WHEN “AGE VERIFICATION” GOES WRONG

connect x protect

How Some Bills Could Backfire for Real Families

Everyone agrees: kids and teens deserve safer online spaces. But some age verification proposals could create new risks while promising protection.

Here’s what that might look like in real life.

Scenario 1: The Data Breach

A mom uploads her driver’s license to verify her teen’s age for access to an app. Months later, a centralized verification database is hacked or a third-party provider mishandles the data.

Her teen’s:

- Full name
- Date of birth
- Home address
- ID number

are now circulating online.

The bill was supposed to protect her child. Instead, it created a permanent digital vulnerability by forcing the collection of sensitive data that platforms never needed in the first place.

When we mandate the collection of sensitive ID data, we create massive targets for hackers.

Scenario 2: The False Sense of Security

A dad believes the new law means his teen can’t access inappropriate content anymore. But his daughter:

- Downloads a VPN
- Switches to browser-based platforms
- Joins encrypted messaging groups where content is entirely unmoderated

The content didn’t disappear. The law simply drove her to "darker corners" of the internet with fewer safeguards.

Dad thinks she’s protected. She’s actually less supervised than before.

Safety that’s easy to bypass isn’t safety.

Scenario 3: The Teen Who Needs Help

A 16-year-old in a small town searches online for:

- LGBTQ+ support
- Mental health resources
- Eating disorder recovery information

Under strict ID verification requirements, she must upload personal documentation to access educational forums or community groups. She decides not to for fear of discovery.

She loses access to the only safe, anonymous support system she had.

When privacy disappears, at-risk teens go silent.

Scenario 4: The Problem That Was Never Fixed

A kid begins seeing increasingly extreme content in his feed.
His parents assumed new age verification laws would make platforms safer. But nothing about the platform's design changed because the law focused on the "front door" instead of the product itself.

- The recommendation algorithms still prioritize engagement over safety.
- Harmful content is still amplified to age-verified users.
- Addictive product features remain in place.

The teen's age was verified. The system worked as designed. But the content ecosystem itself was untouched.
When safety measures focus only on verifying age, rather than addressing foundational problems around how content is amplified and monetized, the underlying risks remain.
Verifying a birthdate does not remove a dangerous algorithm or fix harmful design.
Real protection requires accountability for the products and systems shaping what teens see.

Scenario 5: The Sidelined Parent

A state mandate sets rigid digital age restrictions, prohibiting minors under the age of 16 from accessing a wide array of digital content and services.
A parent who knows her mature 15-year-old can responsibly use certain educational or social platforms now has no flexibility.
Instead of empowering parents with better tools, the law replaces family judgment with state-mandated bans.
Parents should be supported, not replaced.

What Real Protection Looks Like

Real online safety means:

- Privacy-preserving age assurance (not ID checks)
- Stronger safety-by-design requirements that fix the product
- Real accountability for harmful algorithms and platform design
- Clear, flexible parental controls that keep families in charge
- Solutions that work across the entire internet, not just "device-limited" targets

Kids and teens shouldn't have to give up their personal data to be protected. Parents shouldn't be given false promises. And social media companies shouldn't be allowed to shift their liability onto app stores and parents.