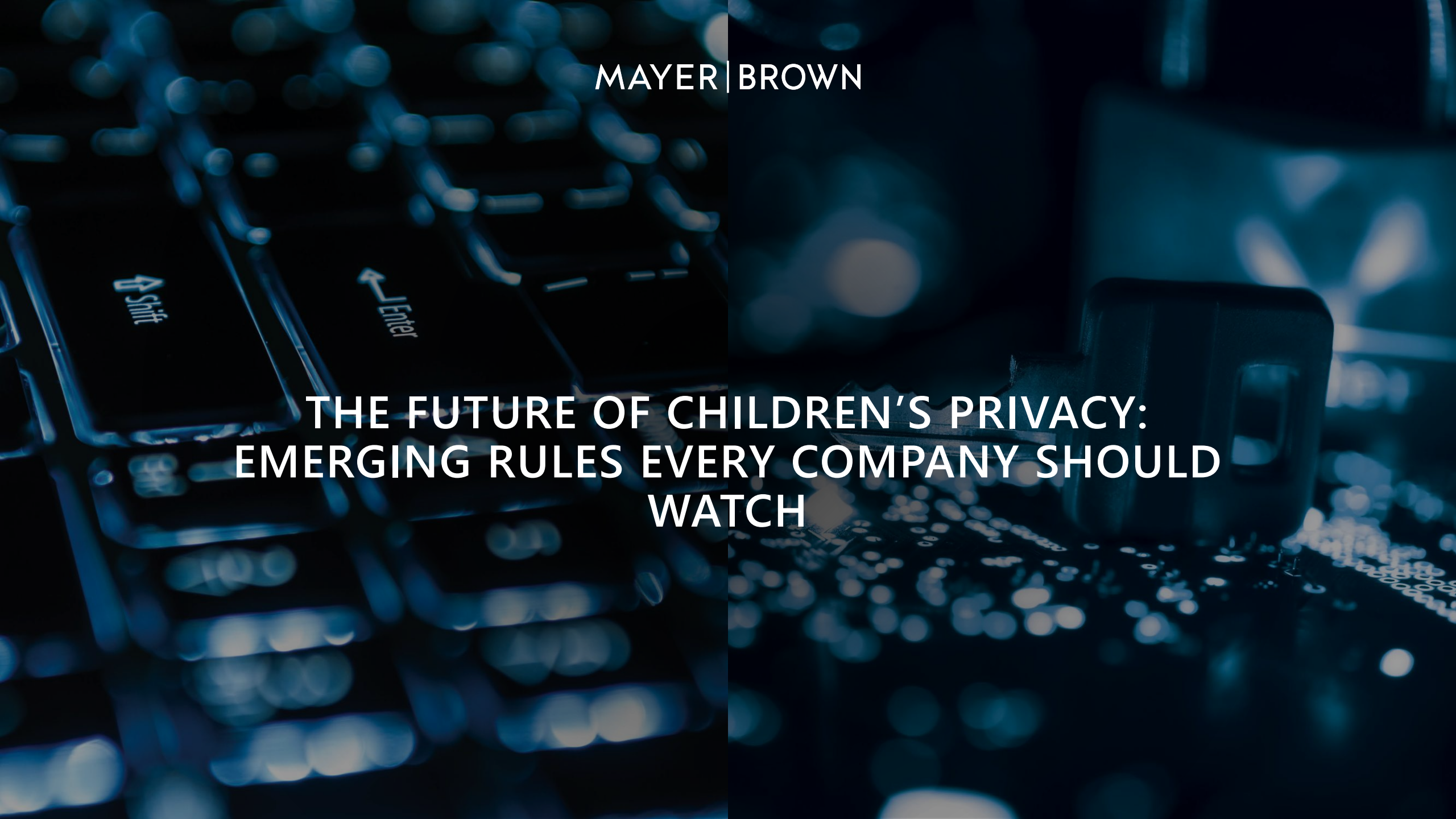


THE FUTURE OF CHILDREN'S PRIVACY: EMERGING RULES EVERY COMPANY SHOULD WATCH

TODAY'S PRESENTERS

PARTNER
CYBERSECURITY & DATA PRIVACY

AMBER THOMSON

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

ASSOCIATE
CYBERSECURITY & DATA PRIVACY

MEGAN VON KLEIN

CHICAGO +1 312 701 8089
MVONBORSTEL@MAYERBROWN.COM

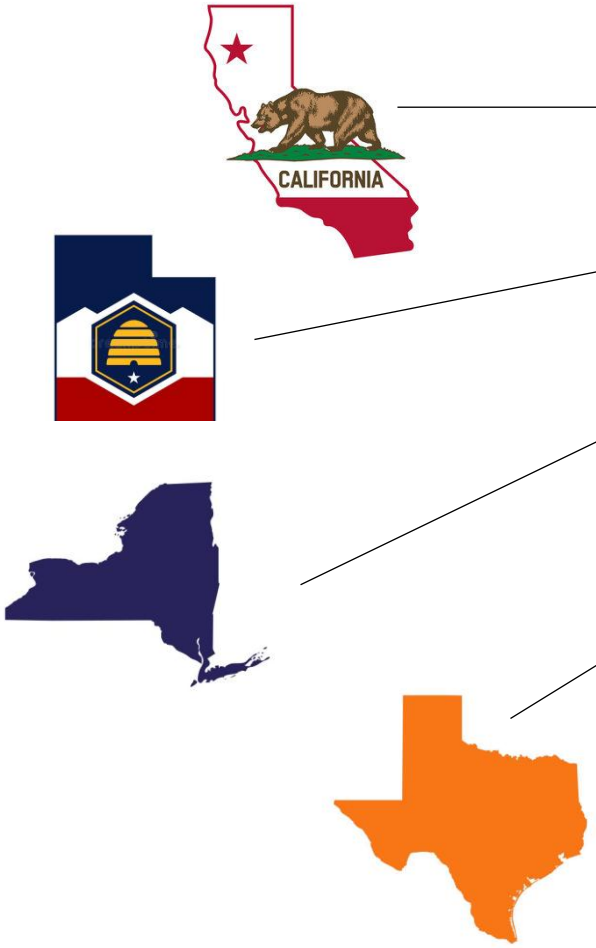
AGENDA

1. The Patchwork Problem
2. Why Youth Online Safety Laws Are Reshaping Compliance
3. Children's Privacy Provisions in State Comprehensive Privacy Laws
4. Age-Appropriate Design Codes
5. State AG Enforcement and Litigation
6. Roadmap for 2026
7. Q&A

01

