MAYER | BROWN

JANUARY 28, 2026

LITTLE USERS, BIG RULES: TRACKING CHILDREN'S PRIVACY LEIGISLTATION

Amber Thomson, Howard Waltzman, Megan Von Klein, Even Han, Dara Garcia

---

Legislative and regulatory activity throughout 2025 and the beginning of 2026 reflects sustained federal and state attention on how children's personal information is collected and used online and protecting children's privacy and mental health. At the federal level, the Federal Trade Commission (FTC) published its Final Rule Amendments to the Children's Online Privacy Protection Rule (COPPA) on April 22, 2025, and subsequently, on June 27, the US Supreme Court upheld a state law requiring age verification to access adult-content websites. Several states are also advancing legislation aimed at strengthening children's privacy protections. Before delving into a more detailed discussion of this recent activity, the following developments help to provide important context:

- **Texas's Supreme Court Victory**: The Court upheld Texas's age-verification law for adult content sites, paving the way for similar state measures.
- **Harmful Content Age-Verification**: States are adopting site-level age-gating requirements for adult content sites and apps, including "commercial age-verification systems," session timeouts, prompt deletion of verification data, and substantial civil penalties.
- **Device-Based Filters**: States like Alabama and Utah now require default filters on internet-enabled devices used by minors.
- **Age-Appropriate Design Codes**: California, Maryland, Nebraska, and Vermont have enacted child-centric platform design obligations limiting profiling, dark patterns, and geolocation; however, California's law remains under a preliminary injunction, and Maryland's law is facing a pending legal challenge.
- **App Store Accountability**: California, Texas, Louisiana, and Utah require app stores to verify users' ages, obtain parental consent, and display clear age ratings.
- **Social Media Restrictions**: 16 states are advancing measures to restrict minors' access to social media platforms and require parental consent and platform-level age checks.
- **Children's Data Protection**: Beyond COPPA, states are imposing consent requirements for targeted advertisements and data sales, data minimization and purpose limitation obligations, DPIAs for high-

risk processing, restrictions on dark patterns and precise geolocation, recognition of universal opt-out signals, and attorney-general enforcement with per-violation penalties.

Below, we examine the Supreme Court's ruling in greater detail and highlight insights from our Children's Privacy Legislature Tracker.

Supreme Court Upholds Texas Law Requiring Age Verification for Adult-Content Websites

On June 27, 2025, the Supreme Court upheld Texas' HB 1181 in Free Speech Coalition, Inc. v. Paxton (6–3, Thomas, J.). The Court held that Texas may require adult-content websites to verify that users are 18 or older before displaying sexual material harmful to minors. While adults retain the right to access the content, the Court held that this right does not include the ability to bypass age-verification requirements.

What HB 1181 Requires: HB 1181 applies to any commercial website where more than one-third of the content constitutes sexual material harmful to minors. Covered operators must implement a "commercial age-verification system" that relies on government identification, transactional data, or digital ID, either directly or through a third-party provider. Noncompliance may result in injunctions, civil penalties of up to $10,000 per day, and up to $250,000 if a minor gains access.

The Court's Reasoning: The Court determined that HB 1181 regulates minors' access to harmful material and that any burden on adults is incidental, triggering intermediate scrutiny. The Court emphasized age checks are an "ordinary and appropriate" means of enforcing age-based restrictions, drawing analogies to checks for alcohol, firearm sales, and driver licensing.

Scope and Signal. The Court noted that more than 20 states have enacted similar laws and that its decision effectively affirms the constitutionality of state age-verification regimes targeting sexually explicit material harmful to minors. The Court underscored that no person—adult or child—has a First Amendment right to access materials that are obscene to minors without first providing proof of age, foreclosing arguments that adults may bypass verification.

In light of this ruling, adult-content websites serving Texas users should now treat age-gating as a firm compliance obligation. Practical steps include selecting a compliant verification method, updating public-facing disclosures, and implementing privacy controls to minimize, secure, and promptly delete verification data. The Texas Attorney General is positioned to pursue injunctions and monetary penalties promptly.

Businesses should anticipate more active enforcement and potential multistate coordination as other jurisdictions with similar statutes rely on the Court's intermediate-scrutiny framework.

Snapshots of State Legislation

Below, we provide a high-level overview of legislative activity across the states in several key categories of children's privacy laws. More detailed state-by-state information is available in our Children's Privacy Legislation Tracker.

Supreme Court Upholds Texas Law Requiring Age Verification for Adult-Content Websites

On June 27, 2025, the Supreme Court upheld Texas' HB 1181 in Free Speech Coalition, Inc. v. Paxton (6–3, Thomas, J.). The Court held that Texas may require adult-content websites to verify that users are 18 or older before displaying sexual material harmful to minors. While adults retain the right to access the content, the Court held that this right does not include the ability to bypass age-verification requirements.

What HB 1181 Requires: HB 1181 applies to any commercial website where more than one-third of the content constitutes sexual material harmful to minors. Covered operators must implement a "commercial age-verification system" that relies on government identification, transactional data, or digital ID, either directly or through a third-party provider. Noncompliance may result in injunctions, civil penalties of up to $10,000 per day, and up to $250,000 if a minor gains access.

The Court's Reasoning: The Court determined that HB 1181 regulates minors' access to harmful material and that any burden on adults is incidental, triggering intermediate scrutiny. The Court emphasized age checks are an "ordinary and appropriate" means of enforcing age-based restrictions, drawing analogies to checks for alcohol, firearm sales, and driver licensing.

