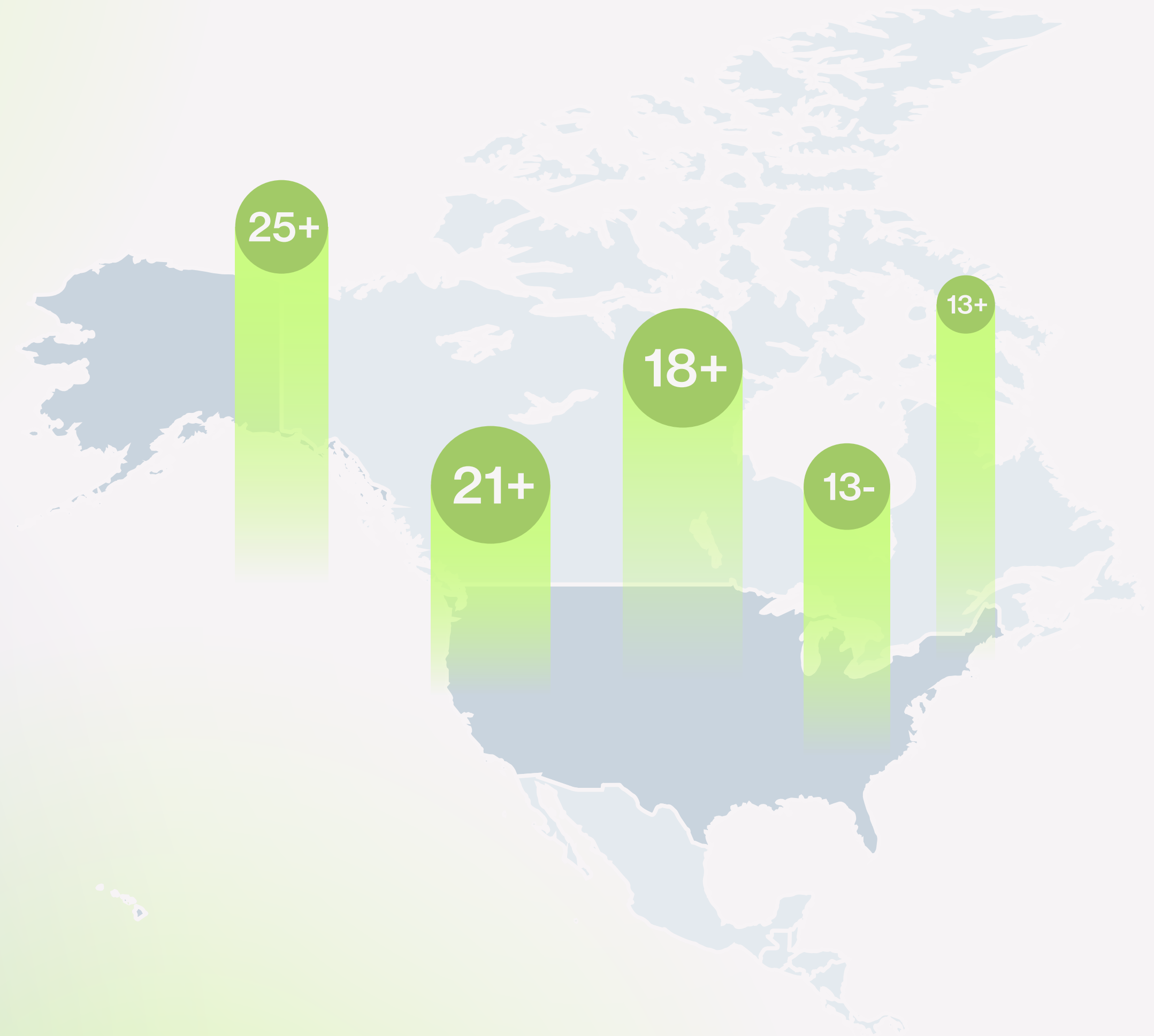


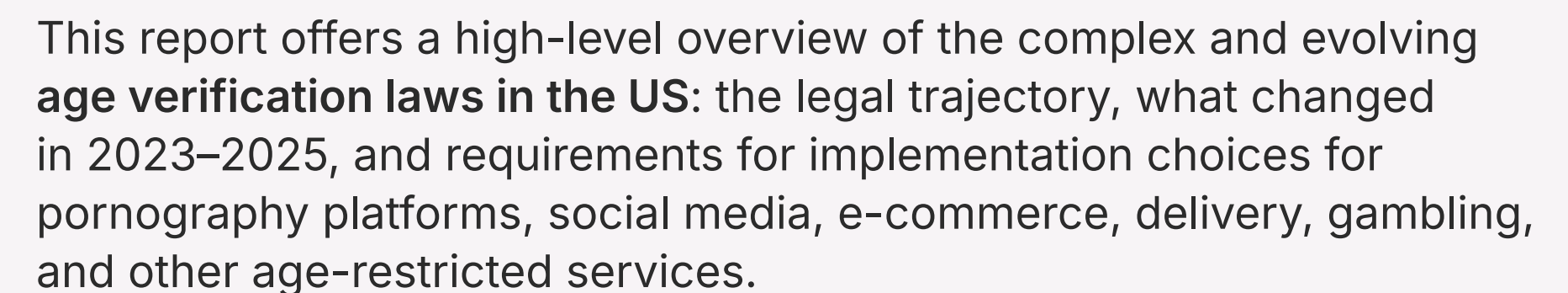
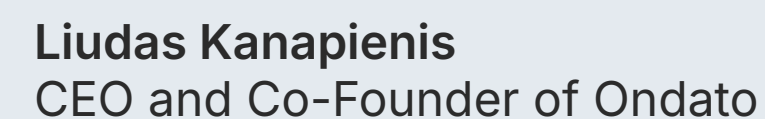
The Surge of the US Age Verification Laws: 2026 Outlook

A practical guide to current requirements, risks,
and implementation options



As we move into 2026, understanding the trajectory of these developments is crucial. The momentum built over the past years suggests that more states are likely to adopt or revise age verification requirements, shaping the compliance environment for businesses in increasingly complex ways. Recognizing the patterns of 2023–2025 will help you anticipate and better prepare for what lies ahead in 2026.

With more US states introducing and debating age verification laws, businesses are under growing pressure to stay compliant. At Ondato, we've built our solutions to make that easy, helping companies adapt quickly to new rules and prepare for what's coming next in 2026.



2

Contents

A Historical Overview of Age Verification in the US	4
From Anonymity to Identity: Key Shifts in Age Verification Legislation	9
Challenges of Age Verification Implementation	11
Age Verification Law State Tracker	13
Industries Subject to Age Verification	18
Technologies and Age Verification Methods	20
Age Verification Debates and Controversies	23
Ondato's Age Verification Solutions	26
Key Terminology	27

A Historical Overview of Age Verification in the US

American age checks started in the analog world: bouncers at the door, clerks at the counter, and state “police powers” to protect minors. Here is a chronological evolution of the age verification legislation in the US.