THE PATCHWORK PROBLEM

THE PATCHWORK PROBLEM



Age Estimation

Parental Consent

Algorithmic Feed Restrictions

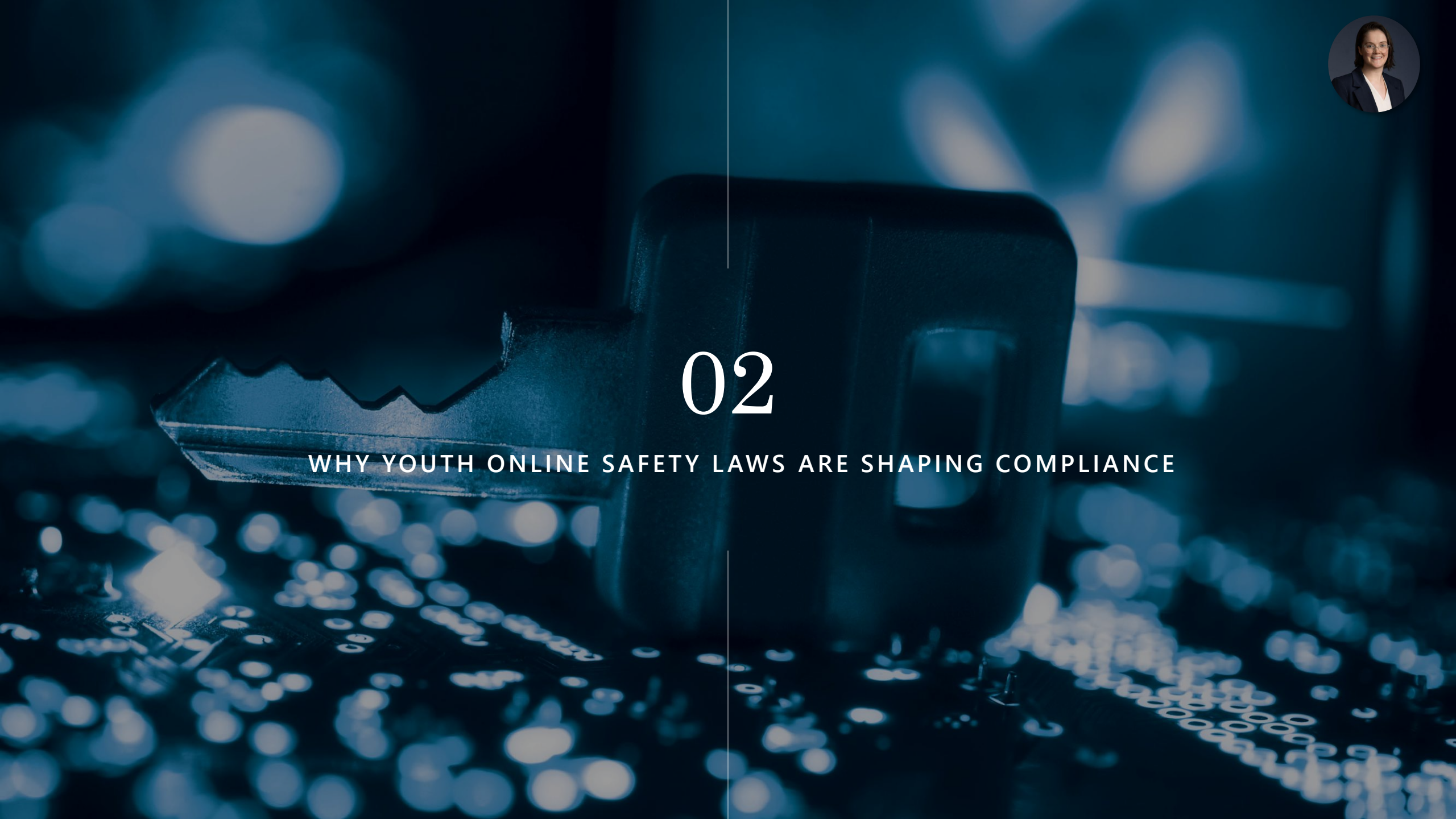
Age Verification

A single feature.
Four different compliance regimes.

- A national platform prepares to launch a new **teen-focused feature**.
- Each state imposes a different requirement, from **age estimation** to **parental consent** to **algorithmic feed restrictions**.
- One product becomes **four versions**, each with its own rules, workflows, and litigation exposure.
- **Operational Impact** = slower launches, inconsistent user experiences, higher costs, litigation and enforcement exposure.

