2023

KEEPING KIDS SAFE ONLINE:

HOW SHOULD POLICYMAKERS APPROACH AGE VERIFICATION?

The Center for Growth and Opportunity at Utah State University

X

UNC CENTER ON TECHNOLOGY POLICY

Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?

Authors:

Scott Babwah Brennen[a]

Matt Perault[b]

June 2023

Policy Paper

The Center for Growth and Opportunity at Utah State University is a university-based academic research center that explores the scientific foundations of the interaction between individuals, business, and government.

We support research that explores a variety of topics from diverse perspectives. Policy papers are published to stimulate timely discussion on topics of central importance in economic policy and provide more accessible analysis of public policy issues.

a Scott Babwah Brennen is the head of online expression policy at the Center on Technology Policy at the University of North Carolina at Chapel Hill, where he leads the Center's work on online expression, misinformation, and political advertising.

b Matt Perault is the director of the Center on Technology Policy at the University of North Carolina at Chapel Hill, a professor of the practice at UNC's School of Information & Library Science, and a consultant on technology policy issues.

The Center for Growth and Opportunity at Utah State University

UNC CENTER ON TECHNOLOGY POLICY

Contents

Executive Summary

As policymakers across the US consider new regulations meant to protect children online, they are increasingly confronting a central challenge: to protect children online, you first must know who is a child.

There is nothing simple or straightforward about determining the age of internet users. There are many methods—from submitting government IDs to AI-based facial age estimation—and every one of them has tradeoffs. For example, uploading government IDs requires platforms to collect, process, and store sensitive data, raising the risk of data misuse or theft, as well as concerns about inequitable access to official documentation.

In selecting a method to identify a child, platforms and regulators will always be forced to prioritize some criteria and deprioritize others.

Given this, as policymakers devise new online child safety regulations, how should they approach the issue of age assurance?

This paper seeks to answer that question. It begins with an overview of regulators' growing concern with online child safety and a review of international, national, and state legislation in this area. It then elaborates on some of the key tradeoffs inherent in different age assurance approaches.

The paper concludes with a set of options for how US regulators might approach age assurance in new online child safety legislation. Due to the active policy debates on this issue in state capitols and Congress, these recommendations are targeted at US regulators and policymakers. However, many of the recommendations may be relevant for lawmakers outside the United States as well.

The ten recommendations are grouped into three categories: balance, specificity, and understanding.

Balance

Regulators should balance costs associated with different assurance methods. This includes

- completing cost-benefit analyses of potential legislation,
- adopting a risk-based assurance approach, and
- offering tax breaks for small companies that use trusted third-party assurance vendors.

Specificity

Regulators should be specific so that companies clearly understand the obligations, best practices, and the tradeoffs associated with different assurance methods. This includes

- tasking the National Institute for Standards and Technology (NIST) to release guidance on the risks of online features,
- instituting a voluntary certification program for age assurance vendors,
- specifying the privacy practices that platforms may use to provide age assurance, and
- expanding Federal Trade Commission (FTC) guidance on complying with the Children's Online Privacy Protection Act (COPPA).

Understanding

Regulators should facilitate research about assurance methods and technologies and about the impacts of age assurance in practice. This includes

- establishing state or federal age assurance sandboxes,
- assessing the impacts of existing state models, and
- requiring certified vendors to share evaluation data.

Introduction

When the House Committee on Energy and Commerce recently held a hearing with TikTok CEO Shou Zi Chew, Representative Buddy Carter (R-GA) asked Chew how the app determines the ages of its users.[1]

Chew responded by describing TikTok's inferential system that analyzes users' public posts to see if their content matches the age users claim to be. Before Chew could finish, Rep. Carter interrupted and exclaimed, "That's creepy!"

The exchange highlights a tension in the emerging policy debates around online child safety: maximizing child safety online often comes at the expense of all users' privacy, data security, and experience.

There are no silver bullets to the problem of age verification. Each method, whether age gating, requiring government IDs, checking credit card statements, or using AI-based facial analysis, involves some tradeoff between privacy, security, accuracy, usability, and legality—among others.

Yet many of the new regulations—from the laws passed in Utah or California, to those considered by federal legislators—provide only minimal guidance about how platforms or apps should verify a user's age. These laws typically come without any clear accounting of how policy frameworks should balance these tradeoffs.

This paper provides guidance for how policymakers should approach the issue of age assurance, offering ten recommendations in three categories: specificity, balance, and understanding.

1 C-SPAN, *TikTok CEO Shou Zi Chew Testifies Before Congress*, YouTube, March 23, 2023, https://www.youtube.com/watch?v=_E-4jtTFsO4.

Understanding Age Assurance

Defining Age Assurance

Despite growing public attention to age verification, regulators and commentators see age verification as one of a series of approaches under the umbrella term, *age assurance*. The International Standards Organization defines age assurance as the "the process of establishing and communicating an individual's age."[2] In contrast, age verification is one type of age assurance that narrowly involves the "process of age determination by reference to identity attributes associated with a person." [3]

Another form of age assurance, age estimation, refers to "the process of assessment that an individual is likely to fall within a category of ages, over a certain age or under a certain age by reference to assurance components, inherent features, or behaviours related to that individual."[4]

Age Assurance Methods

Age assurance methods fall into four categories: self-declaration, user-submitted hard identifiers, third-party institutional attestation, and inferential age assurance.

These four categories are discussed in more detail below. We discuss tradeoffs that can be used to assess each method in a later section.

Self-declaration

Right now, many platforms rely on users to report their own age or birth date when registering for a new account or simply to confirm that they are older than a certain age threshold. This approach is commonly called *age gating*. Critics, such as the 5Rights Foundation, have noted that while self-declaration means platforms do not need to collect sensitive or personal data (beyond age or birthdate), it is very easy for a user to lie about their age.[5]

In what could be seen as a new twist on self-declaration, Instagram recently announced that it is testing a system of social vouching. If a minor claims that they are over 18, they can ask three 18-year-old 'mutual followers' to confirm their age.[6]

User-submitted Hard Identifiers

Instead of simply reporting their own birthdays, some systems require users to upload images of official documents that include birthdays. Drivers' licenses and passports are the most common. This method may be harder for minors to bypass, but it is far from foolproof and requires platforms to collect, store, and process potentially sensitive personal data.

