May 2026

Age Checks: Protection or Overreach?

By Mark Costlow

Using age verification to limit use of online services for children has **become a hot topic** over the past year. At least 28 US states have enacted age verification laws, although some are currently blocked in the courts.

This area of social regulation is changing very quickly. Consider the numbers cited here to be valid in May, 2026, but very fluid and almost immediately out of date. This overview is primarily concerned with the US, where every state has different laws. Other countries, particularly in Europe, are also running full-speed into this morass.

Why Check Ages?

Age-check crusaders have a variety goals, which generally boil down to "protect the children". The big three things to protect them from are pornography, gambling, and social media.

Pornography is legal in the US if produced consensually and only provided to adults. Pre-Internet, age checks were done by the clerk at the sex shop who was supposed to refuse to sell to minors. Porn has been on the internet since the very early days, but with no clerk to deny access to kids. Some justified the situation by requiring a credit card to access adult material, but an enormous amount of porn is available for "free". As with most free services, **there is a cost**, usually advertising exposure, compromised privacy, or risk of being scammed. But none of that verifies the customer's age.

Gambling is a quiet problem in our society. Most aren't even aware of how pervasive it has become. Hundreds of gambling sites offer casino games, lotteries, and hugely popular and profitable sports betting. Sites like FanDuel and DraftKings have been accused of **enticing underage gamblers**, trying to pull in life-long **suckers**. **49% of 17-year-olds report gambling**, both sports betting and in-game gambling such as paying real money for a random loot box of unknown virtual contents.

Social media has been with us for 20 years, and the potential mental health harms are becoming apparent. With features like infinite scroll and algorithmic feeds designed to maximize engagement, one may feel more like cattle being herded than a human engaging with community.

Epidemics of isolation, loneliness, and cyberbullying all contribute to the urge to limit young minds' constant exposure.

The Internet didn't create these social woes or moral hazards. But it acts as a force multiplier, removing the physical-world friction that once stood between our worst impulses and regrettable action. You don't have to fly to Vegas or even drive to a local casino to place a sports bet, just pull out your phone. Porn isn't in the box in the back of the closet, it's in your pocket with you all the time. And if you're being bullied at school, there's no going home to get away. It can follow you everywhere.

How to Check Ages?

This is the obvious first question: how can you reliably determine someone's age over the Internet without compromising their privacy and opening the door to even more egregious consequences? Sadly there is no good answer. Every solution to date has significant problems.

In the lingo of this topic, most of the laws require "**Age Assurance**". That is, a web site must be assured that the user is above the required age for the service, using one of these methods:

- **Self Attestation** - You check a box that says you are over 18. Obviously, people may lie.
- **Age Estimation** - Algorithms try to guess your age based on your picture, voice, and/or online behavior: what you watch, like, or post. Computers are bad at classifying accurately over large populations. For example, people of color are routinely misidentified by facial recognition systems.
- **Actual Verification** - You submit government documentation to prove your age: driver's license, passport, utility bill, or other documents. This has huge privacy impacts. Do you really want to give an offshore gambling site your passport details or home address?
- **Age Assurance** by proxy - A 3rd party attests that you are of age without giving up details about your identity.

That last option is likely to be widely adopted. Here's a **brief overview of how it works**.

Microsoft, Google, and Apple operating systems have tamper-resistant unique identifiers and storage, which we talked about in our **December, 2025 issue**: Microsoft's TPM and Apple's Secure Enclave in particular. The idea is that you go through a process to prove your age to your phone or computer. Your identity is confirmed by biometrics (fingerprint or facial recognition). When asked, the Microsoft, Google, or Apple servers indicate your age bracket to the requesting site or app without giving them your private information, just a yes or no to the age question.

This seems like the closest thing to a solution

that is privacy-preserving, accurate, and scalable to thousand of apps and web sites. It shifts the burden of age verification away from parents, and away from site and app operators, onto computer Operating System providers.