FEDERAL LEGISLATIVE LANDSCAPE

- **COPPA 2.0 (Children and Teens' Online Privacy Protection Act):**
  - Extends COPPA protections to minors under 17.
  - Bans targeted/"individual-specific" ads to children and teens.
  - Requires an "eraser button" to delete minors' data.
  - Creates an FTC Youth Marketing & Privacy Division.
- **Kids Online Safety Act (KOSA):**
  - Imposes a platform "duty of care" to prevent and mitigate specified harms to minors, defaults to the most protective settings, and robust parental tools and reporting mechanisms.
  - Mandates transparency (including audited risk reports for large content platforms).
  - FTC and state AGs share enforcement.
- **App Store Accountability Act:**
  - Shifts child-safety gating to app stores by requiring age verification at account creation, parental consent for minors to use stores/download apps/make in-app purchases, standardized age ratings and content descriptors, and developer obligations to check age/consent signals.
  - FTC enforcement and federal preemption are contemplated in current versions. Watch for First Amendment and privacy challenges and implementation costs.
- **SCREEN Act:**
  - Requires 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 and FTC audits/enforcement.
  - Designed as a broad age-gating mandate rather than platform-specific design rules.
- **SAFE BOTs Act (Safeguarding Adolescents From Exploitative BOTs Act):**
  - Targets 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/alcohol.
  - FTC and state AGs enforce, with express preemption of overlapping state requirements.



02

WHY YOUTH ONLINE SAFETY LAWS ARE SHAPING COMPLIANCE

WHY STATES ARE ACTING NOW

- **Protecting children's well-being.** Legislatures are responding to heightened concerns about youth mental health and online harms by advancing youth online safety frameworks, including age assurance verification and restrictions on social media use.
- **Regulatory momentum.** Active state AG enforcement priorities and a rapidly evolving litigation landscape are accelerating state action and reshaping compliance expectations.
- **Filling federal gaps with design-led standards.** Perceived limitations of COPPA's scope are prompting states to adopt age-appropriate design codes and privacy provisions to address teen data and platform design risks beyond traditional notice and consent models.

UNDERSTANDING THE LANDSCAPE

- **Age Assurance/Verification Regimes**
  - Content-specific age-gating (e.g., “You must be 21 to continue”)
  - Platform-level/user-level age checks for social media and app platforms (e.g., age estimation or verification via biometrics or ID)
- **Social Media Access Restrictions**
  - Laws range from outright bans for children under a set age to parental mandates for teens, default time limits, and restrictions on “addictive” features.
- **First Amendment Challenges**
  - Many social media laws face First Amendment challenges.
  - Some are permanently enjoined. Others are pending litigation or appeal.

SOCIAL MEDIA AND PARENTAL CONSENT RELATED PLATFORM LAWS

Currently effective state social media laws:

- **California SB 976 (Protecting Our Kids from Social Media Addiction Act):** Addictive feed parental-consent requirement and default "private mode" for minors are currently enforceable.
- **Florida HB 3:** Age restrictions and parental consent framework took effect Jan. 1, 2025; law remains in effect pending final resolution.
- **Tennessee HB 1891 (Protecting Children from Social Media Act):** Effective Jan. 1, 2025, preliminary injunction was denied, leaving parental consent, age-verification, and parental supervision requirements operative.
- **Texas HB 18 (Scope Act):** In effect with partial injunction; courts enjoined "harm prevention," parental-tool and algorithmic explanation provisions but other requirements, including age-assurance and minors' protections are still effective.
- **Virginia SB 854:** Effective Jan. 1, 2026, limits minors under 16 to default one-hour/day on social media without verifiable parental consent. Subject to ongoing litigation but not enjoined.
- **Mississippi Walker Montgomery Protecting Children Online Act:** Effective July 2025, requires age verification, parental consent, and data minimization. A federal judicial panel allowed the law to take effect in July 2025, with the Supreme Court declining to halt it, meaning it's currently active while litigation continues.

SOCIAL MEDIA AND PARENTAL CONSENT RELATED PLATFORM LAWS (CONT.)

Enacted but not yet effective:

- **Arkansas SB 611:** Effective April 21, 2026, requires age verification, disabling late-night notifications, and adding parental rights.
- **Nebraska Parental Rights in Social Media Act:** Requires age verification and parental consent for anyone under 18 to open accounts; grants parents monitoring and control rights; takes effect July 1, 2026.
- **New York SAFE For Kids Act:** Not yet in effect; requires AG to finalize rules first. Proposed rules were issued Sept. 15, 2025. Law takes effect 180 days after final rules are published.

- Temporarily or permanently enjoined:
  - **Ohio's Parental Notification by Social Media Operators Act:** Permanently enjoined by federal court in April 2025 (First Amendment and vagueness grounds).
  - **Georgia's "Protecting Georgia's Children on Social Media Act of 2024" (SB 351):** Temporarily enjoined by federal court in July 2025 (First Amendment grounds).
  - **Utah's Minor Protection in Social Media Act (SB 194/HB 464):** Temporarily enjoined by federal court (First Amendment grounds); federal appeals court heard appeals in late 2025.
  - **Louisiana's Secure Online Child Interaction and Age Limitation Act:** Currently enjoined by federal court (First Amendment grounds); Louisiana's AG intends to appeal the decision to the Fifth Circuit.

