AMERICAN STYLE AGE VERIFICATION

Meg Leta Jones, Provost's Distinguished Associate Professor, Georgetown University
Clare Morell, Fellow, Ethics and Public Policy Center

The fight to protect kids online is global, but the U.S. has the opportunity to set the standard for strong technical design in age verification and we should take it.

Many of our friends around the world have been working hard to make children safer online. The UK rolled out aggressive site-by-site age verification in July 2025, requiring platforms like Reddit and Discord to demand government IDs or easily bypassable facial scans before users could access what may or may not have been deemed mature content. France has been systematically blocking major porn sites for months, forcing Pornhub, YouPorn, and RedTube to go dark rather than comply with strict "double anonymity" verification rules. Australia is preparing to ban social media entirely for users under 16 by December 2025, while conducting the world's most comprehensive technical trial of age verification technologies.

Each approach is yielding valuable lessons for the United States to use as we develop an American-style age verification infrastructure. Like previous computer challenges in global history, the U.S. has the potential to create and implement *the* standard for seamless, interoperable, innovative age verification. We have the greatest technological means, talent, and resources. The U.S. should be leading the development of the most effective, user-friendly, and privacy-preserving age verification system worldwide.

An American-style age verification infrastructure, unlike other systems we have seen so far, should provide a two-layer system of accountability and interoperability, where each layer works together rather than in isolation to provide the most effective protection to kids and most efficient experience for adults. The two layers are:

1. **Device level**: Whether you're on your phone, laptop, or tablet, major U.S. tech platforms already verify your identity for purchases and security. Apple and Google represent 99% of mobile, Apple and Microsoft represent 89% of desktops, and Apple, Google, and Microsoft represent 89% of browsers–these companies can leverage their existing infrastructure to generate trusted age signals (simple 1 for adult and 0 for child) without sharing personal data.
2. **App/site level**: Categories of sites, platforms, apps, and experiences can then be responsive to these signals. Social media platforms, pornography sites, and AI companions would receive a signal about the age of a user and then implement appropriate protections or restrictions, as well as conduct additional verification when no device signal is sent or they detect a potentially mis-aged user.

This belt and suspenders approach spreads accountability across our Big Tech companies while extending resources to new innovators. Similar to how cybersecurity practices must evolve as landscape changes and companies are held accountable for not using the best practices, an American style age verification system would require "**commercially reasonable**" standards, as many state laws have already included, ensuring that companies are utilizing the technologies and practices that best serve policy goals.

NEW CONSTITUTIONAL CLARITY

For nearly three decades, the U.S. has relied on a single framework for protecting children online: the Children's Online Privacy Protection Act (COPPA) of 1998, which requires companies to treat users under the age of 13 differently from parents. In practice, however, even that boundary has largely collapsed. Most platforms rely on self-declared ages with no verification, allowing millions of children to enter digital spaces as adults. For the seven to nine hours a day that American children now spend online, they are exposed to the same data collection, exploitation, and risks without meaningful safeguards. But change is imminent. In June 2025, the Supreme Court upheld Texas's age-verification law for porn sites in *Free Speech Coalition v. Paxton*, ruling that "adults have no First Amendment right to avoid age verification" and that targeted, well-tailored age verification can survive constitutional scrutiny when designed properly. A number of existing U.S. laws and a slate of bills introduced by Congress and state legislators call for treating children differently than adults online, like age-verification for pornography website laws, the App Store Accountability Act that requires parental consent for app downloads, and other state social media laws that provide restrictions for minors. The U.S. age verification system thus needs to be built now and built well.

HOW IT WORKS

Major platforms already possess sophisticated verification technologies but currently deploy them only selectively for various features. Americans routinely use robust verification daily – from unlocking phones with Face ID to ordering alcohol delivery online – demonstrating that effective, privacy-preserving verification is not only possible but familiar. To make this work for protecting children online, however, platforms must be **required to verify age and required to share verification**. Without a clear legal obligation, devices and operating systems have little incentive to share a simple age signal with sites and apps. Lawmakers should consider mandating both strong age verification and use of an age signal to ensure the most seamless, interoperable, and privacy-protecting experience for users.