Scope and Signal. The Court noted that more than 20 states have enacted similar laws and that its decision effectively affirms the constitutionality of state age-verification regimes targeting sexually explicit material harmful to minors. The Court underscored that no person—adult or child—has a First Amendment right to access materials that are obscene to minors without first providing proof of age, foreclosing arguments that adults may bypass verification.

In light of this ruling, adult-content websites serving Texas users should now treat age-gating as a firm compliance obligation. Practical steps include selecting a compliant verification method, updating public-facing disclosures, and implementing privacy controls to minimize, secure, and promptly delete verification data. The Texas Attorney General is positioned to pursue injunctions and monetary penalties promptly.

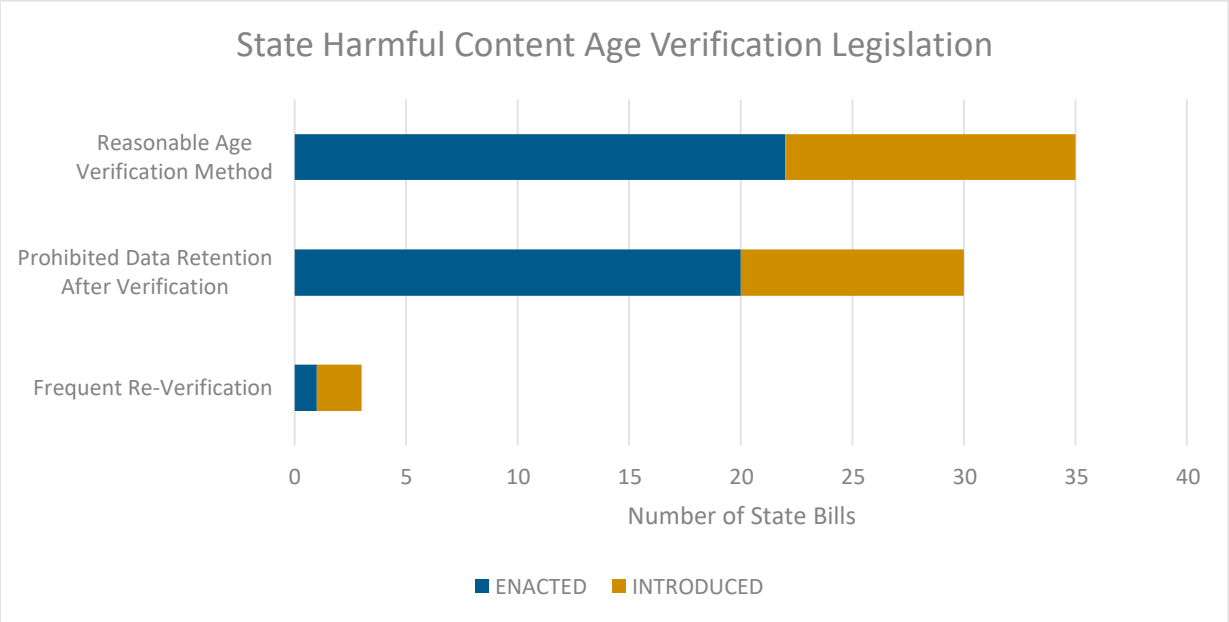
Businesses should anticipate more active enforcement and potential multistate coordination as other jurisdictions with similar statutes rely on the Court's intermediate-scrutiny framework.

Snapshots of State Legislation

Below, we provide a high-level overview of legislative activity across the states in several key categories of children's privacy laws. More detailed state-by-state information is available in our Children's Privacy Legislation Tracker.

I. Harmful Content Age-Verification Legislation

Even before the Supreme Court's decision upholding Texas' HB 1181, states had begun advancing age-verification laws to restricting minors' access to harmful content. The Court's ruling has further validated and accelerated these efforts. By confirming that such laws are subject to intermediate scrutiny—requiring a substantial relation to the important governmental interest of protecting children—the Court provided a workable constitutional framework that other states can rely on when defending similar statutes. As of January 2026, 25 states have enacted or introduced age-verification laws targeting minors' access to harmful content, as reflected in the graph below.



Among these, Tennessee's Protect Tennessee Minors Act is particularly notable, as it captures the full range of compliance requirements and illustrates how state-level harmful content legislation operationalizes age-verification and privacy safeguards:

Reasonable Age Verification Method: The Act requires website operators to verify users' ages through a "reasonable age-verification method," which may include matching a real-time photo of the user to a government-issued ID or using a commercially recognized data source, such as transaction or employment records, to confirm that a user is over 18. The verification method must be implemented in a manner not easily bypassed or circumvented and applied before adult content becomes accessible.