AGE ASSURANCE AND VERIFICATION LAWS

- **Adult content age verification**
  - Following Supreme Court's June 2025 ruling upholding HB 1181, more than 20 states have enacted or advanced age checks for sites with sexually explicit material harmful to minors.
- **Device-level filters**
  - States, such as **Alabama** and **Utah** require companies that offer online products and services on internet-enabled devices used by minors to enable default content filters at setup and provide password-controlled management.
- **Platform-level age checks**
  - Social media, apps, OS-level controls; user-level age estimation or verification

UNPACKING AGE ASSURANCE: TECHNOLOGIES AND TRADEOFFS

FUTURE OF PRIVACY FORUM

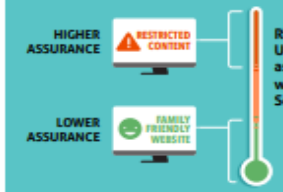
Age Assurance is the broadest term for methods to discern the age or age range of an individual. There is no one-size-fits-all method, and it is important to consider context to determine a proportionate method of age assurance for each specific use case. Proportionality is key because in some contexts, a higher level of certainty is appropriate. This must be carefully balanced against the privacy risks and risk of barring access to legitimate content - especially if content restrictions have inequitable impacts. It may be appropriate to employ multiple methods in a layered approach.

AGE ASSURANCE QUESTIONS

WHAT ARE THE GOALS?
- Facilitate parental consent
- Limit access to an age-restricted service or provide age-appropriate content
- Verify an individual's exact age
- Place individuals within an age band (e.g. 13-15)

WHAT ARE THE POTENTIAL HARMS TO MINORS?
Harms could include children or teens accessing age-restricted services, content, or contact by unknown individuals.

WHAT IS THE APPROPRIATE ASSURANCE METHOD?
Choose a method or methods that provides a level of age assurance (accuracy) proportional to the goals and risks of the service, keeping in mind that legal obligations may dictate a specific method.



IS ASSURANCE BALANCED WITH PRIVACY RISKS?
After considering privacy risks and mitigations, confirm that the assurance goal warrants the level of privacy risks and other impacts associated with the chosen age assurance method.

COMMON EXISTING & EMERGING METHODS

DECLARATION

AGE GATE

A user indicates their birthdate without providing supporting evidence. This common method is most appropriate in low risk situations, as children and teens frequently bypass by providing a false birthdate. Privacy risk is low, especially if birthdates are not retained or matched with a name or other indirect identifier.

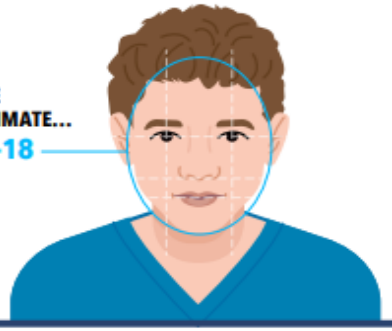
PARENTAL CONSENT/VOUCHING

A parent with a verified account (e.g. using government ID, credit card, etc.), declares the child or teen's age by providing consent or adding the child to their account. This has higher assurance than an age gate, but may impact the teen's autonomy.

ESTIMATION

FACIAL CHARACTERIZATION

Estimates age using a facial image, but the individual is not uniquely identified. Best used to place users in age bands, or signal that a user meets an age threshold, such as under 13 or 21+. Estimation is less effective for discerning age in a narrow range like 17 vs 18.



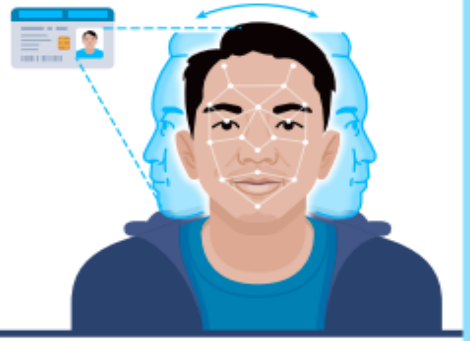
OTHER ALGORITHMIC ESTIMATION METHODS

Other algorithmic methods could include estimation of age or age range based on browsing history, voice, gait, or using multiple data points or signals from a VR game.

VERIFICATION

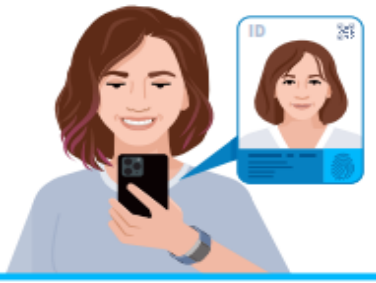
BIOMETRIC + GOVERNMENT ID

Matches a scan of a government-issued ID and live photo or video using facial recognition. This method is more appropriate for higher risk, regulated or age restricted services. Government ID only is another method, but provides less assurance.

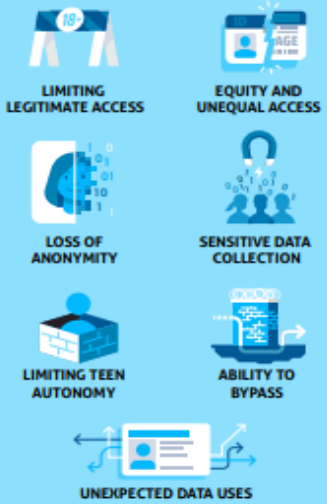


ON DEVICE DIGITAL ID/WALLET

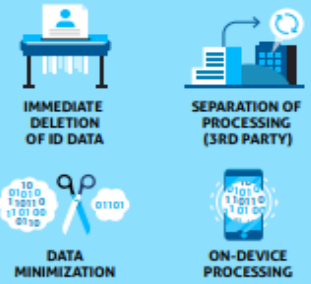
Using a wallet app, users add one or more verified credentials to create a reusable digital ID stored either on device or in the Cloud. Users verify their age with the service by inputting a code to share details required for age assurance (e.g. 18 or over).



RISKS OF AGE ASSURANCE



RISK MANAGEMENT TOOLS



EXAMPLE USE CASE

AGE ASSURANCE FOR ONLINE GAMING

In this scenario, Miles, a 16 year old, is accessing an online gaming service that is designed for teens and older. It has optional age-restricted features.