In an American style verification system, strong and easy methods to verify age can be combined and provided by big platforms or third party vendors (similar to payments). When users set up Face ID, a process most users opt into, the process could also easily determine if the user is obviously over 18. Scanning a driver's license or state ID with your phone camera takes 10-15 seconds, with the system reading the barcode or chip to confirm your birthdate, the same technology delivery drivers use when you order alcohol and that TSA uses at airport security. Apple now even lets users upload their driver's license once to their Apple Wallet, verified by the state issuing authority, and then it can be easily used to verify the user's age or identity in apps. Some states, like Louisiana, even have their own digital ID program that offers completely anonymous verification for accessing age-restricted sites or platforms. Military, teachers, and first responders have been using ID.me to verify their status for years, and would certainly serve to confirm a user is an adult. Credit card verification (if you have a valid credit card, you're at least 18) or checking with your mobile carrier (phone companies know the account holder's age and can confirm it) can also serve as reliable points of verification.

AGE VERIFICATION AT SET UP

The best moment for age verification is at "set up": when setting up a device, like a phone or tablet, creating an app store account, or logging into a browser. When you get a new phone or computer, age verification happens *once* during the setup process, right alongside setting up Face ID, choosing your password, and signing into your Apple or Google account. Many options are available, but here are a few set up scenarios explaining some of the options:

For adults setting up their own device: During setup, your phone asks "Let's verify you're an adult to enable full features." You choose from several options: take a quick selfie that AI analyzes to confirm you're over 18 (15 seconds, photo deleted immediately), scan your driver's license with your camera (20 seconds) and add it to your digital wallet, use a digital ID, or use the verification you already completed for Apple Pay or your bank (instant if already set up).

When apps or websites need to know if you're an adult, your iPhone generates a temporary signal and the app receives a simple "18+" confirmation but no other personal information about you and no identifier that could track you across different services. Instagram can't tell you're the same person who verified on Pornhub. TikTok can't see what other apps you've verified for. Each verification is a standalone "yes" or "no" with no breadcrumb trail and no personal information about you revealed.

For parents setting up a child's device: During setup, the phone asks "Let's verify you're an adult to enable full features," since in this case the user is a child they will have no means to verify they are an adult, and so when no ID or other verification is provided to prove the user is an adult then the device will say"This appears to be a minor's device. Connect to parent/guardian?" Your child enters your phone number, you get a notification on your phone, you enter your child's date of birth, and you approve the connection with one tap using your Face ID. Now you're connected: your child's device has a "supervised minor" signal and an age category (under 18 or under 13), and you automatically get notifications when they try to download apps, change privacy settings, or make purchases. You can approve or deny with one tap. The device connection uses encrypted signals so apps never learn your child's exact age, name, or your relationship, just that this is a supervised account.

For computers and browsers: The same process happens when you first sign into Chrome, Safari, or Edge, or when you set up Windows Hello or Mac login. Since 89% of browsers and desktops are made by Apple, Google, or Microsoft, companies that already verify identity for payments and security, they can generate age signals the same way phones do. Once the user verifies their age once using an ID or other means for the browser at set up, including even an age signal stored on the device that was established at device set up, the browser then stores the simple age data locally, and when websites request age verification for access, the browser sends the simple "18+" signal and access is granted or in the case of a minor sends the signal that the user is a child and access is blocked. For family computers and shared devices, different accounts for different users can be set up so that each individual's browser is configured to their respective age signal.

USING APPS AND WEBSITES EVERYDAY

American style age verification should not, however, rely exclusively on device verification at set up, but should spread the responsibility of age verification over both "set up" providers like those that control devices, app stores, and browsers, as well as require apps and websites that are age-restricted or require parental consent by law, like social media, messaging apps, and pornography sites, to be responsible for age verifying their users so that minors do not unlawfully gain access. This could be done by requesting an already-existing device age signal for the user or relying on other means to verify the user's age. Here is what this could look like in the following scenarios:

For adults accessing age-restricted content: You open an adult website or try to watch 18+ content on YouTube or you want to create a new social media account or access adult app, like gambling apps. Instead of creating an account or uploading your ID to that website or app, you see: "This site/app requires age verification. Verify with: [Your Phone] [State Digital ID] [Third-Party Service]." You tap "Your Phone," and if you already completed device-level verification, you see "Send age verification signal?" with a simple "Allow" button. You tap Allow, your device sends the encrypted "18+" signal, and you're in. This signal could also be sent automatically if preferred. The website never sees your name, birthdate, address, or ID, just proof that you're verified as an adult. If you have not set up age verification on your device, you could choose your preferred third party service, like ID.me which is already used by millions to verify their age, military, teacher, first responder, insured, employed, etc status. An age signal can easily be sent from these saved sources of verification that have already occurred. Or a user could choose to go through a third-party verifier service that is contracted with the app or website, to verify age through scanning a license (currently used to buy alcohol or ammunition online) or doing a biometric scan of the face or certain hand movements (often used by dating sites to prevent both children and adults from claiming to be an age they are not).