ACCESS TO SEXUALIZED (OBSCENE) PUBLICATIONS

- Mid-20th century**
States used “police powers” to regulate morality and commerce.
- 1968**
The US Supreme Court ruled in the Ginsberg vs. New York that states can ban sales of sexually explicit materials to minors.
- Following 1968**
Nearly every US state adopted “harmful to minors” laws.

MINIMAL DRINKING AGE

- Mid-1900s**
US states began using physical ID checks for alcohol and tobacco sales.
- Early 1970s**
Many states lowered the minimum legal drinking age to 18–20.
- 1984**
Congress passed the Uniform Drinking Age Act, linking highway funding to a drinking age of 21.
- 1988**
All states raised the minimum legal drinking age back to 21.

Youth protection era

The arrival of the internet complicated things – it became very difficult to regulate what children can see, consume, and buy online. For years, websites relied on “**I am 18+**” buttons, which wasn’t a strong protection measure. And since children were particularly vulnerable to data exploitation, manipulation through targeted advertising, and harmful content, the US governmental bodies sprang into action to stop this.



1998

The Children's Online Privacy Protection Act ([COPPA](#))

- Applies to websites directed at children under 13
- Requires websites to provide clear privacy notices
- Mandates verifiable parental consent before collecting children's personal information
- Allows parents to review and delete their children's data
- Focuses on data privacy rather than age verification
- Requires the verification of parents' identity for consent

2000

The Children's Internet Protection Act ([CIPA](#))

- Ties federal E-rate subsidies to internet safety policies in schools and libraries
- Requires content filters that block obscene or harmful material
- Mandates monitoring of minors' online activities
- Requires education about appropriate online behavior
- Emphasizes content filtering over user identification
- Set the stage for ongoing debates about blocking content vs. verifying age to protect children

2019

[Tobacco 21](#) Legislation

- Amendment to the federal Food, Drug, and Cosmetic Act
- Prohibits to sell all tobacco products, including e-cigarettes, to anyone under 21
- Creates a uniform national standard, replacing inconsistent state laws

2020

California Privacy Rights Act ([CPRA](#))

- Grants consumers new rights to correct inaccurate data and limit the use of sensitive personal information
- Defines "sensitive personal information", including health, biometrics, and precise location data
- Requires businesses to practice data minimization and use data only for stated, necessary purposes
- Mandates transparency about data collection, sharing, and targeted advertising
- Enhances accountability through risk assessments, audits, and stricter enforcement powers

Surge in age verification state laws and litigation

2023-2025

- [Louisiana](#) passed Act 440 becoming the first state law requiring adult websites to verify that users are at least 18 before granting access.
- [FDA](#) Final Rule requires retailers to check photo IDs of all customers who appear under 30 and limits vending machine sales to adult-only locations.
- At least 25 states enacted similar pornography age verification laws.
- At least 15 states enacted or attempted [“kids’ codes”](#) for social media platforms, requiring age verification and parental consent for minors’ accounts.
- Many laws held adult content platforms liable for failing to verify ages and allowed parents or minors to file civil lawsuits.
- Laws required social media companies to verify user ages, ban the collection of minors’ personal data, and provide parental dashboards.
- Courts blocked parts of Arkansas’s Social Media Safety Act and California’s Age-Appropriate Design Code due to First Amendment concerns.

Precedent:

In June 2025, the US Supreme Court ruled in [Free Speech Coalition v. Paxton](#), upholding [Texas’s HB 1181](#), which mandates age verification on pornography websites via government IDs or by checking transaction data. [The Court also ruled](#) that no one has a First Amendment right to avoid age verification for content that is harmful to minors. However, the Court’s decision did not address a separate part of the Texas law that would have required health warnings on these sites – that provision remains blocked and was not part of this case.

After June 2025

More states proceeded to advance age verification bills, while attorneys general started enforcing existing laws.

2023

First Wave of Age Verification Laws

- Louisiana Act 440 (HB 142)
- Utah SB 287
- Mississippi SB 2346,
- Virginia SB 1515
- Texas HB 1181
- Arkansas SB 66 (passed, enforced 2024)

2024

Enforced Laws

- FDA Final Rule - ID check for all under-30 tobacco/vape customers
- Arkansas Act 612 (SB 66)
- North Carolina HB 8 (PAVE Act)
- Idaho HB 498
- Nebraska LB 1092 (Online Age Verification Liability Act)
- Oklahoma SB 1959
- Alabama HB 164
- Indiana SB 17
- Kansas SB 394

2025

Laws Enforced or Taking Effect

- Texas HB 1181 (upheld by SCOTUS)
- Florida HB 3
- South Carolina HB 3424
- Georgia SB 351
- Arizona HB 2112
- Ohio HB 96
- Wyoming HB 43
- North Dakota HB 1561
- South Dakota HB 1053
- Missouri AG Rule 15 CSR 60-17 (rulemaking)

From Anonymity to Identity: Key Shifts in Age Verification Legislation

Driven by state legislations, the US is gradually moving from a philosophy of online anonymity towards **the mandatory digital identity** aimed at protecting children. Yet, the practical result is a fragmented, privacy-invasive system that is not fully effective and is pushing smaller online entities out of business.



From Self-attestation to Proof-based Methods

Early internet sites relied on self-attested age ("Are you over 18?"), which is easily circumvented. After realizing that minors are likely to misreport age, modern laws demand stronger proof: government-issued ID scans, credit card data matching, or biometric age estimation.

Acceleration of Patchwork Laws

Between 2022 and 2025, US states rapidly enacted laws for adult content and social media. **Adult content laws** typically require site operators to implement age verification technology or face liability. **Social media laws** often impose parental consent for users under 18. Adding to the confusion, some laws apply only to large platforms, while others cover nearly all online services. All this patchwork has intensified compliance burdens and highlighted the need for federal legislation.

Court Interventions and Enforcement Blocks

Several laws have been challenged for violating the First Amendment or the dormant Commerce Clause. Courts temporarily blocked parts of Arkansas' Social Media Safety Act and Montana's TikTok ban. Before the Supreme Court's 2025 decision, lower courts often found that age verification mandates chilled free speech for adults. Meanwhile, the new precedent reduced the likelihood of successful challenges for pornography regulation but leaves open questions for social media regulations.

Enforcement Patterns

In the US, attorneys general lead enforcement, sometimes joined by private rights of action. Many laws create statutory damages per violation, encouraging lawsuits against non-compliant platforms. Others designate state agencies to impose penalties or revoke business licenses. Civil penalties may reach thousands of dollars per violation, and some laws allow minors to sue for emotional distress.