INITIAL EXPERIENCE

DECLARATION

The default user experience is "teen-friendly." Miles can sign up by providing their birthdate.

ASSURANCE
PRIVACY RISK

SECONDARY FEATURE

ESTIMATION

Later, Miles wants to enable a feature which the game developer has restricted to 16+. The developer wants a higher level of assurance. A "live selfie" uses facial characterization to determine Miles is between 14-18.

ASSURANCE
PRIVACY RISK

GREATER ASSURANCE NEEDED

VERIFICATION

Because the estimated age range includes ages that aren't allowed to use the feature (14-15), greater age assurance is needed. Miles must scan their driver's license and take a "live selfie." However, many users, including 75% of 16 year olds, do not have a driver's license.

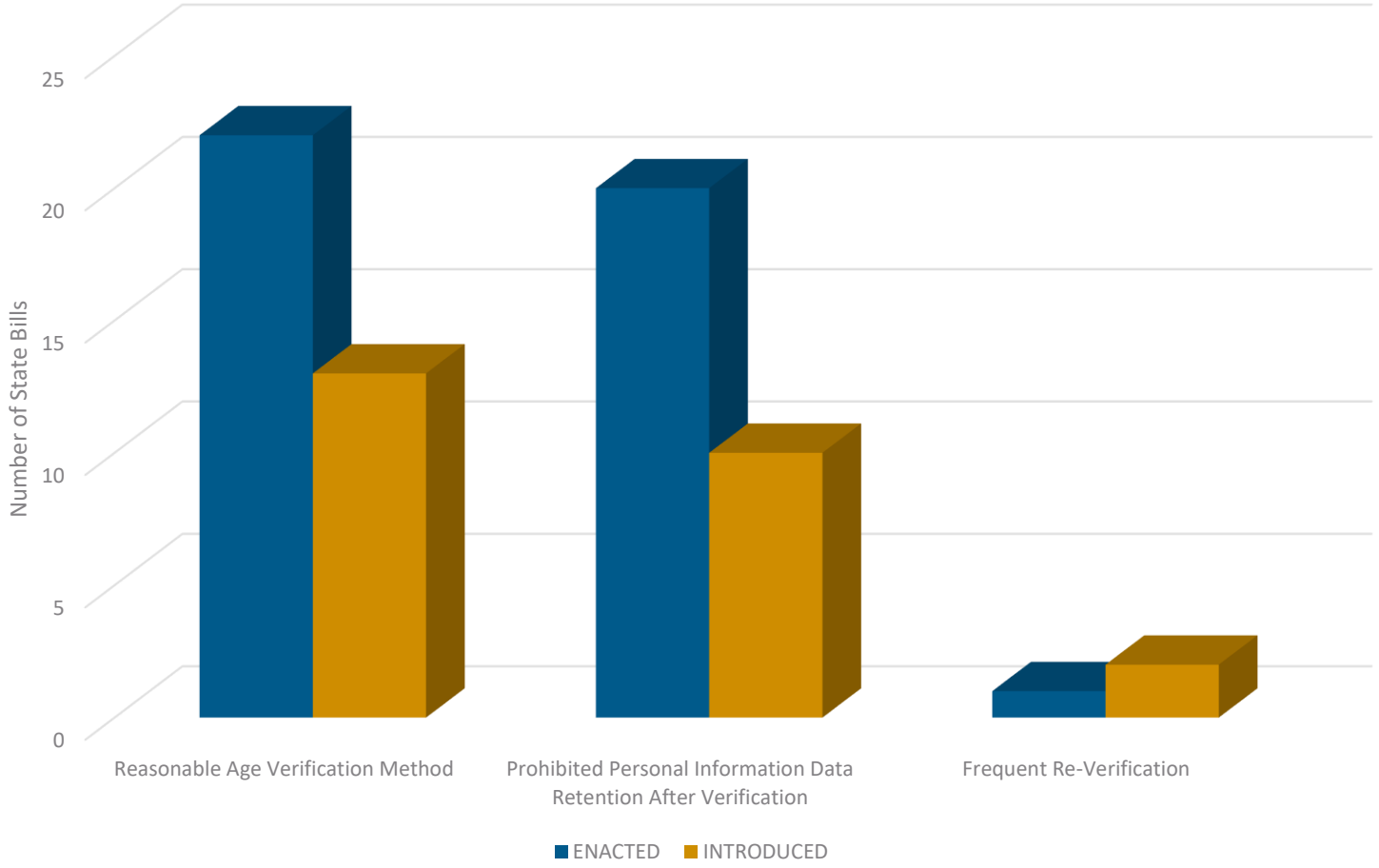
ASSURANCE
PRIVACY RISK

Source: Future of Privacy Forum, https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf