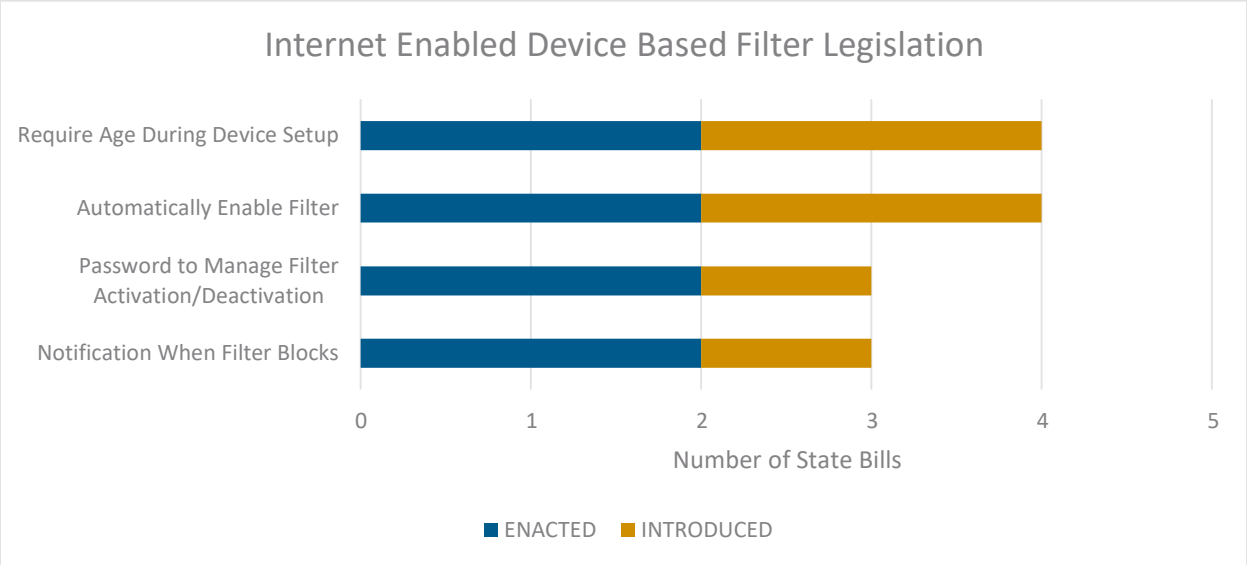
Prohibited Personal Information Retention: Operators and third-party verification providers must delete personally identifying information once access is granted. Only anonymized verification data, i.e., documentation proving that verification occurred without linking it to individual identities, may be retained for compliance purposes.

Frequent Re-Verification. An age-verified session lasts for the lesser of the verified user's active session or 60 minutes from the time of verification. After that period, users must re-verify to maintain access.

II. Internet-Enabled Device-Based Filter for Harmful Content

Another emerging legislative strategy requires new internet-enabled devices to activate a filter for minors. Under these laws, any device identified as being used by a minor must automatically enable a filter that blocks access to harmful content. As these requirements are relatively new, no legal challenges have yet been filed.

As of January 2026, Alabama (SB 186) and Utah (SB 104) have enacted these laws, while Idaho (SB 1158) and South Carolina (H. 3399), have introduced similar bills.



Alabama's SB 186 illustrates how the device-based filter model is implemented:

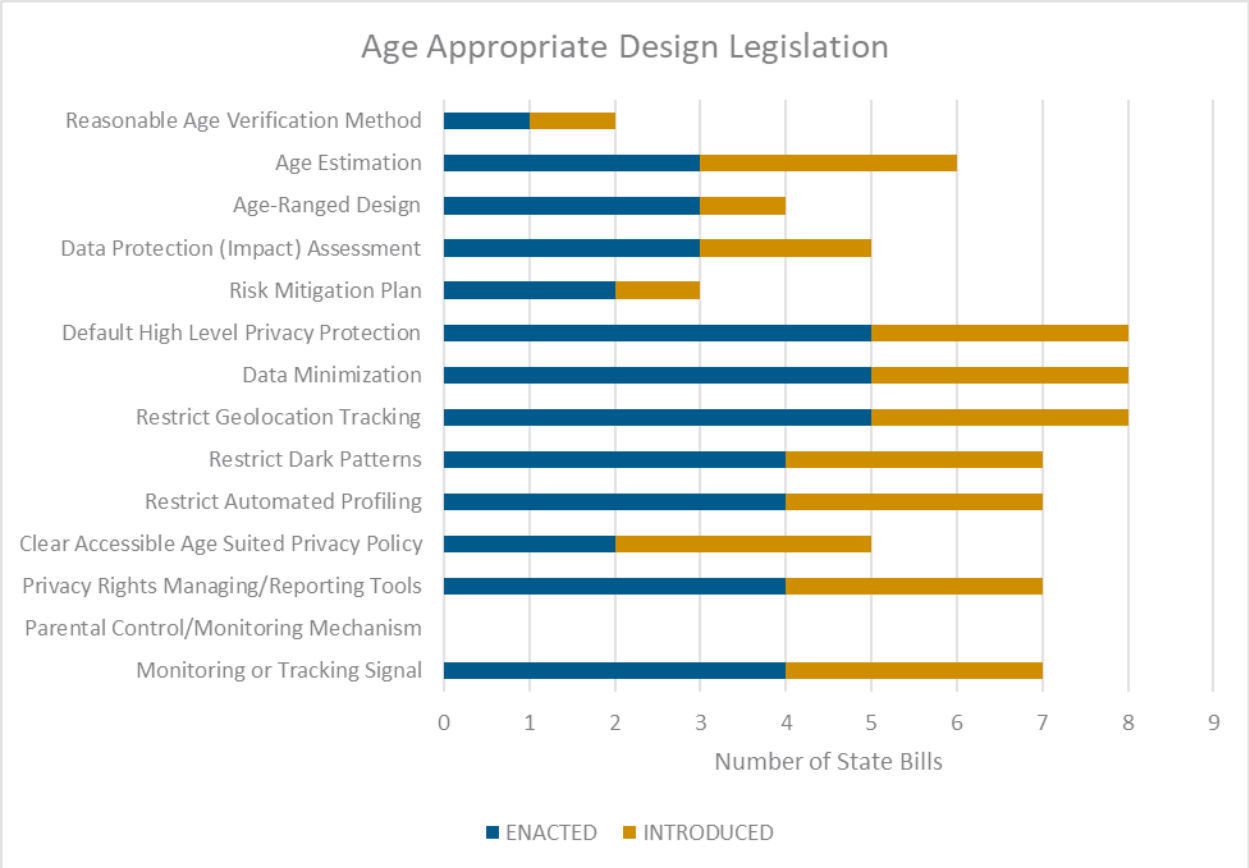
- Age Prompt During Device Setup: During activation and account setup, the device must prompt for the user's age to determine whether the user is a "minor" for compliance purposes.
- Automatic Filter Activation: If the user is identified as a minor, the device must automatically enable a filter. The filter must be "generally accepted and commercially reasonable" software that blocks access to obscene material across manufacturer-controlled browsers and search engines on mobile, wired, and Wi-Fi networks.
- Password-Protected Management: The device must allow a password to manage the filter. Any non-minor with the password may deactivate and later reactivate the filter.
- User Notification: The device must notify the user when the filter blocks access to a website.
- Liability Frame: Manufacturers may face civil liability if a device activated in-state lacks the required filter at activation and a minor accesses obscene material. A good-faith effort to auto-enable a compliant filter provides protection.