For teens trying to access restricted platforms or apps: A 14-year-old tries to create a TikTok account. TikTok requests age verification from their phone. The phone sends the "under 18" signal. In states that now require parental consent for minors under 18 to create a social media account or to download apps (under the App Store Accountability Act for instance), the app store or platform would then also have to prompt the user to obtain parental consent, sending a verification and consent mechanism to the teen's parent. At the very least, TikTok automatically puts the account in teen mode: no messaging with strangers, limited data collection, no targeted ads for alcohol or gambling, content filtered for age-appropriateness, and stricter default privacy settings. If the teen tries to later change their birthdate to claim they're 18, TikTok triggers additional verification, asking for a real-time verification that could include selfie with liveness detection (blink, turn your head), third party ID verification, device level verification, or another method the company chooses to rely on.

For children who shouldn't have access at all to certain apps and sites: An 11-year-old tries to create a Snapchat account (13+ requirement). Their phone sends "supervised minor" signal to Snapchat. Snapchat sees this and checks: the device signal says this user is under 13, which violates Snapchat's terms. Snapchat blocks account creation and sends a notification to the connected parent: The parent can see what app was attempted but the child cannot bypass the restriction without the parent's explicit approval. Or a minor under 18 tries to access a pornography site (18+ requirement), and the phone sends an under 18 signal or the child can't verify using the other methods of digital ID or third-party, their access to the site is blocked.

NEXT STEPS FOR POLICYMAKERS

Going forward, policymakers should be skeptical of any child protection legislation that fails to mandate robust age verification. An effective American approach should include three key mandates: first, that device manufacturers and operating systems allow users verify age and generate transmittable signals; second, that apps and websites accept and respond to these signals and provide additional options for verifying age; and third, that all parties engage in cooperative technical development to ensure interoperability. Without these requirements working in tandem, we risk creating a patchwork of well-intentioned but messy and potentially toothless regulations. Laws that merely suggest or encourage platforms to verify or communicate ages should not be taken seriously.

CONCLUSION

An American style age verification regime is one that spreads accountability and legal liability across our Big Tech companies, so that both devices and apps are responsible for verifying age in their respective spheres, and this regime will help ensure these two layers work seamlessly together so that the American system is both the most effective at protecting kids and efficient and privacy-protecting for adults. An American style age verification system also would require "**commercially reasonable**" standards, so that companies are utilizing the technologies and practices that best serve policy goals. In sum, the U.S. has the potential to create and implement the gold standard for seamless, interoperable, innovative age verification. We should not miss this opportunity to lead.

AUTHORS

Meg Leta Jones

Prof. Meg Leta Jones is a Provost's Distinguished Associate Professor in the Communication, Culture & Technology program at Georgetown University where she researches rules and technological change with a focus on families, privacy, and automation. Her first book, *Ctrl+Z: The Right to be Forgotten*, explores the social, legal, and technical issues surrounding digital oblivion. Most recently, she published *The Character of Consent: The History of Cookies and Future of Technology Policy*, which tells the history of digital consent through the lens of a familiar technical object. She co-teaches the Tech Impact Lab, which trains students to conduct technical research in partnership with state attorneys general guiding tech policy in their states, and regularly works with policymakers to support strong family technology policy.

Clare Morell

Clare Morell is a fellow at the Ethics and Public Policy Center in the Bioethics, Technology and Human Flourishing Program. Prior to joining EPPC, Ms. Morell worked in both the White House Counsel's Office and the Department of Justice, as well as in the private and non-profit sectors. She is also the author of *The Tech Exit: A Practical Guide to Freeing Kids and Teens from Smartphones*, published by Penguin Random House.

ETHICS AND PUBLIC POLICY CENTER