---

2 International Organization for Standardization, "ISO Working Draft Age Assurance Systems Standard."

3 International Organization for Standardization, "ISO Working Draft Age Assurance Systems Standard."

4 International Organization for Standardization, "ISO Working Draft Age Assurance Systems Standard."

5 5Rights Foundation, *But How Do They Know It Is a Child?*

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

Furthermore, this approach is both underinclusive and overinclusive: some minors may be able to use others' IDs to pass these checks, while some adults may have difficulty complying. The difficulty some adults may face complying with age verification was the basis for the federal court decision striking down the Children's Online Protection Act.[7]

Third-party Attestation

In some cases, third-party institutions can provide age assurance. For example, YouTube and other platforms allow users in some countries to use credit cards to verify their age. The implication is that in order to hold a credit card, a user must provide an accurate age.[8] Some experts have also suggested using voter data.[9] Perhaps most notably, there are now a series of efforts to create digital identities, such as the European Union's planned digital identity wallet, which will allow users to submit documents to a central system to verify their age. They can then use that system to certify their age or identity across other services without sharing anymore personal data.[10] A series of countries, including India, have also been experimenting with and implementing universal ID systems.[11] These systems have been criticized for security breaches, accessibility issues, privacy concerns, and technical bugs.[12]

Notably, some commentators have suggested that rather than requiring individual platforms, apps, or websites to determine users' ages, age assurance can and should be done at the device, operating system, or even ISP level.[13] Intermediaries could create an age verification token to indicate that a user of that device is above a certain age threshold. This approach may require device manufactures or ISPs to collect additional personal data, undermine online privacy and anonymity, and fail in situations where different people use the same device, including when a child occasionally uses a parent's device.

Inferential Age Assurance

Finally, there are a series of ways that platforms or third parties attempt to infer the age of users without directly asking them. Some platforms build AI-based inference systems to assess user content and behavior to identify users who might fall under a certain age.[14] These systems can look broadly at the content users share for obvious indicators that a user is not the age they have reported. For example, a user might reference being in a certain grade at school or having a birthday that does not align with the age they have reported to the platform.

---

7 American Civil Liberties Union v. Reno, 217 F.3d 162 (3rd Cir. 2000).

8 "Access Age-Restricted Content & Features," Google Account Help, Google, accessed May 23, 2023, https://support.google.com/accounts/answer/10071085?visit_id=638138865778895836-1023392832&p=age-verify&rd=1.

9 Tony Allen, Lynsey McColl, Katharine Walters, and Harry Evans, *Measurement of Age Assurance Technologies*, Age Check Certification Scheme, 2022, https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf.

10 "Digital Identity for All Europeans," European Digital Identity, European Commission, accessed May 23, 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

11 "Unique Identification Authority of India," Internet Archive, accessed May 23, 2023, https://web.archive.org/web/20230420081840/https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html.

12 "ID Systems Analysed: Aadhaar," Privacy International, November 19, 2021, https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar.

13 Simone van der Hof, "Age Assurance and Age Appropriate Design: What Is Required?" *The London School of Economics and Political Science* (blog), November 17, 2021, https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/.

14 Erica Finkle, Sheng Luo, Christine Agarwal, Dave Fryer, "How Meta Uses AI to Better Understand People's Ages on Our Platform," *Tech at Meta* (blog), June 22, 2022, https://tech.facebook.com/artificial-intelligence/2022/06/adult-classifier/.

These are the types of methods that TikTok's CEO attempted to explain in his congressional testimony, and which Rep. Carter referred to as "creepy."

Some commentators have suggested that AI systems could assess other user characteristics, including voice, gait, or hand geometry.[15] Regardless of the exact approach, inferential assurance methods may require platforms to collect or process large quantities of user data—including data from minors. In some circumstances, social media companies already have this data, but more expansive collection and processing of minors' data is precisely what some regulators are trying to prevent.

Social media companies also train content moderators to assess the age of users. A moderator may look at user content or activity to estimate their ages. If a moderator believes a user does not meet a certain age requirement, the account may be placed in a checkpoint that requires the user to engage in some additional age assurance method in order to regain use of the account.[16]

The British company Yoti offers six different ways for users to prove their ages, including AI-based models to estimate users' ages based on images and videos.[17] Yoti's model is trained on a large corpus of facial images. According to a Yoti white paper, it can reliably estimate a users' age within a year or two for most age groups and skin tones.[18] Several platforms, including Instagram, Facebook, and digital gambling platforms and machines use Yoti to estimate users' ages.[19]

Age Assurance in Action

Digital platforms, apps, and websites use a wide range of age assurance methods. Most social media platforms, including Facebook, Reddit, Spotify, Instagram, TikTok, and Snap, initially ask users to provide their birth date when registering a new account.

Some platforms, including TikTok, YouTube, and Facebook, have instituted AI-based age inference systems. As described above, these systems review user content and behavior to identify users likely to be minors.[20] When the system identifies a potential user under 18 or under 13, many platforms will require additional forms of age verification, particularly for products that may pose more risks to minors. For example, when Facebook's inferential system determines a user is likely under age when using Facebook Dating, the platform may require the user to complete age verification by uploading either an ID or a video selfie.[21]

Some platforms, including Instagram, TikTok, and Facebook require additional verification checks when a minor attempts to change their birthday so that they appear to be over 18. In those instances, Instagram allows users to verify their ages by submitting a government ID, submitting a video for Yoti's facial age assessment, or through "social vouching," where three friends attest your age.[22]

---

15 Allen, McColl, Walters, and Evans, *Measurement of Age Assurance Technologies.*

16 "Underage Appeals on TikTok," Safety, TikTok, accessed May 23, 2023, https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok.

17 "About Yoti," Yoti, accessed May 23, 2023, https://www.yoti.com/about/.

18 Yoti, *Facial Age Estimation White Paper*, updated March 2023, https://www.yoti.com/blog/yoti-age-estimation-white-paper/.

19 "Age and Identity Verification for Online Gambling," Yoti, accessed May 23, 2023, https://www.yoti.com/gambling/.

20 Pavni Diwanji, "How Do We Know Someone Is Old Enough to Use Our Apps," *Meta* (blog), July 27, 2021, https://about.fb.com/news/2021/07/age-verification/.

21 Erica Finkle, "Bringing Age Verification to Facebook Dating," *Meta* (blog), December 5, 2022, https://about.fb.com/news/2022/12/facebook-dating-age-verification/.

22 "Introducing New Ways to Verify Age on Instagram," *Instagram.*

Sites that involve sensitive types of content, such as pornography, alcohol sales, and gambling, may also have more stringent age assurance controls. For example, OnlyFans and Pornhub require content creators to verify their ages before posting content. [23] OnlyFans requires creators to upload a government ID. Pornhub allows creators to upload a government ID or perform a "live face scan," which is assessed by Yoti's age estimation system. However, neither site requires users to verify their ages.[24] Some prominent adult sites, such as Xvideo, which is based in the Czech Republic, do not require either content uploaders or subscribers to verify their ages.[25]

Websites that sell alcohol and online gambling sites also have stringent assurance processes. Sites that sell alcohol usually require someone who is over 21 to present a valid ID upon delivery.[26] Online gambling sites must comply with federal laws, including Know Your Customer provisions and anti-money laundering laws, that require users to verify their identities and ages.[27] While gambling sites rely on a range of different means of verifying age and identity, some go as far as to require users to submit their social security number.[28]

Tradeoffs in Age Assurance Methods

Each of the age assurance methods discussed above has advantages and disadvantages. For instance, if the goal is to identify a user as being over or under a certain age threshold, any method has the potential to make errant determinations, either allowing some minors to access content or products intended for adults, or preventing some adults from accessing content or products based on the false determination that they are minors. The challenges are compounded when platforms have different levels of access or restrictions for different ages of minors.