For manufacturers, these laws signal a meaningful shift in compliance expectations: regulators are increasingly looking to device-level safeguards—not just platform or content-level controls. With new bills already pending in states such as Illinois and New Hampshire, this device-oriented approach is likely to spread, raising the stakes for proactive compliance planning and implementation.

III. Age-Appropriate Design Codes

States are increasingly adopting child-centric design laws that require online platforms to prioritize minors' privacy and safety by default. As of January 2026, four states have enacted such laws: California (California Age-Appropriate Design Code Act), Maryland (Maryland Kids Code), Nebraska (Nebraska Age-Appropriate Online Design Code Act), and Vermont (Vermont Age-Appropriate Design Code Act). On January 21, the

South Carolina legislature also passed legislation including an age appropriate design code, which is now awaiting signature by the governor.



Maryland's Age–Appropriate Design Code Act illustrates many of the requirements commonly found in these laws:

- **No Mandatory Age Verification Method**: This Act does not require the use of a specific age-verification method. The requirements apply to covered entities that offer online products "reasonably likely" to be accessed by children.

- **Age Estimation Limits**: Covered entities may not process personal information to estimate a child's age beyond what is reasonably necessary to provide the online product. They may not collect additional data beyond what is necessary to determine whether a product is reasonably likely to be accessed by children.

- **Age-Ranged Design Obligations**: Covered entities must design, develop, and provide online products consistent with the best interests of children reasonably likely to access them. Privacy disclosures must be tailored using clear, age-appropriate language.

- **Data Protection Impact Assessments**: Covered entities offering online products reasonably likely to be accessed by children must complete and maintain a data protection impact assessment on

specified timelines, addressing concrete risks and describing steps taken and planned to meet the duty to act in the best interests of children.

- **Risk Mitigation Planning**: Each assessment must include a description of measures implemented in a manner consistent with the best interests of children reasonably likely to access the online product, be reviewed following material changes, and be provided to the Division upon request within statutory timeframes.

- **Default High-Privacy Settings**: All default privacy settings for children must offer a high level of privacy, unless the covered entity can demonstrate a compelling reason that a different setting is in the best interests of children.

- **Data Minimization Requirements**: Covered entities may not process a child's personal information that is not reasonably necessary to provide the online product with which the child is actively and knowingly engaged. They may not process such data for purposes other than those for which it was collected.

- **Restrictions on Geolocation Tracking**: Processing precise geolocation data by default is prohibited unless strictly necessary to provide the product and only for the limited time needed; an obvious signal must be provided for the duration of the collection.

- **Restrictions on Dark Patterns**: Covered entities may not use dark patterns to cause a child to provide unnecessary personal information, circumvent privacy protections, or take actions the entity knows or has reason to know are not in the child's best interests. A "dark pattern" is defined as a user interface that substantially subverts or impairs user autonomy, decision-making, or choice.

- **Limits on Automated Profiling**: Profiling a child by default is prohibited unless appropriate safeguards ensure it is consistent with the child's best interests, and that it is necessary to provide the requested product for features the child is actively and knowingly using, or there is a compelling best-interests justification.

- **Clear, Accessible, Age-Appropriate Privacy Policies**: Privacy information, terms of service, policies, and community standards must be provided concisely, prominently, and in clear language suited to the age of children likely to access the product.

- **Privacy Rights Tools**: Covered entities must provide prominent, accessible, and responsive tools to help children or their parents or guardians exercise privacy rights and report concerns.

- **Meaningful Reporting Tools**: The Act requires tools that enable children or their parents or guardians to report concerns and seek assistance in exercising privacy protections.