First Amendment Re-evaluation

The Supreme Court applied a lower standard of scrutiny to an adult content age verification law, departing from a history of striking down such laws under the strict scrutiny test. By ruling that requiring ID to access protected speech is only an "incidental" burden, the court made it easier for governments to impose verification mandates on broader online services – delivering a major blow to digital free speech.

Challenges of Age Verification Implementation





User Circumvention and Laws' Ineffectiveness

Practice shows that after a state enacts an age verification law on a major compliant platform, like a porn site, users simply move to non-compliant sites or use VPNs to bypass the restriction. This way laws fail to fully achieve their goal of protecting minors and instead drive users (minors and adults) toward smaller, less regulated, and potentially more dangerous platforms that operate outside US standards, worsening the overall safety problem.



Only Giant Companies Can Afford to Comply

Implementing robust age verification systems is expensive, involving complex technology, data security, and legal counsel. As a result, smaller platforms can't afford to meet new compliance regulations and are forced to geo-block states or shut down. Only major tech giants can absorb the expense and legal risk, thus consolidating market power and reinforcing the dominance of Big Tech.



Lack of Interoperability Standards

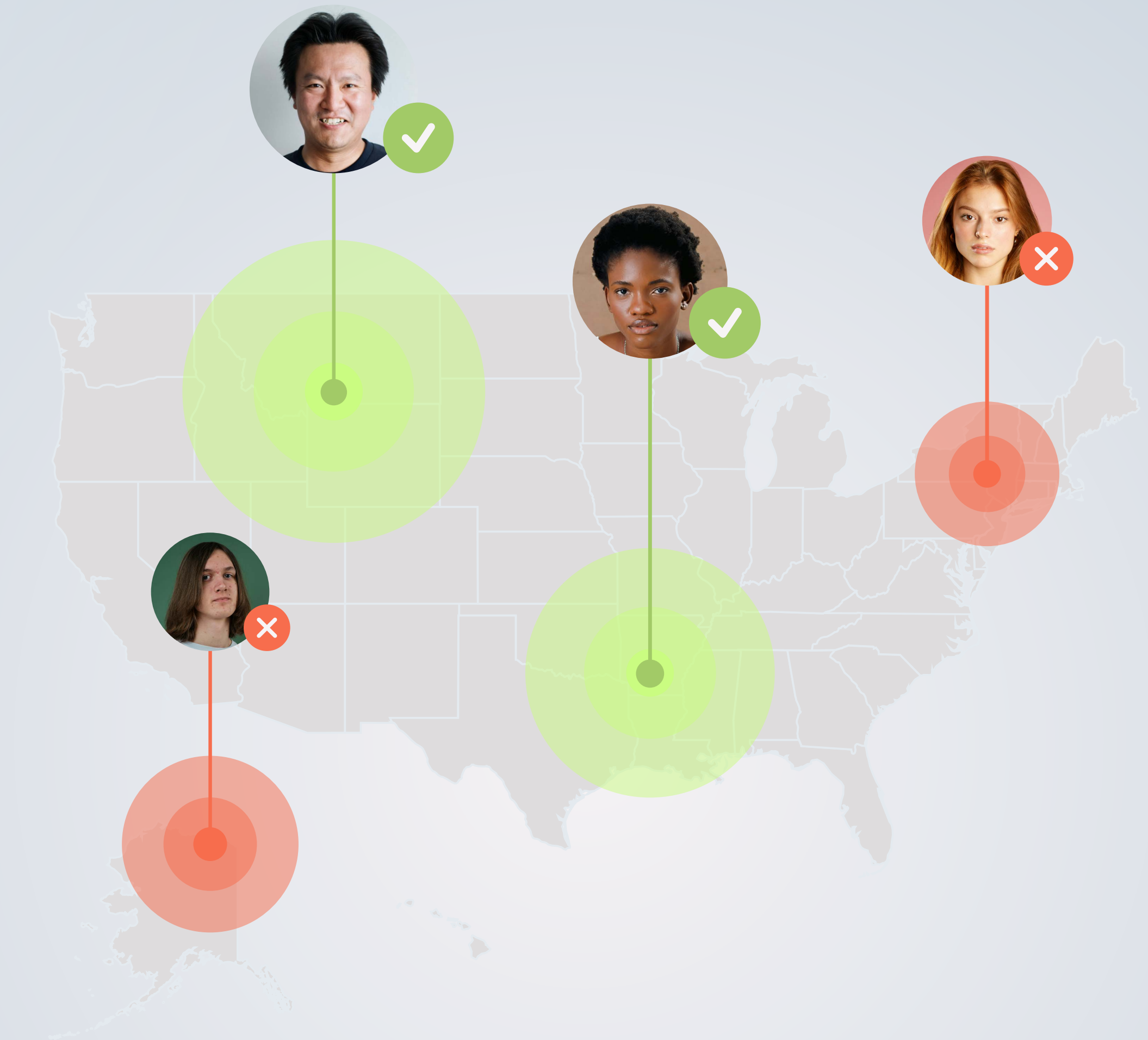
Accurately verifying age without requiring excessive disclosure of personal information while protecting data privacy and security is very difficult. And cross-border coordination remains a persistent challenge, as national preferences and legal frameworks vary, making technical interoperability essential. Without standardized systems, users must repeatedly verify their age on each platform, resulting in friction and increased abandonment. So, a widespread adoption requires standards (like ISO 27566), consensus, and governance.



Technical Inaccuracy and False Results

The accuracy of age verification is based on factors like image quality, gender, region of birth, and age, with no single algorithm working reliably across all demographics. Mean absolute errors have decreased from 4.3 to 3.1 years over the past decade, but this may still not be reliable enough for applications requiring precise age verification. To maintain low false positive rates, age estimation tools often require setting the challenge threshold between 29 and 33 years, meaning systems designed to block 18-year-olds might only reliably block users who appear under 30. Also, these systems can be circumvented using deepfake technology or simple image modifications.