We recognize that in selecting age assurance methods, platforms and regulators will always be forced to prioritize some criteria and deprioritize others. We identify 10 tradeoffs that regulators and platforms should consider in specifying age-assurance methods.

Accuracy

No age assurance method is totally accurate, but some are more accurate than others. Misidentifying people's true ages may result in underage users being able to access content and products they shouldn't be able to or overage users being unable to access content and products they should be able to. This could either be a result of a method being easy to circumvent, like self-disclosure, or of the method not being accurate in certain circumstances, like AI-based photo or video estimation. Importantly, even those methods that involve users submitting hard identifiers

23 "Age & Identity Verification," OnlyFans, accessed May 23, 2023, https://onlyfans.com/transparency-center/verification; "How to Sign Up and Join the Model Program," Help Center, Pornhub, accessed May 23, 2023, https://help.pornhub.com/hc/en-us/articles/4419879760403-How-to-Sign-Up-and-Join-the-Model-Program.

24 "Age & Identity Verification," OnlyFans, accessed May 23, 2023, https://onlyfans.com/transparency-center/verification; "How to Sign Up and Join the Model Program," Help Center, Pornhub, accessed May 23, 2023, https://help.pornhub.com/hc/en-us/articles/4419879760403-How-to-Sign-Up-and-Join-the-Model-Program.

25 "XVideos Terms of Service," XVideos, accessed May 23, 2023, https://info.xvideos.net/legal/tos/.

26 "Welcome to wine.com," Wine.com, accessed May 23, 2023, http://wine.com/.

27 Financial Crimes Enforcement Network, "Exceptive Relief for Casinos from Certain Customer Identity Verification Requirements," US Department of the Treasury, October 19, 2021, https://www.fincen.gov/sites/default/files/2021-10/Casino%20Exceptive%20Relief%20101921_0.pdf; American Gaming Association, "Best Practices for Anti-Money Laundering Compliance: 2019–2020," https://www.americangaming.org/wp-content/uploads/2019/12/AGA-AML-Best-Practices_12-9.pdf.

28 "Why Am I Being Asked to Verify My Identity? (US)," Help Center, DraftKings, accessed May 23, 2023, https://help.draftkings.com/hc/en-us/articles/360058767233-Why-am-I-being-asked-to-verify-my-identity-US.

are not always accurate: a minor could circumvent that system by using a fake ID or by using someone else's login account to access a site.

In addition to selecting appropriate methods of age assurance, platforms must determine how rigorously to confirm the accuracy of submitted or collected information, which is often called the "level of confidence" or "level of assurance."[29] Most age verification methods can be done with varying levels of effort to verify the accuracy of the information submitted. For example, a system that requires a government ID could simply require a user to upload a copy of the ID, which it checks via optical-character recognition, even though some users might submit fake or expired IDs. Alternatively, the system could confirm with the agency that issued the ID that it is real and valid. Finally, the system could ensure that the user submitting the ID is the same person to whom the ID was issued.

Increasing the level of certainty also increases the resources required to complete the verification and may have downsides in terms of privacy, equity, or user experience. In addition to considering specific *methods* of assurance, regulators should also address what *level* of assurance (confirmed accuracy) is required for platforms to be in compliance.

Equity and Accessibility

Accuracy concerns stem not simply from precision or error rate, but *how* a given method is wrong. Are there certain populations for whom a method is less accurate? This concern raises significant questions of equity.

Some experts have worried that certain facial recognition systems result in significant racial, income, or other disparities.[30] For example, automated facial age assurance systems continue to have different accuracy rates for people with different skin tones. In its latest white paper, Yoti reports its system is less accurate predicting the age of people with darker skin tones for many age groups.[31]

Differential accuracy rates may be an issue for other age assurance methods as well. Many platforms ask their human content moderators to estimate user ages and recognize those users below 13. While we have less public data about racial, gender, or ethnic disparities in age estimation of human moderators, existing scholarly literature suggests that humans are better able to estimate the ages of people who look like them.[32]

Beyond differential accuracy rates, some age assurance methods raise other equity concerns. For example, several new proposed state bills specifically require users to submit a US driver's license. If enacted, these laws would restrict product access for anyone unable to produce an official government ID. As we've seen in other policy debates about ID requirements, racial minorities,

29 International Organization for Standardization, "ISO Working Draft Age Assurance Systems Standard."

30 Samuel Wehrli, Corinna Hertweck Mohammadreza Amirian, Stefan Glüge, and Thilo Stadelmann, "Bias, Awareness, and Ignorance in Deep-Learning-Based Face Recognition," *AI and Ethics* 2, no. 3 (August 1, 2022): 509–22, https://doi.org/10.1007/s43681-021-00108-6; eSafety Commissioner, *Age Verification Roadmap Consultations: Round 2*, Australian Government (October 2022), https://openresearch-repository.anu.edu.au/bitstream/1885/280477/1/AusOH_134.pdf.

31 Yoti, *Facial Age Estimation White Paper.*

32 Hedwige Dehon and Serge Brédart, "An 'Other Race' Effect in Age Estimation from Faces," *Perception* 30, no. 9 (September 2001): 1107–13, https://doi.org/10.1068/p3122.

immigrants, people with lower incomes, and those with disabilities are less likely to hold government IDs.[33]

Privacy and Security

Many age assurance methods require the collection and processing of personal or sensitive data—including from minors. Companies could potentially store or access users' drivers' licenses, passports, and other sensitive information.

Some critics, such as the Electronic Frontier Foundation, have expressed concern that age verification would vastly increase online surveillance, undermining long-held and essential anonymity protections online.[34]

Pragmatically, some states already impose additional regulations on how companies handle such content, which creates additional compliance burdens for companies. More importantly, this collection of sensitive data creates significant risks: both that companies could misuse those data, including by selling it for commercial purposes, or that the data could be subject to a security breach. Data breaches are common, and if more companies hold more personal data in order to comply with age assurance mandates, it is likely that some data will be exposed to security breaches. The likelihood increases for companies that do not have the resources to hire large, well-trained cybersecurity teams.

Accountability and Transparency

Age assurance methods should incorporate platform accountability and transparency. Users should be able to understand how platforms determine or estimate age and have recourse when they believe an age determination is incorrect.

Even if providers are transparent about their methods, it may still be difficult to ascertain error rates. When incorrect age determinations are made, some providers offer little explanation or little opportunity for appeal. Accountability is more complicated when a platform incorporates a third-party tool for verifying age, since ultimately an aggrieved user may need to seek recourse with the third party, rather than with the platform.

Interoperability

Users benefit when an age assessment tool can be used across services. It allows them to avoid going through an age assurance process each time they visit a new website or use a new service. To achieve this result, regulators should consider the value of this type of interoperability in when they craft age assurance requirements.

