-act-and-children>.

¹¹² Ofcom, *Consultation: Guidance on Age Assurance and other Part 5 Duties for Service Providers Publishing Pornographic Content on Online Services*, (Dec. 5, 2023),

<https://www.ofcom.org.uk/online-safety/protecting-children/guidance-service-providers-pornographic-content/>.

¹¹³ Ofcom, *Tech Firms Must Tame Toxic Algorithms to Protect Children Online* (May. 8, 2024),

<https://www.ofcom.org.uk/online-safety/protecting-children/tech-firms-must-tame-toxic-algorithms-to-protect-children-online/>.

¹¹⁴ *Id.*

¹¹⁵ European Commission, *The Impact of the Digital Service Act on Digital Platforms* (last accessed Sep. 27, 2024),

<https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms>.

¹¹⁶ *Id.*

Commission has created a Task Force on Age Assurance under the DSA with the goal of creating standards and best practices for age verification.¹¹⁷

Australia: When the Australian Online Safety Act (OSA) went into effect in January 2022, it regulated access to inappropriate material online.¹¹⁸ Since then, Australia's eSafety Commissioner has created consultations with stakeholders, and assembled a road map toward requiring age assurance under the Australian OSA.¹¹⁹ These efforts have culminated in an age assurance trial—the eSafety Commissioner, in consultation with industry stakeholders and the Australian government, is testing a number of age verification and estimation systems in order to inform the next phase of policy guidance and rulemaking under the OSA.¹²⁰

Conclusion

Age assurance mechanisms are maturing, and can constitutionally protect children while respecting adult access to the internet. This progress is important because age assurance is increasingly necessary given the ongoing challenges to keeping children and teens safe online.

According to the U.S. surgeon general's report "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory," up to 95% of youth age 13–17 report using social media, with more than a third saying they use social media "almost constantly."¹²¹ With our kids spending so much time on social media, it is common sense that we create platforms designed to be safe for their age. The U.S. needs to do better in terms of age assurance for children, and to do better in terms of protecting children once sites and services have a sense of their age. Businesses should not be able to cherry-pick when they wish to adequately protect children on their sites, or to hide behind claims of outdated technology when they otherwise act as if technology has no bounds. While not all sites will require age assurance, sites that are particularly risky to children and teens could in many instances benefit from them.

Age assurance should be privacy protective, proportionate, fair, and equitable. There is, to be sure, continued work to be done to make this a reality. But it is increasingly possible to protect children online while protecting adults'—and children's—privacy and speech rights. It is possible for age assurance, and protections for children online, to exist within the bounds of the First Amendment. Technology—the same technology that many opponents herald for all of its other benefits—is advancing. Efforts in other countries will demonstrate these capabilities. There are ways to protect privacy and safety—and legislative proposals to do the same—that require no assessment of age. And, when needed or desired, there are ways to assess age in a way that is privacy protective, proportionate, fair, and equitable. It may be that age assurance will be voluntary in some circumstances and required in others, but this is consistent with how we operate in an everyday world. It may be

¹¹⁷ European Commission, *Digital Service Act: Task Force on Age Verification*, (Jan. 30, 2024), <https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0#:~:text=The%20Commission%20has%20set%20up,and%20standards%20in%20age%20verification>.

¹¹⁸ eSafety Commissioner, *Illegal and Restricted Online Content* (Feb. 4, 2024), <https://www.esafety.gov.au/key-topics/illegal-restricted-content>.

¹¹⁹ eSafety Commissioner, *Age Verification* (Aug. 31, 2023), <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>.

¹²⁰ eSafety Commissioner Press Release, *Statement: Announcement of Age Assurance Trial* (May 1, 2024), <https://www.esafety.gov.au/newsroom/media-releases/statement-announcement-of-age-assurance-trial>.

¹²¹ U.S. Dept. of Health and Human Services, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory* (2024), <https://www.hhs.gov/surgeongeneral/priorities/youth-mental-health/social-media/index.html#:~:text=The%20Surgeon%20General's%20Advisory%20on,%2C%20technology%20companies%2C%20researchers%2C%20and>.

that sometimes, children get around gates (for decades, they have gotten into bars with fake IDs, but this has not stopped bouncers from checking IDs at the door). It should not be impossible to draw nuanced lines just because we are talking about digital experiences. And, if it is determined that everything that happens in the digital space implicates the First Amendment in a way that makes any regulation unconstitutional, it is unlikely that minors—or anyone—can ever be adequately protected online.

Age assurance should be approached with care. There is a role for everyone to play:

1. Technologists and industry should voluntarily make this a priority, using methods they have developed to assess age for marketing and commercial purposes for the purposes of protecting children.
2. Parents and caregivers should make any desires and concerns with respect to age assurance clear. So should teenagers. This will take more familiarity for most parents and teens with age assurance, which itself requires industry adoption. And it will also require trust—which industry and lawmakers should earn by protecting privacy. But as individuals become more comfortable with different options, they can influence how industry and lawmakers proceed.
3. Laws should allow for flexibility. Lawmakers should encourage innovation, including via a regulatory sandbox approach or other incentives to hasten development of smart solutions.

Ultimately, there is a path forward that will rely on the participation of industry, experts, public engagement, and policymakers to establish online safeguards for kids. We need continued development of age assurance technology, engagement from families and other users, thoughtful leadership from lawmakers, and even a commitment from social media companies, platform developers, and device makers—all working together to help parents and children thrive in today's digital world.