Age Verification Law State Tracker



State	Law/Bill #	Scope	Enactment	Effective	Key Requirements	Enforcement & Penalties
Alabama	HB 164 (2024)	Adult-content sites (≥33.3% "harmful to minors")	2024-04-24	2024-10-01	Reasonable AV (digitized ID, third-party service, transactional data); no data retention after access	Private right of action; civil penalties; Attorney General (AG) enforcement
Arizona	HB 2112 (2025)	Adult-content sites (≥33.3% "harmful to minors")	2025-05-13	2025-09-26	Reasonable AV; government ID or third-party verification	Civil penalties
Arkansas	Act 612 (SB 66) (2023)	Adult-content sites (≥33.3% "harmful to minors")	2023-04-11	2023-07-31	Reasonable AV; third-party allowed; no data retention	Private right of action; statutory damages, incl. attorney fees
Florida	HB 3 (2024) (Ch. 2024-42)	Adult-content sites (≥33.3% "harmful to minors")	2024-03-21	2025-01-01	Reasonable AV; delete identifying data after use; ID or third-party permitted	Civil penalties; AG enforcement
Georgia	SB 351 (2024)	Adult-content sites (≥33.3% "harmful to minors"); separate social media AV provision enjoined	2024-04-23	2025-07-01	Reasonable AV; government ID or third-party verification	Civil penalties; private lawsuits; AG enforcement
Idaho	HB 498 (2024)	Adult-content sites (≥33.3% "harmful to minors")	2024-03-21	2024-07-01	Reasonable AV; third-party allowed; no data retention	Private right of action; injunctive relief
Indiana	SB 17 (2024)	Adult-content sites (≥33.3% "harmful to minors")	2024-03-13	2024-07-01	Mobile driver's license credential or third-party AV; no data retention after access	Private right of action; AG enforcement
Kansas	SB 394 (2024)	Adult-content sites (≥25% of pages monthly with material "harmful to minors")	2024-04-25	2024-07-01	AV via commercial database or other AG-approved method; no data retention	Civil fines; private right of action
Kentucky	HB 278 (2024)	Adult-content sites (≥33.3% "harmful to minors")	2024-04-05	2024-07-15	Reasonable AV; third-party allowed; no data retention after verification	Civil remedies; AG enforcement; private right of action (up to \$10,000 per violation)

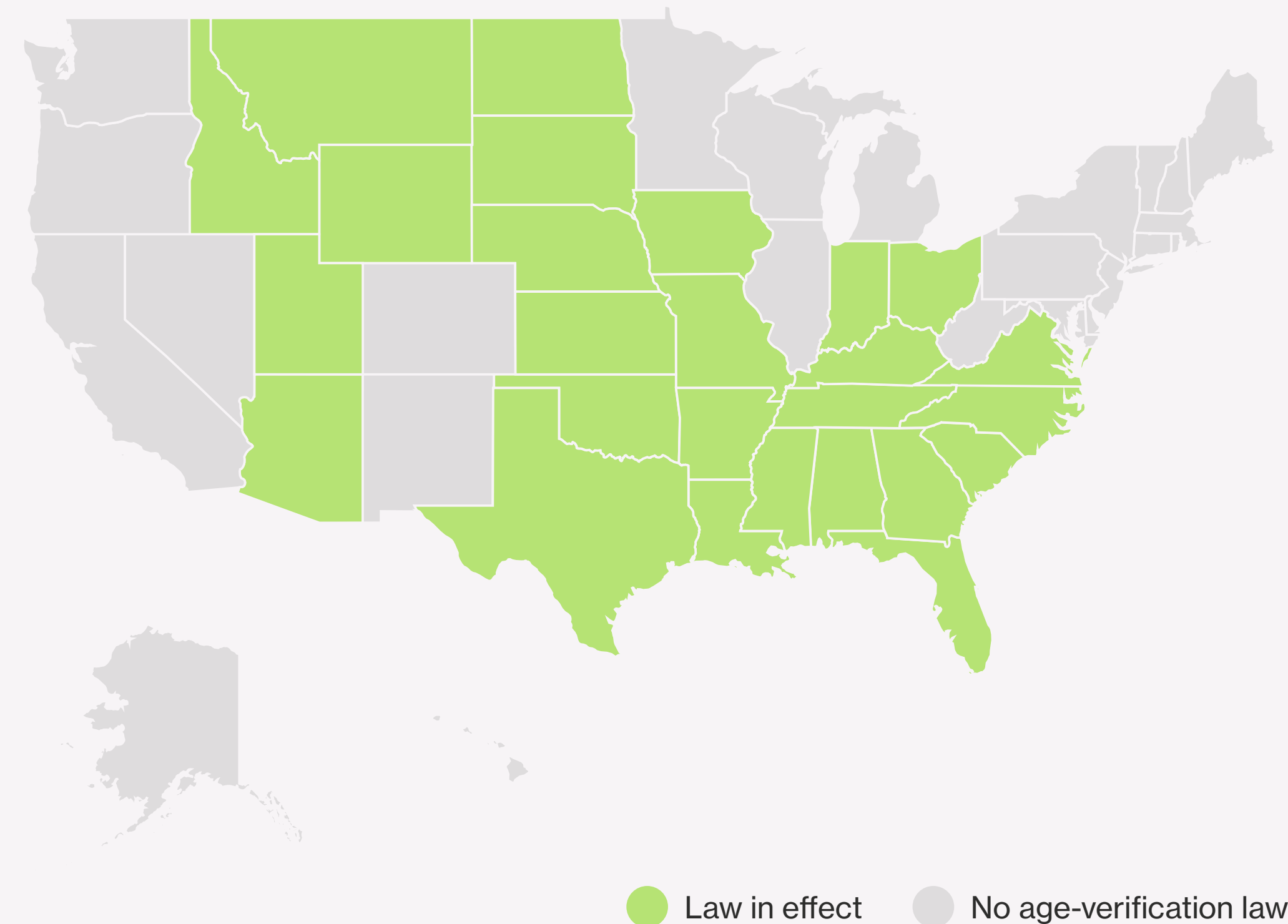
State	Law/Bill #	Scope	Enactment	Effective	Key Requirements	Enforcement & Penalties
Louisiana	Act 440 (2022)	Adult-content sites (≥33.3% "harmful to minors")	2022-06-16	2023-01-01	Digital ID (incl. "LA Wallet" app) or third-party AV; no data retention	Private right of action; \$1,000+ statutory damages per violation
Mississippi	SB 2346 (2023)	Adult-content sites (≥33.3% "harmful to minors")	2023-03-22	2023-07-01	Reasonable AV; third-party allowed; no data retention	Private right of action (civil damages)
Missouri	15 CSR 60-18	Adult content sites with (≥33.3% "harmful to minors")	2025-05-15	2025-11-30 per AG announcement	Digital or government-issued ID or a commercial age verification system; no data retention (unless required by law)	AG enforcement; MMPA private action; ≤ \$10 000/day cap
Montana	SB 544 (2023)	Adult-content sites (≥33.3% "harmful to minors")	2023-05-19	2024-01-01	"Reasonable" AV; annual DOJ enforcement report required; no data retention	Private right of action (including attorney fees and punitive damages); AG may seek injunctions/penalties
Nebraska	LB 1092 (2024) – Online Age Verification Liability Act	Adult-content sites (≥33.3% "harmful to minors")	2024-04-18	2024-07-19	Digitized ID; third-party or transactional data verification; no data retention	Private right of action (civil liability)
North Carolina	S.L. 2023-132 §3.20 (HB 8)	Adult-content sites (≥33.3% "harmful to minors")	2023-09-26	2024-01-01	Commercially available database or third-party AV; no data retention	Private right of action (parent/guardian may sue); civil penalties
North Dakota	HB 1561 (2025)	Adult-content sites (≥33.3% "harmful to minors")	2025-05-27	2025-08-01	Reasonable AV; no data retention	Private right of action (parent/guardian); civil penalties for violations
Ohio	HB 96 (2025)	Adult-content sites ("obscene or harmful to juveniles" content)	2025-06-30	2025-09-30	"Reasonable" AV; periodic re-verification of age every 2 years	Civil penalties (fines); AG enforcement authority