Interoperability involves tradeoffs as well. It may increase concentration, as some Big Tech companies are well placed to provide age assurances at scale. It can also raise privacy and security concerns: a single security breach could expose huge collections of user data.

---

33 Vanessa M. Perez, *Americans with Photo ID: A Breakdown of Demographic Characteristics*, Project Vote, February 2015, https://www.projectvote.org/wp-content/uploads/2015/06/AMERICANS-WITH-PHOTO-ID-Research-Memo-February-2015.pdf.

34 Jason Kelley and Adam Schwartz, "Age Verification Mandates Would Undermine Anonymity Online," Electronic Frontier Foundation, March 10, 2023, https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online.

Usability

Different assurance methods will impose different burdens on users. Some happen more behind the scenes, while others require users to submit information before continuing.

For example, in the wake of the passage of California's Age-Appropriate Design Act (AADA), Mike Masnick, founder and editor of *TechDirt*, has noted that to be in compliance, it is possible that many websites will decide to assess users' ages before allowing them to enter.[35] This could mean that nearly every time a user clicks on a new link, they must re-enter their birthdate, give access to some third-party verification site, or participate in some other assurance mechanism. These types of interventions are likely to decrease the usability of apps or websites.

Regulators should not only consider how policies impact the usability of a single app, but also how it impacts a user's entire experience online. For example, while clicking through a banner on a single website may only be a minor inconvenience, having to do so on every page visited, as is required under the European Union's General Data Protection Regulation (GDPR), may pose significant difficulties.

Competitiveness

Adequately addressing the privacy, security, and usability issues of integrating age assurance efforts may be costly for companies. The largest tech companies will likely have little difficulty affording these additions, but some age assurance methods may present both technical and financial burdens for smaller companies. Imposing significant compliance burdens may make it more difficult for smaller companies to compete with larger ones.

Innovation

Policymakers should consider how new regulation might incentivize or hinder innovation both in age verification technology and platform services. The technology for verifying or estimating users' ages is developing, and it is important that regulations are written to allow for continued product innovation.

Legality

Critics contend that certain forms of age assurance are unconstitutional. NetChoice, a trade association, filed a suit to challenge California's AADA on both First and Fourth Amendment grounds, arguing the law is a content-based speech restriction that requires companies "to serve as roving censors of speech on the Internet."[36]

In an amicus brief filed in support of NetChoice's challenge to the AADA, Santa Clara University School of Law professor Eric Goldman argues that the AADA, and specifically its requirements around online age assurance methods, would unconstitutionally "chill online readers and authors."[37]

---

35 Mike Masnick, "I Explained to a Court How California's 'Kid Code' Is Both Impossible to Comply with & an Attack on Our Expression," *TechDirt* (blog), February 22, 2023, https://www.techdirt.com/2023/02/22/i-explained-to-a-court-how-californias-kids-code-is-both-impossible-to-comply-with-an-attack-on-our-expression/.

36 NetChoice, LLC v. Bonta, 5:22-cv-08861, (N.D. Cal. 2022).

37 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, http://dx.doi.org/10.2139/ssrn.4369900.

Goldman argues that age assurance imposes a "burdensome barrier" by imposing a delay in access to online sites, and some methods "will require users to provide private and sensitive information." Furthermore, he observes that in striking down the Child Online Protection Act of 1998 (COPA), the US Court of Appeals for the Third Circuit noted that age verification "raise[d] unique First Amendment issues' that ma[d]e the statute unconstitutional."

The resolution of the NetChoice suit will provide an important data point on the constitutionality of age assurances that will serve as useful guidance to other lawmakers who are considering various policy options in this area. As additional laws are passed in other states, there are likely to be future legal challenges that will provide more guidance on the legality of various policy tools for determining age online.

Expression and Association

Aside from these legal questions, platforms and regulators must consider the ways in which different assurance methods permit or prohibit users' ability to express themselves. Children possess rights, including rights of expression and association.[38] Neither the Constitution nor the Universal Declaration of Human Rights says that the rights they afford apply only to people over the age of 13 or 18. If assurance methods are too onerous, minor users may be unable or choose not to comply, thereby inhibiting their ability to express themselves and to associate with others. Regulators should also consider how assurance requirements may impair or protect anonymity online, since some experts have noted that anonymity is an important consideration in protecting expression.[39]

Age Assurance Regulation

To provide an overview of the state of age assurance regulation, we consider both existing regulation and new reform proposals across the United States. Also, given the European Union's recent leadership in technology policy, through legislation including GDPR, the Digital Services Act, and the AI Act, we briefly examine how current EU policy treats age assurance.

Federal Age Assurance Law in the United States

While policymakers and activists have expressed concern over children's safety online since the early days of the internet, US regulators have historically given little attention to age assurance methods.[40]

The 1998 Children's Online Privacy Protection Act (COPPA) remains the principal law governing children's privacy online and age assurance in the United States.[41]

---

38 UN General Assembly, Resolution 44/25, Convention on the Rights of the Child (September 2, 1990), https://www.ohchr.org/sites/default/files/crc.pdf.

39 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York City: Basic Books, 1999).; Lina Eklund, Emma Von Essen, Fatima Jonsson, Magnus Johansson, "Beyond a Dichotomous Understanding of Online Anonymity: Bridging the Macro and Micro Level," *Sociological Research Online* 27, no. 2 (June 2021): 486–503, https://doi.org/10.1177/13607804211019760.

40 "Child Online Protection Act," in Wikipedia, last modified January 12, 2023, https://en.wikipedia.org/wiki/Child_Online_Protection_Act.

41 "15 U.S. Code Chapter 91 - Children's Online Privacy Protection," Cornell Law School, Legal Information Institute, accessed May 24, 2023, https://www.law.cornell.edu/uscode/text/15/chapter-91.

To simplify somewhat, COPPA adopts a "notice and consent" framework for digital services "directed to children" or that "knowingly" collect information from children under 13. Services must give notice and receive consent in order to collect data from minors under 13. However, COPPA does not specify *how* digital service providers should assess or verify children's ages.

FTC guidance on complying with COPPA observes the following:

> The Rule does not require operators to ask the age of visitors. However, an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate.[42]

If online service providers choose to simply use self-declaration to assess age, they do not need to rely on a secondary assessment. The FTC provides six options for service providers to obtain parental consent, but it does *not provide* detailed compliance recommendations for service providers to verify a user's age.[43]

Some critics have opined that COPPA disincentivizes services that are not explicitly "directed to children" from determining if they are serving children under 13.[44] For those services, the law's requirements apply only if they know they are serving or collecting data about children under 13. If they know this, then they must take the extra steps prescribed by the law, including obtaining parental consent, providing access and editing privileges regarding one's data, and following a data minimization framework. If they don't know their users ages, then they can avoid these additional requirements.