AGE VERIFICATION PRODUCT WORKFLOW: ROBLOX

Age Assurance and Verification Laws

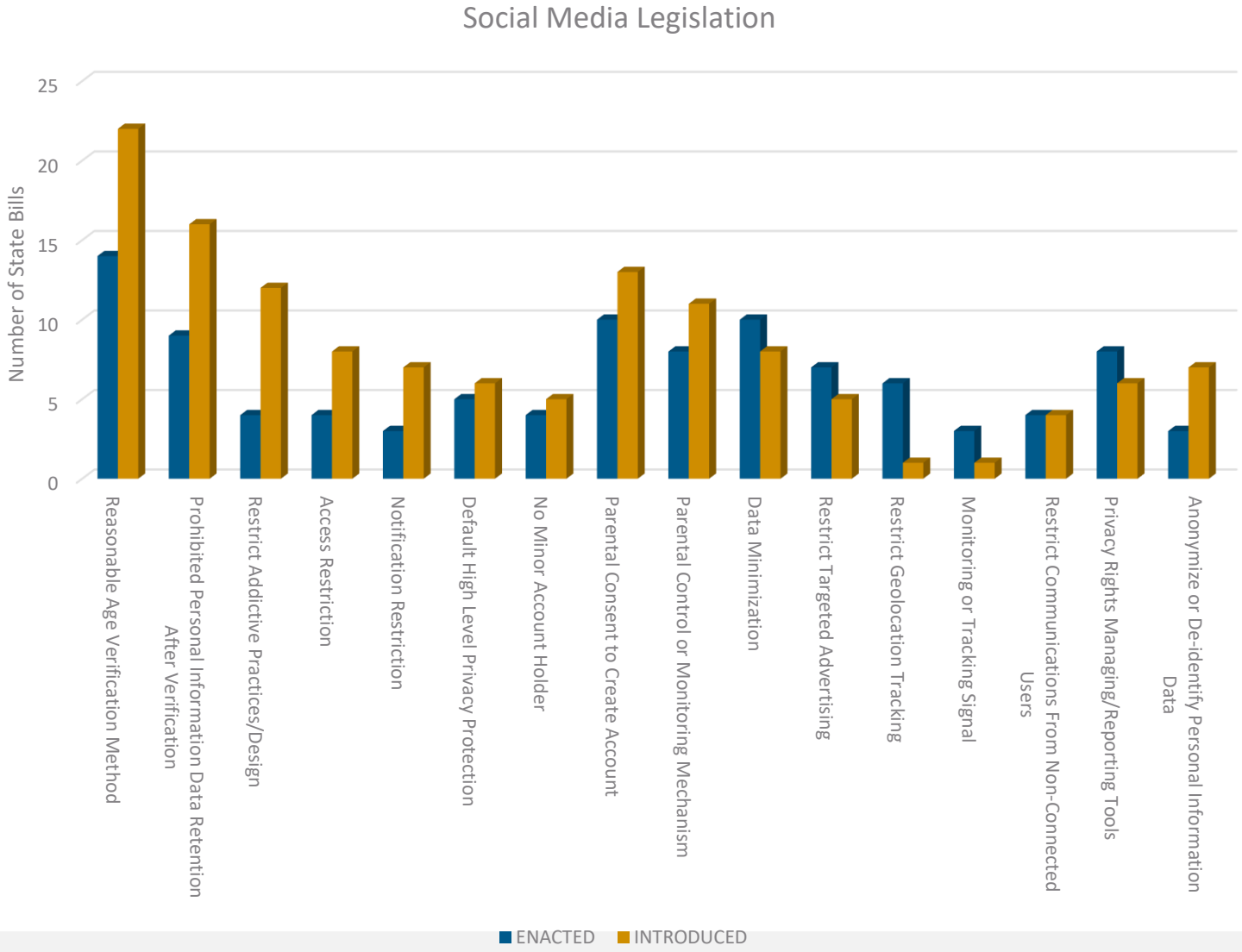
Harmful Content - Age Verification Legislation



LAWS BANNING OR RESTRICTING SOCIAL MEDIA USE FOR CHILDREN UNDER 16

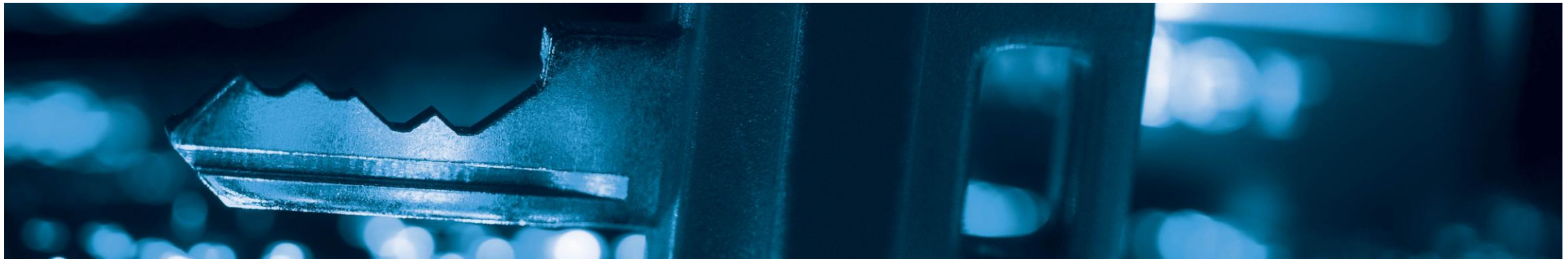
- **Parental consent or bans.**
  - Multiple states have enacted laws prohibiting minors under the age of 13 from holding social media accounts all together, while other states require verifiable parental consent for minors over 13 until they reach 18.
  - **Example:** Florida's Online Protection for Minors Act
- **Use restrictions.**
  - Some laws impose daily usage caps.
  - **Example:** Virginia's law sets a one-hour default limit for users under 16.
- "**Addictive feeds" and design restrictions.**
  - Some states' laws target algorithmic feeds unless parental consent is obtained.
  - Portions of some laws are enjoined.
  - **Examples**: New York (active) and California (enjoined).

SOCIAL MEDIA LEGISLATION



KEY TAKEAWAYS

1. Expect continued rapid state activity, including device-level filters, app store accountability, and design-focused restrictions, and ongoing litigation that may delay enforcement.
2. Consider developing modular, jurisdiction-aware age assurance and parental consent workflows now to reduce enforcement risk.
3. Treat verification data as sensitive: minimize, secure, and delete promptly.