State	Law/Bill #	Scope	Enactment	Effective	Key Requirements	Enforcement & Penalties
Oklahoma	SB 1959 (2024)	Adult-content sites (≥33.3% “harmful to minors”)	2024-04-26	2024-11-01	Digitized ID; third-party or transactional data verification; opt-out exemption for ISPs/mobile carriers	AG enforcement; private lawsuits
South Carolina	HB 3424 (2024)	Adult-content sites (≥33.3% “harmful to minors”)	2024-05-21	2025-01-01	“Reasonable” AV; third-party allowed; no data retention	Civil penalties; AG enforcement
South Dakota	HB 1053 (2025)	Adult-content sites (no threshold specified)	2025-02-27	2025-07-01	Government-issued ID, financial info, or other “reliable” method to verify age; no data retention	Criminal offense (Class 1 misdemeanor) for violations; AG enforcement (90-day notice to cure)
Tennessee	SB 1792 (2024) – Protect Tennessee Minors Act	Adult-content sites (≥33.3% “harmful to minors”)	2024-05-28	2025-01-01	Government-issued photo ID with liveness check or transactional data; re-verify age every 60 minutes; strict data deletion rules	Criminal penalties; private lawsuits (minors’ parents may sue)
Texas	HB 1181 (2023)	Adult-content sites (≥33.3% “harmful to minors”)	2023-06-12	2023-09-01	Government ID or “commercially reasonable” transactional data verification; (required health warning provision struck down)	Civil penalties (up to \$10,000 per violation); AG injunctive enforcement
Utah	SB 287 (2023)	Adult-content sites (≥33.3% “harmful to minors”)	2023-03-23	2023-05-03	Reasonable AV; third-party allowed; no data retention	Private right of action; civil penalties
Virginia	SB 1515 (2023)	Adult-content sites (≥33.3% “harmful to minors”)	2023-03-27	2023-07-01	Commercial age verification service or database; no data retention; must post privacy notice	Private right of action; \$150,000 statutory damages per violation
Wyoming	HB 43 (2025)	Adult-content sites (no threshold specified)	2025-03-13	2025-07-01	Reasonable AV; applies based on user’s Wyoming residency or presence; no data retention	Private lawsuits (user or parent); \$5,000 statutory damages per failure + costs

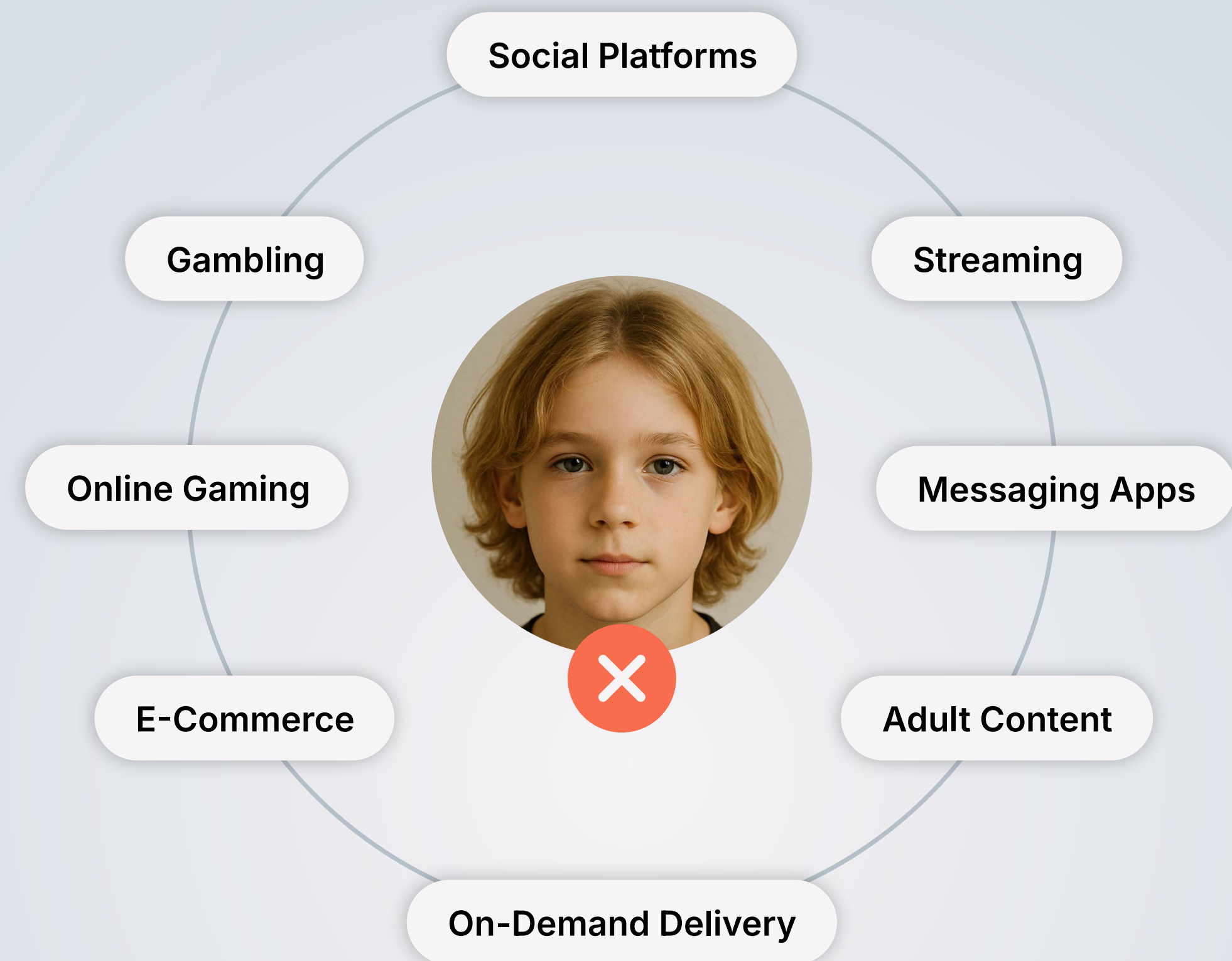
No State-Level Age Verification Law in Effect