While a detailed legal review of jurisprudence on age assurance is beyond the scope of this paper, existing case law raises some challenges to the legality of age verification measures. For example, the Children's Online Protection Act (COPA) and sections of the Communications Decency Act (CDA) were struck down by courts that, in part, expressed concerns about the laws' age verification requirements.[45] The CDA prohibited transmitting any "indecent" material online to minors. COPA more narrowly only prohibited commercial speech involving "material harmful to minors."[46] Both laws established age verification as an affirmative defense. However, in overturning the CDA, the Supreme Court ruled in *Reno v. ACLU* that because it is "not economically feasible for most noncommercial speakers to employ such verification," age verification would not ameliorate harms to noncommercial speech imposed by CDA.[47]

Considering the constitutionality of age verification more directly, the Third Circuit in *ACLU v. Mukasey,* echoing its decision in *ACLU v. Ashcroft*, wrote that the age verification requirements in COPA "present their own First Amendment concerns" because of the burdens they place on both

42 "Complying with COPPA: Frequently Asked Questions," Federal Trade Commission, last modified July 2020, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

43 "Complying with COPPA," Federal Trade Commission.

44 5Rights Foundation, *But How Do They Know It Is a Child?*

45 Child Online Protection Act, HR 3783, 105th Cong. (1998 2nd Session).; The Communications Decency Act is the short name for Title V of the Telecommunications Act of 1996. Telecommunications Act of 1996, S 652, 104th Cong. (1996 1st Session).

46 Mark S. Kende, "Filtering out Children: The First Amendment and Internet Porn in the U.S. Supreme Court," Michigan State Law Review 2005, no. 3 (Fall 2005): 843–856.

47 Reno v. ACLU, 521 U.S. 844 (1997).

online publishers and on "many users who are not willing to access information non-anonymously."[48] The court held that the law was unconstitutional.

Age Assurance Law in the European Union

Over the past several years, many governments have sought to pass new legislation to provide more protections for children online. The European Union has been one of the most aggressive governments in imposing new age assurance regulations and has become a global leader in online safety regulation.

There are three main regulations in the EU that establish age verification or assurance mechanisms.

First, Article 8 of the General Data Protection Regulation (GDPR) establishes age verification requirements in some circumstances. It requires covered companies to "make reasonable efforts to verify" they have received consent to process data of children under the age of 16.[49] However, other than noting that age and consent assurance must "tak[e] into consideration available technology," GDPR offers few specifics. Some commentators have noted that GDPR's requirements constitute a "risk-based approach" because they require companies to complete impact assessments whenever there is a "high-risk" to users' data and to minimize data collection.[50]

Second, the Audiovisual Media Services Directive (AVMSD) requires member states to ensure that "media service providers" that "may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them."[51] The directive requires the use of "age verification tools or other technical measures" that are "proportionate to the potential harm of the programme." Providers are prohibited from using the personal data of children collected in the operation of these protection mechanisms for commercial purposes.

The directive also encourages member states to reduce children's exposure to advertisements promoting alcohol, tobacco, and foods and beverages that do not comply with the national or international nutritional guidelines (e.g., high in salt and fat). The commercials should not be designed to highlight the "positive quality of the nutritional aspects of such foods and beverages."

Third, the recently enacted Digital Services Act includes a series of provisions meant to protect minors.[52] For example, online platforms are required to craft their terms and conditions in a way that children can easily understand, and they cannot serve targeted advertising to minors. Platforms should also work to protect minors "by designing their online interfaces or parts thereof with the highest level of privacy, safety and security for minors by default where appropriate or

48 American Civil Liberties Union v. Mukasey, 534 F.3d 181 (3d Cir. 2008).; Ashcroft v. ACLU, 542 U.S. 656 (2004).

49 Regulation (EU) 2016/679 (GDPR) OJ L 119/1–88, 4.5.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1686683319938#d1e1797-1-1.

50 Media Policy Project, *What Does the European General Data Protection Regulation Mean for Children in the UK?* London School of Economics, April 2018, https://www.icmec.org/wp-content/uploads/2018/04/EU-GDPR-Roundtable-LSE-final-pdf.pdf.; "Data Protection Impact Assessment (DPIA)," GDPR.eu, August 9, 2018, accessed May 24, 2023, https://gdpr.eu/data-protection-impact-assessment-template/.

51 Directive (EU) 2018/1808 (AVMSD), OJ L 303/69–92, 28.11.2018.

52 Regulation (EU) 2022/2065 (DSA), OJ L 277/1–102, 27.10.2022; "Questions and Answers: Digital Services Act," European Commission, last modified April 25, 2023, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348.

adopting standards for protection of minors, or participating in codes of conduct for protecting minors." Article 35 notes that very large online platforms (VLOPs) should implement "reasonable, proportionate and effective mitigation measures" to minimize harms to children, including age verification tools.

Beyond these regulations, last May, the EU adopted a new "strategy" called Better Internet for Kids (BIK+).[53] This new guidance document has three pillars: it seeks to protect children from inappropriate and illegal content, empower them with the skills necessary to navigate the digital space, and encourage meaningful online participation. Although it is not legally binding itself, the BIK+ agenda may prod EU member states to adopt similar language in their own domestic regulation.

Under BIK+, the EU is funding a pilot project, "euCONSENT," to test an electronic age verification method.[54] Iain Corby, a project manager of euCONSENT, has told BiometricUpdate.com, "the focus of the solution developed by euCONSENT is on how, having established a user's age, we can anonymously confirm to online services whether that customer meets their age-restriction criteria without a highly disruptive impact on the user's online experience."[55]

The BIK+ also discusses how the development of the European Digital Identity wallet will likely allow children to prove their age in a secure way when using digital services.[56] The technology will allow EU citizens, residents, and businesses to voluntarily "prove their identity and share electronic documents" on personal mobile devices by having their national digital identities linked to the system.

Recent US Reform Efforts

Federal

In April 2023, federal legislators reintroduced two child safety bills that had failed to pass previous sessions. The Children and Teens' Online Privacy Protection Act (COPPA 2.0), introduced by Senators Markey (D-MA) and Cassidy (R-LA), would expand the scope of COPPA protections to include children under the age of 16.[57] The bill would expand COPPA's coverage of sites "directed to children" to include the broader set of sites "used or reasonably likely to be used by children or minors." It would also remove COPPA's standard that restrictions apply only when providers have "actual knowledge" that minors are using their services.

The Kids Online Safety Act (KOSA), introduced by Sens. Marsha Blackburn (R-TN) and Richard Blumenthal (D-CT) would establish a "duty of care" for platforms to minimize harm to children and impose new transparency and privacy requirements.[58]

---

53 European Council Communication COM/2022/212 (BIK+), 11.5.2022.

54 "euConsent: Electronic Identification and Trust Services for Children in Europe," euConsent, accessed May 24, 2023, https://euconsent.eu/.

55 Frank Hersey, "Age Verification and Digital Wallets for Minors," BiometricUpdate.com, May 12, 2022, https://www.biometricupdate.com/202205/age-verification-and-digital-wallets-for-minors-eu-launches-strategy-for-online-child-safety.