The dark side of this solution is that it requires you to be logged in to Apple, Microsoft, or Google at all times, and that has privacy implications. If you are concerned about having your every digital move tracked and have taken pains not to participate in forced enrollment in these large corporate surveillance grids, you may be locked out of visiting many web sites.

What Do the Laws Require?

Every state has a different take on this issue. We'll glance at a couple of the laws that have already been passed, starting with California, because laws there tend to have a resounding "us too" effect on the rest of the country.

The "California Age-Appropriate Design Code Act" was passed in 2022, blocked in 2023, partially re-instated in 2024. It is based on a similar UK law, and requires services used by minors to accurately guess their age. Companies are prohibited from using "**dark patterns**" to coerce users into sharing data or allowing tracking that they did not intend. There are penalties, $2,500 or $7,500 per child, for negligent or intentional violations respectively.

The "California Digital Age Assurance Act" has been signed into law and goes into effect Jan 1, 2027. This law requires operators to estimate the age of users and categorize them in 4 slots: under 13, 13-15, 16-17, and 18+.

California's "Protecting Our Kids from Social Media Addiction Act" was enacted Jan 1, 2025, and requires age verification be in place by Dec 31, 2026. It requires platforms to exclude under-18s from "addictive" feeds. It also prohibits the sending of notifications from 12AM to 6AM year round and 8AM to 3PM on school days, to prevent social media alerts from disrupting sleep or school. Both limitations can be lifted with parental consent.

New Mexico doesn't have an age verification law yet. HB 313 in 2025 would have required age range signals for device makers and app stores. Among the opposition to this law, the **Computer Communication Industry Association argued** that the bill was not well thought out. It contained many vague and undefined directives which they said would inevitably lead to costly litigation. The bill did not pass and was not re-introduced in 2026.

All of these laws are lacking. They are reactionary, fail to consider many unintended consequences, and are mostly debated by people with limited technical understanding. For example, limiting notifications might reduce engagement somewhat, but most phone-addicted people don't need a notification to keep checking for new content. The California law which prohibits "notifications" does not define "notifications", and that lack of specificity always invites gaming of the system.

The **Free Speech Coalition's Bill Tracker** is watching the progress of about 40 current bills. This patchwork of legal and technical requirements is spurring development of services and advice for getting around the requirements.

For example, age verification requirements in the US prompted the PornHub pornography site to deny access to customers in about 20 US states rather than comply with the laws. This means PornHub determined that it was less expensive to block those users and force them to find their own way around the problem than to add the controls.

It is easy to use a VPN to get around a geographical block for a site like PornHub that refuses to do age verification. It will require more creativity to get around age verification that is tightly coupled with device operating systems, but motivated teens will find a way.

One glaring contradiction in these debates is that the dark patterns and coercive algorithms used by YouTube, TikTok, and Facebook are somehow only dangerous for children. These practices work quite well on adults. A New York University study found that 65+ individuals are more susceptible to some dark patterns than younger people. Why are we treating a symptom of the problem, only for part of the population, instead of addressing the real issue of using devious practices to manipulate people?

Education would be better way to prevent harm. Social Media Literacy classes could help kids recognize when they are being manipulated. **ConnectSafely.org** has parents' guides for every kind online service. It's not a panacea, but being consciously aware of the environment goes a long way to keep people from falling into traps. Media and Financial Literacy would also help a great deal. Understanding how you are targeted in each of those areas is a great defense against forces that rely on us scrolling infinitely and clicking without thinking.

This Month in Ideas & Coffee

- **May 13 6pm-7:30pm –** Phish Proof Founders will host a game of *Backdoors and Breaches*.
- **May 19 6pm-7:30pm –** *WordPress Work Along* – Answers to your pressing WordPress questions. Bring your laptop!

Watch the **Ideas & Coffee** event calendar at **https://swcp.com/calendar** for future info.

Southwest Cyberport – swcp.com

New Mexico's Expert Internet Service Provider since 1994

505-232-7992 | Support: help@swcp.com

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Click on bold blue type in browser for links.