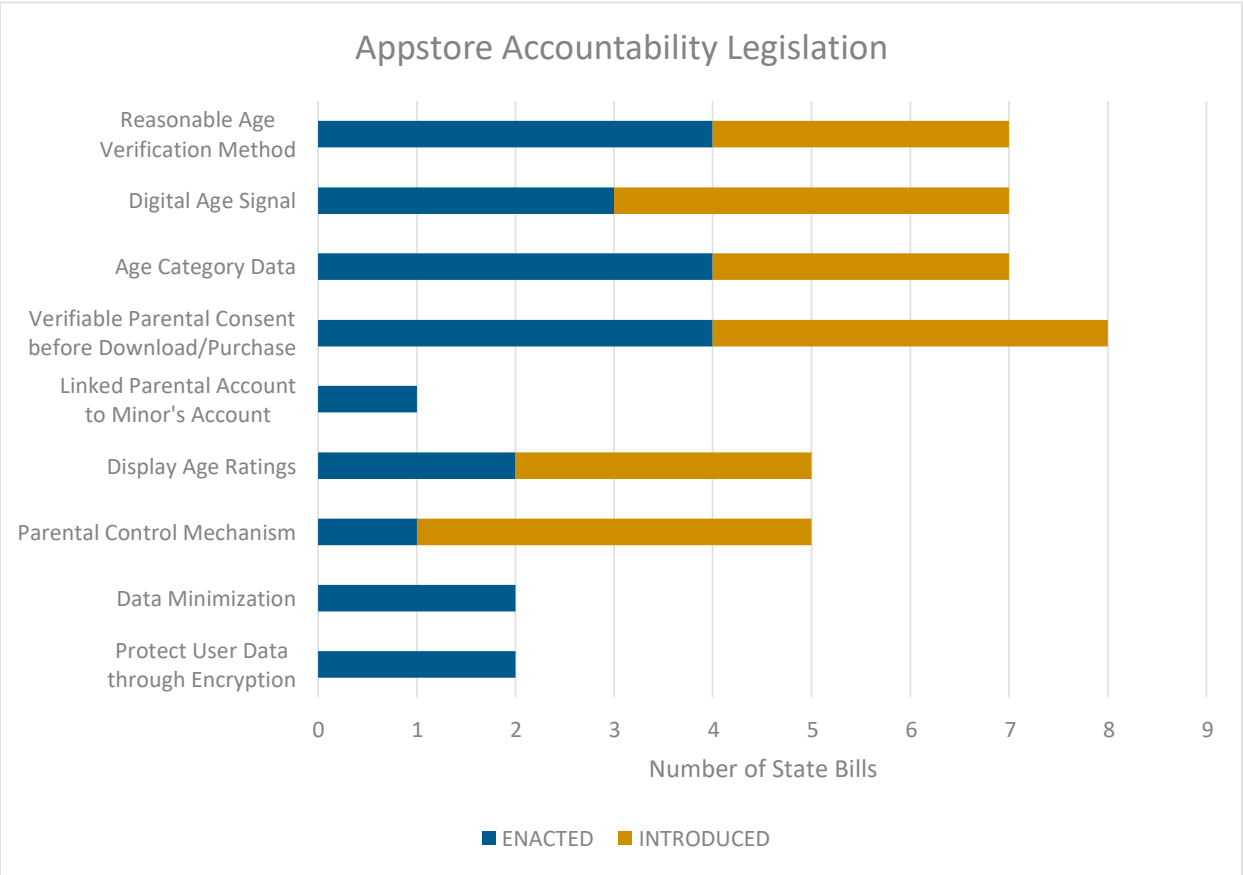
- **Parental Control/Monitoring Mechanism**: The Act authorizes parental/guardian monitoring or location tracking of a child and prohibits monitoring by others without notifying both the child and the parent or guardian. Parental monitoring may be permitted without on-screen signal as provided in the statute.

- **Monitoring or Tracking Signals**: Covered entities must provide an obvious signal when a child's precise geolocation is collected, regulate signals related to monitoring or tracking, and permit parental monitoring without a signal, as provided in the statute.

IV. App Store Accountability Acts

States are increasingly adopting App Store Accountability Acts (ASAAs), which require app marketplaces and developers to use digital age-assurance signals, require verifiable parental consent for each download or purchase by a child, and provide parental control features that allow parents to authorize, monitor, and limit app access. As of January 2026, Louisiana, Texas, Utah, and California have enacted such laws, and several other states have introduced similar measures.

California's Digital Age Assurance Act (DAAA) also imposes age-verification obligations but differs materially from the ASAAs by expanding its scope to include "operating system providers," defined as a person or entity that develops, licenses, or controls the operating system software on a computer, mobile device, or any other connected device.