The following states (and territories) have not yet enacted state-level age verification laws for adult content or social sites (end of 2025), but many are actively considering proposals for future enactment:

- › **Alaska**
- › **California**
(injunction in place blocking enforcement)
- › **Colorado**
- › **Connecticut**
(only Kids Code applies for privacy, no explicit age verification for adult content)
- › **Delaware**
- › **District of Columbia**
- › **Hawaii**
- › **Illinois**
- › **Maine**
- › **Maryland**
(Kids Code applies, no explicit age verification law)
- › **Massachusetts**
- › **Michigan**
- › **Minnesota**
- › **Nevada**
- › **New Hampshire**
- › **New Jersey**
- › **New Mexico**
- › **New York**
- › **Oregon**
- › **Pennsylvania**
- › **Rhode Island**
- › **Vermont**
- › **Washington**
- › **West Virginia**
- › **Wisconsin**



Industries Subject to Age Verification



Adult Content Platforms

Age verification mandates for pornography sites are the most developed. Laws require sites to confirm that users are 18 or older before displaying explicit material. Many statutes provide safe harbors for platforms that rely on third-party age verification providers. Non-compliance can result in fines, civil action by parents, or platform de-listing. Following [the Supreme Court's Paxton decision](#), new laws may survive First Amendment challenges. However, [civil-rights groups](#) argue that rigorous verification deters adult access, threatens anonymity, and could create databases of users' sexual interests.

Social Media and Online Communities

Kids' codes require social media platforms to estimate users' ages at sign-up, obtain verifiable parental consent for minors, and offer privacy protections. Some laws restrict features such as algorithmic feeds or messaging for minors. Enforcement is complex because social-media platforms have global user bases, and verifying age across jurisdictions is challenging. Laws often target large platforms (with more than 5 million users). Civil society groups warn that age gates could push minors to unregulated sites and harm their ability to access support communities.

E-Commerce and On-Demand Delivery

E-commerce platforms delivering age-restricted products (alcohol, tobacco, cannabis) must implement age verification at purchase and delivery, by using devices to scan government IDs at the point of delivery. Some states require the delivery person to check ID physically rather than rely on digital signatures. Proposed laws may extend age verification to online purchases of knives, fireworks or violent video games.

Alcohol, Tobacco and Vaping

Retailers must verify age for alcohol and tobacco sales. The federal [Tobacco 21 law](#) prohibits any retailer from selling tobacco products to individuals under 21. A [2024 FDA rule](#) requires retailers to check photo IDs of customers under 30 and restricts vending machines to adult-only venues. For alcohol, US states enforce the MLDA of 21 and increasingly require electronic ID scanning. For example, a [2025 compliance update](#) reports that California, New York and Texas introduced tighter ID scanning protocols; retailers must use devices compliant with ISO-18013-5 to read mobile IDs, and failing to verify age can result in fines and license suspensions. Minor missteps, such as not scanning IDs or accepting expired IDs, can lead to penalties.

Medical and Recreational Cannabis

With recreational cannabis legal for adults 21+ in at least 18 states, dispensaries must verify customers' ages. Best practices include training employees to check IDs and using ID scanners; violations can incur hefty fines. For example, [Alaska](#) fines repeat offenders up to \$50,000, California fines up to \$5,000 per violation (and up to \$30,000 for unlicensed establishments), Maine fines up to \$100,000, and Oregon imposes license suspensions or fines for first-time sales to minors. Privacy concerns arise because scanning IDs collects personal data. Therefore, dispensaries must safeguard information and avoid retaining unnecessary details.

Lottery, Gaming, Online Betting

Most US states require players to be at least 18 (or 21 for some games). Online betting platforms often rely on credit-header databases, knowledge-based authentication (KBA), or geolocation tools to verify age and residency. Age verification is also integrated into [Know Your Customer \(KYC\)](#) procedures mandated by anti-money laundering laws.

Technologies and Age Verification Methods





Self-Attestation and Payment Checks

The simplest approach is asking users to affirm they are of age by using payment card information as a proxy; for example, requiring a credit card for purchase. These methods are easy but unreliable because minors can lie or use adults' cards.



Document Scanning and Barcode Parsing

Most laws require scanning government IDs (driver's licenses, passports) and parsing barcodes to validate the date of birth. Modern retail environments often use electronic ID scanners integrated with point-of-sale systems; some states mandate scanning rather than visual inspection. Mobile driver's licenses (mDLs) using the ISO 18013-5 standard are increasingly accepted; they allow age verification without revealing full identity.



Verifiable Credentials and Zero-Knowledge Proofs

Emerging standards allow third-party attestations (for example: "Over 18") to be stored in wallets. Zero-knowledge proof is a cryptographic technique that confirms a user's age without revealing their identity or storing raw data. The adoption of these methods is still in its infancy, but it could help reconcile age verification with privacy concerns.



Biometric Age Estimation

Emerging technologies are very effective when it comes to analyzing faces and estimating age. When implemented following the privacy and accuracy standards recommended by the KJM principles, [biometric age estimation](#) offers a convenient solution that quickly verifies age while significantly minimizing user data collection.



Knowledge-Based Authentication (KBA)

Users answer questions from public records; for example, "Which of these streets have you lived on?". However, the KBA method is declining because personal data breaches may make answers available to minors and criminals.



Database and Credit-Header Checks

Age verification providers can match user-supplied information (name, address, date of birth) against government or credit-header databases. This method is widely used by gambling and financial services but may exclude people without credit histories or those mis-recorded.