56 "European Digital Identity," European Commission, accessed May 24, 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

57 Children and Teens' Online Privacy Protection Act, S 1628, 118th Cong. (2023 1st Session).

58 Kids Online Safety Act, S 3663, 118th Cong. (2022 1st Session).

Although both bills require platforms to take certain steps to protect children, neither includes a detailed discussion of how service providers should determine who is a child. KOSA includes funding for a group of federal agencies, led by the National Institute of Standards and Technology (NIST), to undertake a study "evaluating the most technologically feasible options for developing systems to verify age at the device or operating system level."[59]

Three additional federal bills introduced in 2023, the Social Media Child Protection Act, the Making Age Verification Technology Uniform, Robust, and Effect (MATURE) Act, and the Protecting Kids on Social Media Act would ban all users under a certain age—under 18, 16, and 13 respectively—from accessing social media platforms.[60] The MATURE Act would require users to upload a government-issued ID to verify their age. The Protect Kids on Social Media Act would require platforms to take "reasonable steps beyond merely requiring attestation, taking into account existing age verification technologies" to verify users' ages. And the Social Media Child Protection Act includes both approaches, requiring platforms to collect government IDs or employ "another reasonable method of verification (taking into consideration available technology)."

Also this session, Sen. Mike Lee (R-UT) introduced the SCREEN Act (Shielding Children's Retinas from Egregious Exposure on the Net Act), a bill that would require any service that hosts adult content to institute an age verification system to prevent minors from viewing adult content.[61] The bill would leave it up to the site to choose the specific verification method. However, it stipulates that self-declaration is not sufficient, and the site must publicly disclose how it is verifying user ages. Furthermore, it would establish a "more likely than not" verification standard, lowering the amount of certainty a platform requires to remove a user it suspects might be a minor.

States

While the federal government has failed to pass new online children's safety legislation, state lawmakers have taken action. Several states have passed new laws aimed at protecting children online, and legislators in dozens of states have introduced new online child safety bills in the past two sessions. These bills have typically taken one of two approaches to age verification: a requirement for users to submit identification or a requirement for platforms to adopt a "risk-based approach."

California was the first state to enact a sweeping new law governing online child safety. In 2022, California passed the Age-Appropriate Design Act, a bill that imposes new requirements on internet sites directed at or "likely accessed by" children under 18.[62] And while the upshot of the bill is that most sites will need to verify the age of users, it does not specify how they should do so. Instead, the law states that platforms must "[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."

59 Kids Online Safety Act.

60 Social Media Child Protection Act, HR 821, 118th (2023 1st Session); Making Age Verification Technology Uniform, Robust, and Effective Act, S 419, 118th Cong. (2023 1st Session); Protecting Kids on Social Media Act, S 1291, 118th Cong. (2023 1st Session).

61 Shielding Children's Retinas from Egregious Exposure on the Net Act, HR 6855, 117th Cong. (2022 2nd Session).

62 Cal. Civ. Code §1798.99.28.

However, the law itself does not provide guidance on how to interpret this provision: how a company should assess the risks of their service, or how to match that with a particular age verification technology, or what a "reasonable level of certainty" means. The bill does establish the "California Children's Data Protection Working Group," which will be tasked with the following:

> Ensuring that age assurance methods used by businesses that provide online services, products, or features likely to be accessed by children are proportionate to the risks that arise from the data management practices of the business, privacy protective, and minimally invasive.[63]

Already legislators in a handful of other states, including New Jersey, Oregon, New Mexico, and Minnesota have introduced legislation based on the AADA.[64] None of these bills include additional guidance on how services should verify age. None have passed as of publication of this paper (June 2023).

While there is still ongoing discussion about whether and how the AADA requires most websites to verify users' ages, several other state bills make this requirement far more explicit.[65]

In March, Utah passed two bills that impose new restrictions, both on how minors use social media and how social media platforms treat minors. SB 152 forbids anyone under 18 from holding an account on a social media platform unless they have the "express consent of a parent or guardian."[66] As a result, each platform is required to "verify the age of an existing or a new Utah account holder," and if the holder is a minor, they must confirm they have parental consent to use the platform. This would require all social media platforms to confirm the ages of all their users.

The final version of the law does not specify how platforms should attempt to verify users' ages, instead delegating that responsibility to the state Division of Consumer Protection. The law dictates that the agency will "establish the process or means by which" a platform verifies age and "establish acceptable forms or methods of identification, which may not be limited to a valid identification card issued by a government entity."

The governor of Arkansas signed a similar bill into law in April.[67] The law requires parental consent for minors to use some social media platforms. The law also requires that platforms verify the age of all users, and that they use "a third-party vendor to perform reasonable age verification." It defines "reasonable" methods as those involving "a digitized identification card," "government-issued identification," or "any commercially reasonable age verification method," though it does not further elaborate what constitutes "commercially reasonable." The law also exempts many social media platforms, including any that "provides career development opportunities," offers "cloud storage services, enterprise cybersecurity services, educational devices, or enterprise collaboration tools" for students.

---

63 Cal. Civ. Code §1798.99.28.

64 New Jersey Bill A4919, 220th Leg., 2022–2023 General Session; Oregon SB 196, 82nd Leg. 2023 General Session; New Mexico SB 319, 56th Leg., 2023 General Session; Minnesota HF 2257, 93rd Leg., 2023 General Session.

65 Eric Goldman, "California's Age Appropriate Design Code Is Radical Anti-Internet Policy," *TechDirt* (blog), September 16, 2022, https://www.techdirt.com/2022/09/16/californias-age-appropriate-design-code-is-radical-anti-internet-policy/.

66 Utah SB 152, 65th Leg., 2023 General Session.

67 Ark. Code § 4-88-11.

Another bill proposed in Texas would restrict anyone under the age of 18 from creating a profile on social media.[68] The bill would require an account holder to provide a copy of their driver's license along with a second photo displaying the account holder and the driver's license in a manner that "allows the social media company to verify the identity of the account holder."

Bills recently passed in Louisiana and Mississippi allow any online site that "distributes material harmful to minors on the internet" to be held liable if that site contains at least 33.3 percent "harmful" material, and if "the entity fails to perform reasonable age verification methods to verify the age of individuals attempting to access the material."[69] The Louisiana bill does not specify how platforms should verify user age. It says they must use "reasonable age verification measures," which it identifies as government or digital ID card, or "any commercially reasonable method."

Legislators in at least 11 other states have introduced bills that would require online providers that serve pornography to verify the age of users. In three of those states, the bills have already passed one chamber.[70] Notably, the bills introduced in Oregon and Arizona require a "government-issued" ID for age verification.[71] A related bill introduced in Texas sets the age limit at 13, rather than 18.[72] This Texas bill would also hold a person liable for uploading pornography to a website if the content is subsequently accessed by a minor. If a minor circumvents a platform's age verification measures and accesses that pornography, the original poster of the content could be held liable.