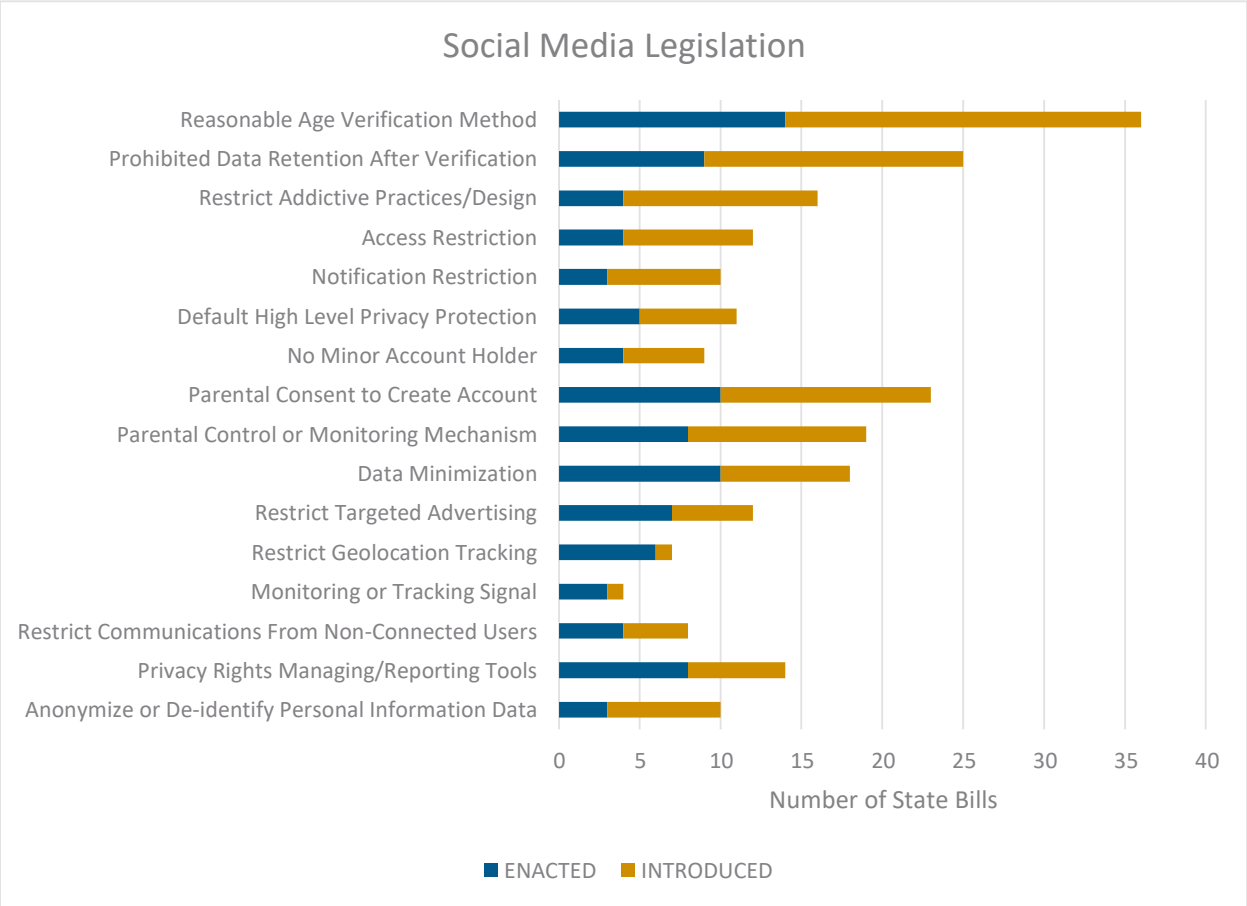
Texas's SB 2420 reflects many of the requirements commonly found in app store accountability legislation:

- **Reasonable Age Verification Method**: App stores must use a commercially reasonable method to verify each user's age category when an account is created.
- **Digital Age Signal**: App stores must make available to developers current information showing the age category assigned to each user and whether parental consent has been obtained. Developers must use this information to enforce age-based restrictions.
- **Age Category Data**: SB 2420 defines four age categories: child, younger teenager, older teenager, and adult; and requires app stores to assign each user to one of these categories.
- **Verifiable Parental Consent for Downloads and Purchases**: SB 2420 requires affirmative parental consent, obtained through a verified parent account, for each individual app download, app purchase, and in-app purchase by a minor. Blanket or ongoing consent is prohibited, and revocations must be communicated to developers.
- **Linked Parental and Minor Accounts**: A minor's account must be affiliated with a verified parent account, and a single parent account may be linked to multiple minors' accounts.
- Display of Age Ratings: App stores must display clear age ratings and content notices for every app. If the store lacks its own rating system, it must display the developer-assigned rating and the specific content that informed that rating.
- Parental Control Mechanisms: While SB 2420 does not include a standalone parental control mechanism requirement, such provisions typically require clear and accessible mechanism for parents or guardians to set filters that block harmful content or impose usage limits, including daily limits and restrictions during school or evening hours.
- Data Minimization Requirements: SB 2420 limits the collection and processing of personal information to what is necessary to verify age, obtain consent, and maintain compliance records, and it requires developers to delete data received from the app store after completing verification.
- Data Security Requirements: Personal information must be transmitted using industry-standard encryption protocols to ensure data integrity and confidentiality.

V. Social Media Legislation

Several states have enacted or introduced laws aimed at restricting minors' ability to create social media accounts, regulating the use of targeted advertising, and governing the collection, use and sale of children's personal information. Some states have gone further by prohibiting minors under the age of 13 from creating social media accounts altogether, while others require parental or guardian consent for account creation by minors over 13 until they reach age 18. These laws generally require social media platforms to perform age verification.