Mobile Driver's Licenses and Digital Wallets

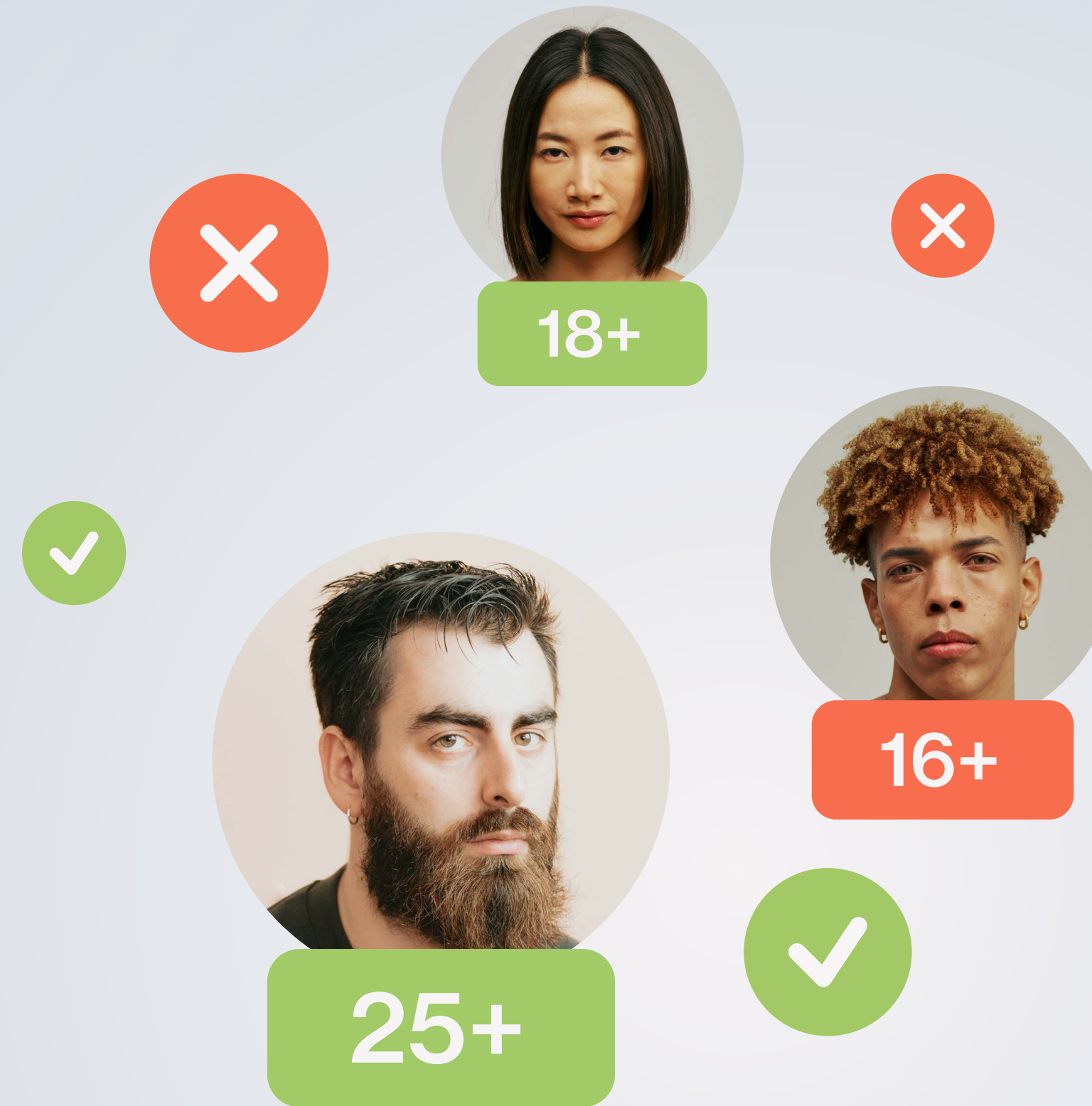
mDLs store encrypted credentials on smartphones. Verification uses cryptographic signatures to confirm data authenticity, allowing selective disclosure of age without revealing full identity. States like California and New York encourage businesses to upgrade scanners to read mDLs.

Risk-Based Age Verification Method Comparison

In order to evaluate how strong each age verification method is, how much friction it adds for users, and where it fits best, let’s review the main types of age verification methods currently used across industries today.

Method	Assurance level	User friction	Use cases
Self-attestation ("I am 18+" checkbox)	Very Low	Minimal	Informational sites, legacy age gates
Payment proxy (credit card / digital wallet check)	Low–Medium	Low	Low-risk online stores, age-restricted marketing
Database match (credit-header, telco, DMV lookup)	Medium	Moderate	Moderate-risk adult content, gambling onboarding
Document scan + mDL verification	High	High	Pornography AV laws, gambling, alcohol delivery
Biometric + liveness (face or voice match to ID)	Very High	Moderate	Financial KYC, repeat user login for adult platforms
Zero-Knowledge / Verifiable Credential (ZK/VC)	High (privacy-preserving)	Low–Moderate	Privacy-sensitive environments; decentralized AV proofs

Age Verification Debates and Controversies



Data Minimization and Retention

Age verification systems collect sensitive personal data (IDs, facial images). Laws often require providers to store data only as long as necessary, but enforcement is uneven. Privacy by design, encryption, and zero-knowledge proofs aim to minimize data retention.



Interoperability and Standards

The growth of mDLs, verifiable credentials, and biometric systems underscores the need for interoperability across states and platforms. Without common standards, users may need multiple credentials for different services, raising friction and privacy risks.

Proportionality and Necessity

Critics question whether broad age verification mandates are necessary to achieve child-protection goals, especially when they expose users to data-collection risks. They advocate targeted measures (for example: content moderation, digital literacy) rather than universal age checks.



Preemption and Federal Action

Tobacco 21 law demonstrates how federal action can harmonize state laws. Some advocate a federal age verification framework to replace the state patchwork, balancing child safety with civil liberties. Others caution that centralizing control could stifle innovation and entrench large platforms.



Business Burden and Compliance Costs

Companies face high compliance costs to implement verification systems across jurisdictions. A patchwork of state laws increases complexity; some call for federal standards. Small businesses and non-profit websites may struggle to afford third-party verification, potentially driving them offline.



Child Safety vs. Privacy and Free Expression

Proponents argue that age verification laws protect children from harmful content and addictive social-media designs. Opponents, including civil-liberties groups, warn that mandatory age gates chill adult speech, deter individuals from accessing lawful content, and jeopardize anonymity. The Electronic Frontier Foundation criticized the Supreme Court's 2025 decision for undermining privacy and argued that adults will be reluctant to share personal information.



Biometric Bias and Accessibility

Age-estimation algorithms may misclassify people of certain demographics (people with darker skin tones, non-conforming gender presentations, and disabilities), raising concerns of discrimination. Additionally, not everyone possesses government ID; for example, undocumented persons or unhoused youth, which could exclude them from services or information. Policymakers must ensure equitable access and alternative verification methods.



2026 Outlook on the US Age Verification Laws

It seems like 2026 will be the year when age verification stops being a niche compliance add-on and becomes a pillar of digital identity governance in the US. Here is what may await us in 2026.

Federal baseline law incoming

The Congress or the Federal Trade Commission will propose national standards driven by the legal certainty created by the Texas HB 1181 Supreme Court decision in 2025.

Expansion beyond adult content

The US Age Verification laws are likely to extend to social media, gaming, app stores, and age-restricted e-commerce.

Higher technological standards

More rigorous proofs will be required, such as mDL-based verification, biometric liveness, and privacy-preserving zero-knowledge proofs.

Litigation wave

As civil-liberties and data-retention challenges will grow, courts will refine the boundary between legitimate state interest (protecting minors) and adult free-speech, data privacy, and anonymity rights.