A handful of other state bills impose device-side filtering requirements. These require that all device manufactures include filters that block "by default" all websites that facilitate "human trafficking or prostitution," display child sexual abuse material (CSAM), or display any "obscene material harmful to minors." The Minnesota, New Jersey, and Oklahoma bills then stipulate that in order to deactivate the filter, all users must submit a request to the platform, "present[] personal identification information to verify that the consumer is 18 years of age or older," and pay a $20 "filter deactivation fee," which goes to the state.[73] A bill introduced in Missouri would require that all internet service providers give customers the option of using a filter.[74]

68 Michael Murney, "Texas Lawmaker Introduces Bill to Ban Kids from Social Media," *Government Technology*, December 13, 2022, https://www.govtech.com/policy/texas-lawmaker-introduces-bill-to-ban-kids-from-social-media.

69 Louisiana Act No. 440, 2022 Regular Session; Mississippi SB 2346, 2023 Regular Session.

70 Arkansas, Mississippi, and Virginia

71 Oregon SB 257, 82nd Leg., 2023 General Session.; Arizona SB 1503, 56th Leg., 2023 Regular Session.

72 Texas HB 1181, 88th Leg., 2023 General Session.

73 Minnesota SF 846, 93rd Leg., 2023 General Session; New Jersey S650, 220th Leg., 2022– 2023 General Session; Oklahoma HB 1050, 59th Leg., 2023 1st General Session.

74 Missouri SB 308, 102nd Gen. Assembly, 2023 1st Regular Session.

Recommendations

With more and more US policymakers considering online child safety proposals that include age assurance requirements, regulators should weigh the tradeoffs of different assurance methods as they select a regulatory path that maximizes benefits and minimizes costs.

Regulators should avoid dictating specific age assurance methods that companies must use. Instead, as they determine the best approach for legislation or executive action, they should consider policy options in three categories:

- Balance: pursue solutions that balance policy objectives and acknowledge tradeoffs.
- Specificity: provide more guidance to users and platforms about age assurance options and requirements.
- Understanding: learn more about how age assurance mechanisms perform in practice.

We offer policymakers and regulators 10 recommendations in these three categories.

Balance

Regulators should choose policy options that acknowledge and mitigate the tradeoffs associated with different assurance methods and that balance competing considerations.

1. **Before enshrining any age assurance methods into law, policymakers should complete cost-benefit analyses (CBAs).**

   It is essential that policymakers formally weigh the advantages and disadvantages of different assurance approaches. A cost-benefit analysis offers a rigorous analytical tool for conducting this assessment. CBAs are commonly used in the executive branch, where offices, like the White House's Office of Information and Regulatory Affairs (OIRA), routinely use them to analyze the impact of agency rules. As Cass Sunstein, a former director of OIRA, has repeatedly emphasized, a CBA is not simply about adding up easily-estimable financial costs.[75] It may also help evaluate the costs and benefits of values that are difficult to quantify, such as privacy. Despite their obvious benefits in helping policymakers evaluate tradeoffs, CBAs are not used routinely in analyzing the potential impacts of proposed legislation. To help better understand the impact of proposed age assurance methods, Congress could provide a CBA of each bill it introduces in this area. The Government Accountability Office or the Congressional Research Service might be well positioned to perform this work. CBAs should be published to inform public debate on proposed legislation.

   CBAs for age assurance in online child safety bills should consider costs and benefits in at least the 10 categories we enumerate above. They should consider not only the impact on minors, but also the impact on other internet users who may be affected by age assurance requirements.

75 Cass R. Sunstein, *Valuing Life: Humanizing the Regulatory State* (Chicago: University of Chicago Press, 2014); Dylan Matthews, "Can Technocracy Be Saved? An Interview with Cass Sunstein," *Vox*, October 22, 2018, https://www.vox.com/future-perfect/2018/10/22/18001014/cass-sunstein-cost-benefit-analysis-technocracy-liberalism.

2. **Regulators should adopt a risk-based age assurance framework that requires providers to match assurance methods to the risks posed by specific products or features.**

   A risk-based framework, which has been adopted in the United Kingdom, Australia, Europe, and California's Age-Appropriate Design Act, permits platforms to reserve more invasive age verification tools for riskier products or features. As a result, platforms may not need to use such tools in low-risk scenarios and may be able to avoid some of the costs of those methods, such as more expansive collection of sensitive data. A risk-based approach permits companies to determine which assurance method is best for their needs and their limitations. This results in companies having the ability to better negotiate tradeoffs.

   For a risk-based approach to work, regulators must provide sufficient guidance for platforms on how to complete risk assessments (see below) and enact verification systems. In the UK's co-regulatory model, there is significant continuing dialogue between platforms and regulators to shape the guidance regulators provide to platforms on compliance.[76] California's AADA establishes the California Children's Data Protection Working Group, which will devise guidance and best practices for implementing and complying with the law. Such guidance for risk-based approaches should be updated regularly and should aspire to be technology-neutral to increase the likelihood that it will endure across new technological developments.

   However, the ultimate success of a risk-based approach will depend on enforcement. If a risk-based approach grants platforms some latitude to adopt unique verification systems that fit their unique needs, it also grants enforcers latitude in interpreting compliance. A risk-based approach may be less successful in the long run if it leaves platforms with too much uncertainty about when governments will decide to enforce it.

3. **Policymakers should provide small companies with tax write-offs for the cost of using certified third-party verification tools.**

   Completing age assurance—and doing so in a way that is equitable, secure, private, and not disruptive—can be expensive, imposing a burden on smaller companies. Federal law provides a range of tax incentives for small businesses, seeking to make it easier for small businesses to grow their businesses in ways that are good for their employees and for society. One example is the credit for small businesses who start a pension plan for employees.[77]

   While regulators likely would face political challenges if they include new tax provisions in an online safety bill, tax policy may be one mechanism to help ensure new compliance obligations do not impose burdens on smaller companies that entrench larger platforms and undermine competition.

76 "Co-Regulatory Model," Resource Center, IAPP, accessed May 25, 2023, https://iapp.org/resources/article/co-regulatory-model/.

77 "About Form 8881, Credit for Small Employer Pension Plan Startup Costs," Internal Revenue Service, last modified September 16, 2022, https://www.irs.gov/forms-pubs/about-form-8881.

Specificity

Regulators should provide sufficient specificity so that companies clearly understand their obligations, best practices, and the tradeoffs associated with different assurance methods.

4. **The National Institute for Standards and Technology (NIST) should release guidance on the risk profiles of different online product features.**

   A risk-based approach relies on platforms realistically identifying the risk of different products or features. However, there may be limited empirical data to understand the risks that some products pose—especially newly released ones. At the same time, larger companies may have an advantage identifying existing evidence regarding the risks their platforms have to children. In providing this resource, the NIST can help protect competition while ensuring that risk assessment is based on empirical data.