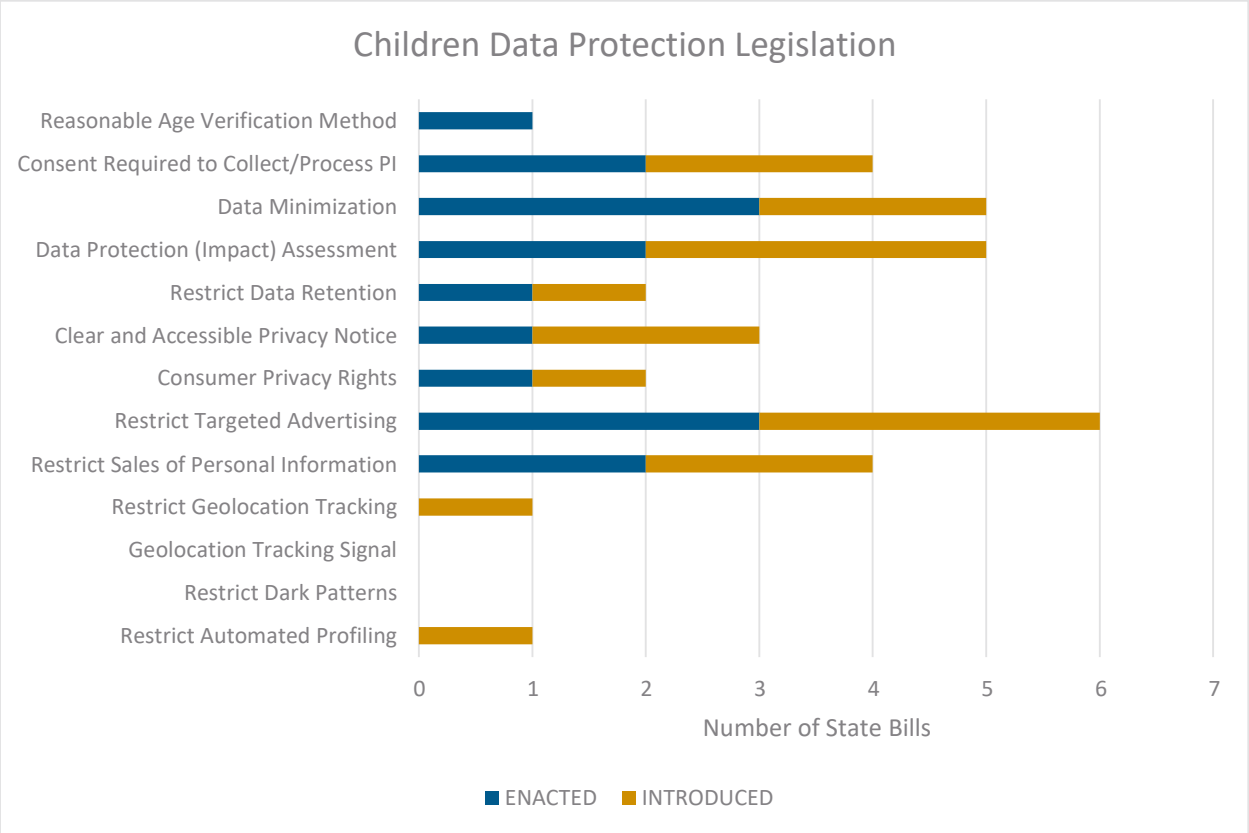
To date, 16 states have passed such legislation. However, many of these laws have faced legal challenges, including Florida's Online Protection for Minors Act, the enforcement of which is currently paused. With the Supreme Court's June 2025 decision upholding age-based access limits, there is an increased possibility that laws requiring social media platforms to implement age verification measures may withstand judicial scrutiny.



VI. Children's Data Protection Legislation

These state laws aim at providing heightened protections for children's personal information beyond the requirements of COPPA. These laws aim to give parents and children additional tools to manage their privacy settings while ensuring that children's personal information is safeguarded against sales, collection, and targeted advertising.

Although COPPA applies nationwide, 15 states have enacted their own children's data protection regulations, several of which impose stricter requirements than federal law.



Montana's Consumer Data Privacy Act (MCDPA) reflects many of the requirements commonly found in children's data protection legislation:

- **Data Security Requirements**: Personal information must be transmitted using industry-standard encryption protocols to ensure data integrity and confidentiality.

- **No Mandatory Age Verification Method**: The MCDPA does not require the implementation of an age-verification method. Instead, it regulates processing involving youths by requiring consent for targeted advertising or sale of personal information when the controller has actual knowledge that the consumer is at least 13 but younger than 16. Parental consent for a known child is tied to COPPA compliance.

- **Consent Requirements for Collecting and Processing**: The MCDPA generally operates on an opt-out model for most processing and sales. It requires consent to process sensitive data and requires consent to sell personal information or process it for targeted advertising when the controller has actual knowledge that the consumer is at least 13 but younger than 16. Verifiable parental consent for a known child is satisfied through COPPA compliance.

- **Data Minimization Obligations**: Controllers must limit collection to personal information that is adequate, relevant, and reasonably necessary for disclosed purposes, and may not process for incompatible purposes without consent.

- **Data Protection Assessment**: Controllers must conduct and document a data protection assessment for processing activities that present a heightened risk of harm, including targeted advertising, the sale of personal information, profiling with specified risks, or processing of sensitive data, and make assessments available to the attorney general upon request.

- **Data Retention Rules**: The MCDPA does not impose explicit data retention limits. It permits retaining minimal data to honor deletion requests, requires cessation of processing within 45 days after consent revocation, and otherwise sets no storage-duration rules.

- **Clear and Accessible Privacy Notices**: Controllers must provide a reasonably accessible, clear, and meaningful privacy notice describing categories of personal information processed, purposes of processing, categories of personal information shared and third parties involved, contact information, and instructions for exercising and appealing consumer rights. Secure and reliable request submission methods must be offered.