Industry convergence

Age Verification laws are likely to merge with digital identity frameworks, age-assurance certification, and privacy mandates (CPRA and state data laws). Regulators may require vendors to delete identifying data once age has been confirmed, or to use encrypted tokens.

Geo-blocking becomes standard

Companies operating nationally or globally will increasingly adopt geo-blocking strategies, i.e. blocking access in specific states, or implement state-by-state variation of flows.

Regulation of other age-sensitive products

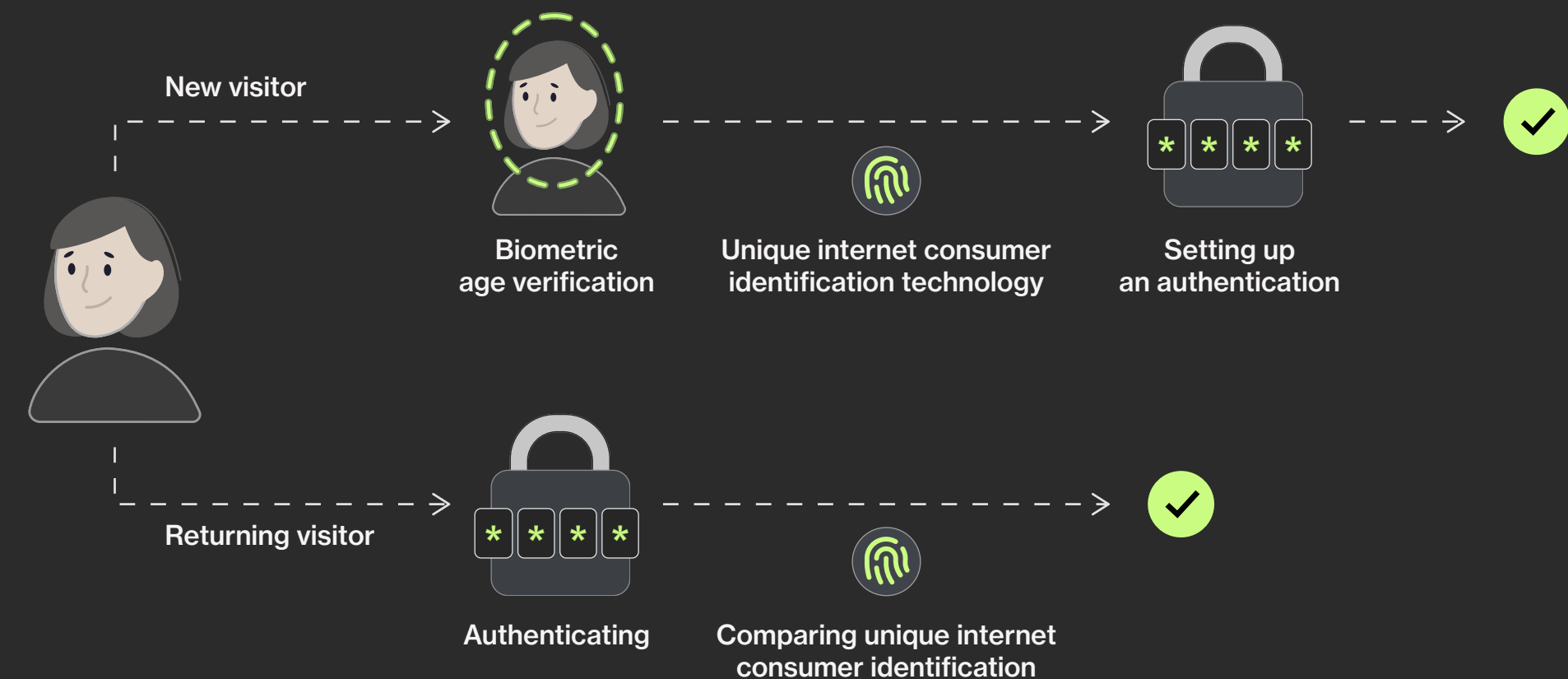
Age Verification laws are likely to target gaming/online betting, streamed gambling-like services, virtual social spaces (metaverse), and age-restricted e-commerce categories (cannabis, erotic accessories, etc.).



Reusable Age Verification

Ondato's latest age verification solution, OnAge, offers reusable verification. Businesses can adhere to even the most stringent privacy and security requirements thanks to our privacy-focused verification, which guarantees that only the user's age eligibility status is kept and that all other data is erased following the verification. Furthermore, "OnAge" allows for customisable integration into any website or application without forcing users to download any extra apps.

To reuse their verification, users set a 4-digit PIN, which grants access to age-restricted content for a time period defined by the service provider. This new solution is designed to streamline age-restricted access, creating a more convenient process for returning users and, in turn, increasing user retention.



Document-Based Age Verification

Ondato's system ensures users meet age requirements by verifying government-issued IDs (passport, ID card, or driver's license). Using advanced OCR and AI, it extracts data like date of birth and checks the document's authenticity against global databases. The system ensures high accuracy, complying with strict regulations, without storing personal data.



Age Estimation

Ondato's AI-powered age estimation uses biometric technology to assess a user's age by analyzing facial features, without needing identity documents. It captures a live image, estimates age in real time, and ensures regulatory compliance while protecting user privacy with strong encryption and GDPR compliance.

Key terminology

Age restriction A type of content or activity legally limited by age (must be 21+ to buy alcohol), and age verification may be one way to enforce it.

Age verification A proof-based check (ID, trusted data, or biometric/age estimation) that confirms a user is 18+ before access or transaction.

Data minimization A privacy principle that suggests companies should limit the collection of personal information, including age or identity data for verification, to what is strictly necessary to achieve a specified purpose.

Digital age of consent The specific age at which a person can legally consent to the processing of their personal data (for example: creating an account or using a service) without requiring parental authorization. This age varies by state in the US.

Harmful to minors A legal standard or definition used in age restriction laws, particularly those related to content, that determines if the material is sufficiently explicit or inappropriate that its access by children should be restricted or prohibited.

Know your customer (KYC) A process, often used in financial services and certain regulated industries, that involves verifying the identity and age of a client to comply with legal requirements and prevent fraud or money laundering.

Minor/child A person under a certain legal age, typically 18 in most US states, though the specific age can vary depending on the context of the law.

Obscene to minors Material that is sexually explicit and meets the legal test for obscenity when aimed at minors, meaning it lacks serious value and can be treated as criminally illegal. It implies content prohibition and potential criminal prosecution.

Parental consent A permission workflow for minors, often for accounts or data processing.

State-level legislation Laws pertaining to age verification or age restriction that are enacted by individual US states, which are distinct from federal law.

**Are you ready to find out more
about Ondato Age Verification?**