   The NIST has experience with this sort of policy guidance. A similar approach was used recently in its AI risk framework.[78] In developing guidance for child safety, the NIST should consult with a wide range of stakeholders across industry, government, and civil society. The NIST should complete, commission, and support additional empirical analyses as needed. This guidance on risk profiles could help online service providers, especially smaller companies, assess and implement age assurance matched to the risks raised by specific features. After publishing it, the NIST should update the resource regularly to account for new product developments.

5. **The FTC should institute a voluntary certification program for third-party age assurance vendors.**

   As age assurance has become more common—either through legal mandate or social or market pressure—third-party companies have begun to offer age assurance services. As noted above, the newly signed Arkansas law requires covered platforms to use third-party age assurance vendors.[79]

   In establishing a certification program, the FTC would first need to identify and then regularly update standards and best practices for age assurance, as well as a set of measures and processes for evaluation. Compliance with these standards will help ensure that third-party age assurance vendors are not only accurately assessing age, but doing so in a way that best balances tradeoffs.

   As a condition of certification, companies should also be required to supply evaluation data with regulators and with independent third-party researchers. This would provide transparency into vendor's methods and allow for broader synthetic analysis of age assurance methods.

   Once a vendor is granted certification, it should be granted a safe harbor from liability if it continues to act in accordance with the program requirements. Similarly, any platform

78 National Institute of Standards and Technology, *NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, US Department of Commerce (January 2023), https://doi.org/10.6028/NIST.AI.100-1.

79 Ark. Code § 4-88-11.

that hires that vendor to handle age assurance should be granted a safe harbor from liability for the age assurance processes provided by that vendor. These limitations on liability will incentivize platforms to offer age assurance options and to choose certified age assurance providers.

6. **Regulators should specify the privacy practices that platforms may use to provide age assurance.**

   The tradeoff between privacy and accuracy is at the heart of much of the concern around age assurance. While the US lacks comprehensive federal privacy legislation, there remains much interest in a federal privacy bill, and eight states have recently passed broad new online policy laws.[80] In privacy regulation and in dialogue with companies, regulators should provide guidance on data minimalization and data retention concerns, specifying the types of data that companies can collect, store, and process as well as what obligations companies have to delete data they have collected. New online data privacy bills often have provisions related to sensitive data, but it is also important that privacy legislation specifically address how data for age assurance can and should be treated.

7. **The FTC should expand its guidance on complying with COPPA to include best practices on age assurance.**[81]

   Beyond providing resources for companies to complete risks assessments, regulators can provide additional guidance on age assurance. Even in the absence of additional regulation in this area, FTC guidance could help companies better understand how to implement age assurance techniques as effectively as possible.

Understanding

Regulators can play an important role in facilitating understanding of the effectiveness of age assurance methods, policies, and the tradeoffs associated with both. Many of these methods and regulatory approaches are novel. As they are implemented in practice, regulators should institute mechanisms to learn about how they perform. Additional understanding will be central to making informed decisions about how to balance different tradeoffs.

8. **State and federal regulators should establish age assurance policy sandboxes to allow participating companies to experiment with age assurance methods while supplying regulators and independent researchers useful data.**

   Several US states, including North Carolina and Arizona, have adopted regulatory sandboxes for financial technology companies.[82] Once admitted to the program, companies in these sandboxes can experiment with new products and approaches without having to comply

80 Joseph Duball, "US House Lawmakers Keep Federal Privacy Legislation Top of Mind," *The Privacy Advisor* (blog), IAPP, March 1, 2023, https://iapp.org/news/a/us-house-lawmakers-keep-federal-privacy-legislation-top-of-mind/; Anokhy Desai, "US State Privacy Legislation Tracker," Resource Center, IAPP, last modified May 19, 2023, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

81 "Complying with COPPA: Frequently Asked Questions," Federal Trade Commission, accessed May 24, 2023, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

82 "Financial and Insurance Regulatory Sandbox," North Carolina Innovation Council, accessed May 24, 2023, https://www.innovation.nc.gov/; Ariz. Rev. Stat. § 41-5601.

with some existing regulation. Sandboxes work by offering to loosen some existing regulatory requirements in exchange for fuller transparency, cooperation, and data access. While state sandboxes would not exempt companies from complying with federal regulation, they could still allow platforms to run time-limited experiments of new age verification systems or products and gain useful insight into product design. Sandboxes could also help supply companies and regulators with additional insight into the true costs of different assurance methods and means of better balancing or mitigating them.

Similarly, the federal government could fund a pilot program to build a secure and private interoperable system for verifying user ages. For instance, the Protect Kids on Social Media Act would establish a "digital identification credential pilot" program.[83] As discussed above, euCONSENT, a pilot program funded in part by the EU, has helped establish the technical systems for an age assurance system that minimizes the data individual companies access or collect.

A similar pilot program in the United States, run as part of a sandbox, could help iron out technical challenges while developing a better understanding of how to reduce some of the risks of implementing this sort of system on a large scale. Importantly, centralizing an age verification system—especially as part of a government program—raises concerns about surveillance and data security. Piloting the program in a limited test could help regulators understand and potentially address some of these concerns.

9. **The federal government should fund research on the impact of different state age assurance regimes.**

   Policymakers can play an important role in facilitating research that helps us better understand and design age assurance systems. As states institute different assurance approaches and regulations, the diversity in state approaches presents something of a natural experiment. Assessing and comparing the impact of these assurance programs can provide better understanding of the strengths and weakness of different approaches. While states individually could offer useful insight into the successes and failures of particular approaches, the federal government can provide a broader comparison across approaches. Toward that end, the FTC should complete and publish a study comparing the costs and benefits of different state models.

10. **The FTC should require certified companies to share limited evaluation data with both government and independent researchers.**

    As discussed above, any third-party FTC certification program should include transparency and data-sharing provisions. Importantly, data-sharing provisions must be carefully constructed. They should not only protect user privacy, but also include safeguards for both researchers and platforms who share data consistent with the terms of the program.[84]

83 S 1291, 118th Cong. (2023 1st Session).

84 Tara Wright, "The Platform Transparency and Accountability Act: New Legislation Addresses Platform Data Secrecy," Stanford Law School, December 10, 2021, https://law.stanford.edu/press/the-platform-transparency-and-accountability-act-new-legislation-addresses-platform-data-secrecy/.

Conclusion

Age assurance policy is hard. While most of us support efforts to ensure children are safe online, identifying which users are children poses persistent and difficult problems. No perfect solution exists. Policymakers are in the unenviable position of choosing from a variety of options that each come with meaningful costs.

In this policy paper, we have attempted to provide a set of options to enable policymakers to make age assurance policy with a full appreciation of the costs of the enterprise. Balancing costs, providing additional specificity, and developing a deeper understanding of both the problem and potential solutions will enable policymakers to make choices about how to proceed without being blindsided by the repercussions. Our hope is that through this framework, future policy will better protect children online, but do so without disproportionately harming other important values, like privacy, usability, competitiveness, and equity.