03

CHILDREN'S PRIVACY PROVISIONS IN COMPREHENSIVE STATE PRIVACY LAWS

DETERMINING APPLICABILITY: DO THESE LAWS APPLY TO MY BUSINESS?

Does the business meet applicability thresholds?

- Revenue
- Data Volume
- Percentage of Revenue Derived from Selling/Sharing Data
- Sector Carve-Out

Does the business process children's or teens' data?

- Directly or through vendors?
- "Known child" triggers

Does the business engage in high-risk processing?

- Targeted advertising
- Profiling
- Data sales
- Sensitive data processing

WHEN TEEN PROCESSING REQUIRES CONSENT: ACTUAL KNOWLEDGE VS. WILLFUL DISREGARD

You **know** the user is age 13–16 because they told you or you collected DOB.

Examples:

- User enters their birthdate during account creation.
- Parent contacts customer support to update a child's age.
- You verify age for another purpose (e.g., eligibility).

You **should reasonably know** the user is a teen based on available information.

Examples:

- You collect school enrollment information indicating middle/high school status.
- User profile shows grade level or student ID.
- Marketing campaigns target teen audiences.
- You ignore age signals in your own analytics.

CORE OBLIGATIONS AFFECTING YOUTH DATA

- **Sensitive personal data categorization**
  - Stricter processing limitations
  - Opt-in consent
  - DPIA requirements
- **Risk assessment obligations**
  - Processing sensitive children's or teens' data
  - Conducting targeted advertising
  - Engaging in profiling with significant effects
  - Selling minors' personal data
  - Using high-risk technologies (AI, biometrics, geolocation)
- **Dark patterns and youth interfaces**
  - Nudging minors to share more data
  - Making it harder to decline tracking
  - Obscuring parental controls
  - Designing consent flows that favor "yes" over "no"
- **Opt-in consent requirements**
- **Parental consent requirements**

TOP 3 MISTAKES COMPANIES MAKE WHEN COLLECTING AND/OR PROCESSING CHILDREN'S/TEENS' DATA

- **Mistake #1: Assuming You Don't Have Minors in Your Data**
  - Relying solely on self-declared age
  - Ignoring signals that indicate teen status (school email, grade level, youth-oriented content)
  - Failing to classify minors as a high-risk data category
- **Mistake #2: Using One-Size-Fits-All Consent & Notices**
  - Applying the same privacy disclosures to adults, teens, and children
  - Missing parental-consent requirements for under-13 users
  - Not providing simplified, age-appropriate notices for teens
- **Mistake #3: Treating Teen Data Like Adult Data**
  - Forgetting that many states require opt-in for targeted ads or data sales for ages 13–16
  - Overlooking teen-specific DPIA triggers
  - Allowing dark patterns or engagement-driven design that regulators flag as manipulative for minors

CHILDREN'S PROVISIONS UNDER COMPREHENSIVE STATE PRIVACY LAWS: WHAT TO REMEMBER

The Regulatory Landscape is Fragmented

- States treat minors differently: children (<13) vs. teens (13–16)
- Teen data is increasingly treated as sensitive
- Opt-in requirements vary widely across states
- Youth-specific laws (social media, age verification, design codes) add another layer

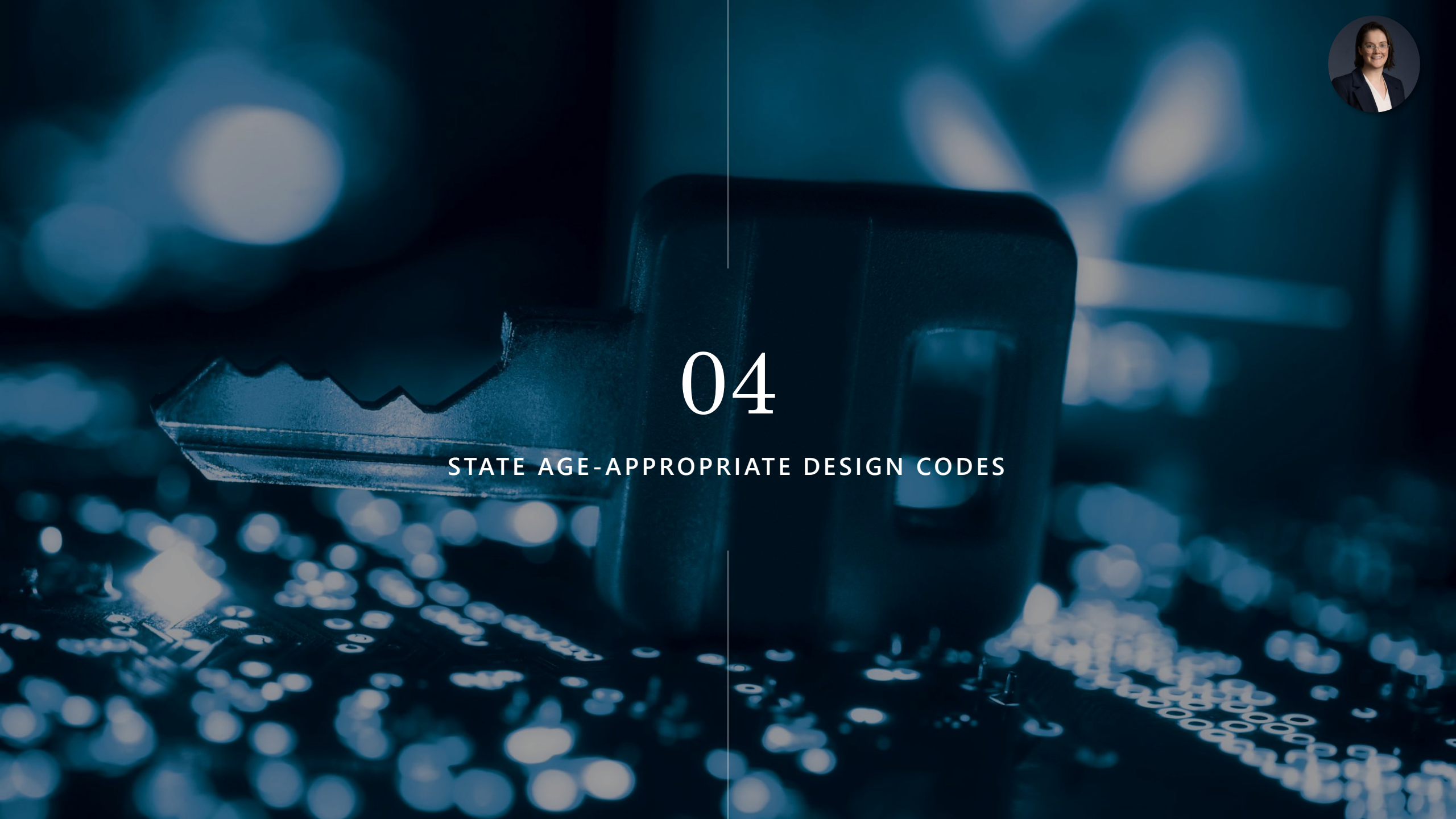
Youth Data Requires Purposeful Workflows