- **Consumer Privacy Rights**: Consumers, including children, have rights to confirm and access processing, correct inaccuracies, delete personal information, obtain a portable copy, and opt out of targeted advertising, the sale of personal information, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. Controllers must respond within 45 days, provide an appeal process, and recognize authorized agents for opt outs.

- **Restrictions on Targeted Advertising**: Controllers must allow consumers to opt out of targeted advertising and must obtain consent before processing for targeted advertising when the controller has actual knowledge that the consumer is at least 13 but younger than 16. Controllers engaged in targeted advertising must clearly disclose the practice and the opt-out method.

- **Restrictions on the Sale of Personal Information**: Controllers must allow consumers to opt out of the sale of personal information and must obtain consent before selling the personal information of consumers at least 13 but younger than 16, when actually known.

- **Restrictions on Geolocation Tracking**: Precise geolocation data is "sensitive data," and processing such data requires consumer consent or, for a known child, COPPA-compliant processing.

- **Geolocation Tracking Signal Requirement**: The MCDPA does not require a tracking signal. Instead, it classifies precise geolocation data as sensitive and requires consent for its processing or COPPA-compliant processing for a known child.

- **Restrictions on Dark Patterns**: Consent obtained through dark patterns is invalid.

- **Restrictions on Automated Profiling**: Consumers may opt out of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. Controllers must conduct DPIAs for profiling that presents specified risks.

- **Age Verification Signals**: The MCDPA does not require an age-verification signal. It does, however, require recognition of an opt-out preference signal for targeted advertising and sales.

VII. Federal Children's Privacy Legislation

At the federal level, several proposals introduced this session would significantly expand children's and teen's online privacy and safety obligations.

- The Children and Teen's Online Privacy Protection Act ("COPPA 2.0") would extend COPPA protections to minors under 17, ban targeted advertising to children and teens, require an "eraser button" to delete minors' data, and establish an FTC Youth Marketing & Privacy Division.

- The Kids Online Safety Act ("KOSA") would mandate default to the most privacy protective settings and require robust parental tools and reporting mechanisms.

- The App Store Accountability Act would shift child-safety gating obligations to app stores by requiring age verification at account creation, parental consent for minors to use stores, download apps, or make in-app purchases, and developer obligations to check age/consent signals.

- The Shielding Children's Retinas from Egregious Exposure on the Net Act ("SCREEN Act") is designed as a broad-age gating mandate, rather than platform-specific design rules, and would require certain interactive computer services to deploy technology-based age verification to keep minors from accessing content harmful to minors, with data-security obligations for verification information.

- Finally, the Safeguarding Adolescents From Exploitative BOTs Act ("SAFE BOTs Act") would target consumer chatbots used by minors by mandating clear AI identity disclosures, crisis-resource notices when prompted about self-harm, prohibiting claims of being a licensed professional, requiring "take a break" nudges after extended sessions, and policies addressing sexual content, gambling, and drugs and alcohol. The FTC and state AGs would share enforcement, with express preemption of any overlapping state requirements.

VIII. Federal Enforcement Priorities

Children's online privacy remains a significant enforcement priority for the FTC. During a virtual IAPP meeting, January 21, 2026, FTC Division of Privacy and Identity Protection Associate Director Ben Wiseman stated that a key focus for the agency this year will be enforcing the updated COPPA Rule. Wiseman also underscored the FTC's focus on enforcing the recently enacted TAKE IT DOWN Act. Effective May 2026, the TAKE IT DOWN Act imposes a 48-hour removal obligation for reported nonconsensual intimate imagery on covered platforms, enforceable by the FTC.

Conclusion

With renewed focus on strengthening children's privacy laws, businesses may need to consider reassessing and updating their operational processes, particularly in light of the recent COPPA amendments and the FTC's stated enforcement priorities. The Supreme Court's ruling enabling states to adopt more robust age-based access limits further underscores the need for businesses offering content that may be unsuitable for minors to evaluate and potentially update their online products accordingly.

Additionally, as states continue to implement these new children's privacy laws, enforcement authority is increasingly being vested in state attorneys general, who may impose civil penalties ranging from $5,000 to $50,000 per violation. Consequently, businesses subject to these new children's privacy laws, including social media companies, online platform providers, and other businesses offering online products and services reasonably likely to be accessed by children, should consider establishing appropriate compliance processes, including reasonable age verification measures and mechanisms for obtaining parental consent, to help mitigate enforcement risk. Failure to do so could result in significant operational and financial consequences.

CONTACTS

For more information about the topics raised in this Legal Update, please contact any of the following lawyers:

PARTNER
AMBER THOMSON
WASHINGTON DC +1 202 263 3456
ATHOMSON@MAYERBROWN.COM

PARTNER
HOWARD WALTZMAN
WASHINGTON DC +1 202 263 3848
HWALTZMAN@MAYERBROWN.COM

PARTNER
MEGAN VON KLEIN
CHICAGO +1 312 701 8089
MVONKLEIN@MAYERBROWN.COM

PARTNER
EVAN HAN
PALTO ALTO +1 650 331 2009
EHAN@MAYERBROWN.COM

PARTNER
DARA GARCIA
LOS ANGELES +1 213 229 5196
DEGARCIA@MAYERBROWN.COM