- Parental consent is mandatory for under-13 users
- Opt-in often required for targeted ads or data sales to teens
- DPIAs triggered by minors' data, profiling, targeted ads, or high-risk tech
- Interfaces must avoid dark patterns and support youth autonomy

Risk and Enforcement are Accelerating

- Regulators expect actual knowledge and reject "willful ignorance"
- Youth-related violations are high-priority enforcement targets
- Vendor and platform ecosystems create fourth-party risk
- Litigation and injunctions create shifting compliance timelines

Build a minor's data playbook: intake, verification where appropriate, parental consent where required, rights handling, retention.



04

STATE AGE-APPROPRIATE DESIGN CODES

AGE-APPROPRIATE DESIGN CODES, COPPA, AND YOUTH SAFETY LAWS

Scope

- **COPPA** covers operators handling personal data from children under 13.
- **Age-Appropriate Design Codes** (AADCs) extend to services "likely to be accessed" by users under 18.
- Other **youth safety laws** vary widely creating a patchwork beyond COPPA's narrow scope.

Obligations

- **COPPA** is a data-protection regime (notice, verifiable parental consent, rights, security, minimization).
- **AADCs** add product-design duties (risk/DPIAs, high-privacy defaults, age estimation, anti-dark patterns) with some CAADCA provisions enjoined pending further proceedings.
- Other **youth safety laws** vary and include both parental consent or age verification and product-design duties.

Enforcement Posture

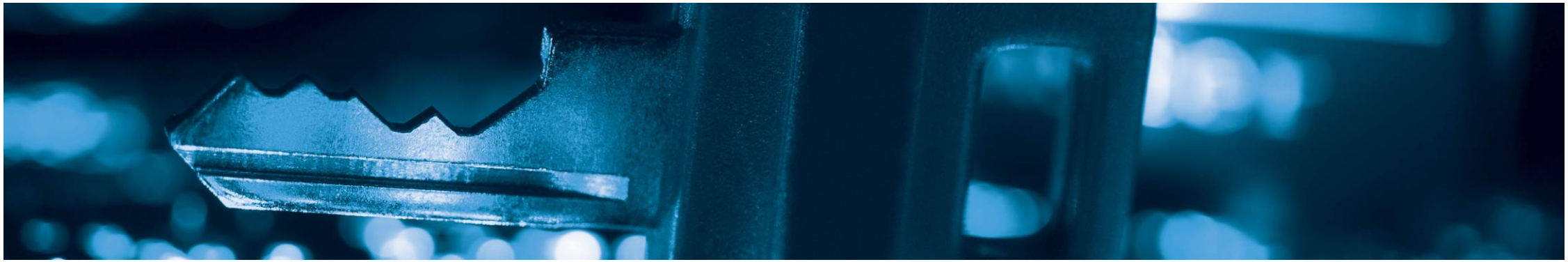
- **COPPA** is enforced by the FTC (and state AGs) and provides a relatively settled federal baseline.
- **AADCs** and other **state youth laws** face active, ongoing constitutional challenges and partial/delayed enforcement.

OVERVIEW OF ENACTED AND PENDING DESIGN CODES

- **Enacted Age-Appropriate Design Codes**
  - **California**: Signed in 2022, California's AADC is currently blocked from enforcement due to preliminary injunction issued on March 13, 2025, by a federal court.
  - **Maryland**: Effective Oct. 1, 2024, the "Kids Code" mandates that online businesses likely accessed by minors under 18 prioritize children's safety and privacy by design with DPIAs required by April 1, 2026. Pending litigation in *NetChoice v. Brown*, which has advanced to discovery phase.
  - **Nebraska**: Effective Jan. 1, 2026, the Nebraska AADCA requires provision of parents with tools to help parents protect and support minors, e.g., viewing child account settings.
  - **Vermont**: Set to take effect January 1, 2027, the Vermont AADCA requires provision of a prominent, accessible, and responsible tool to request a minor's social media account be unpublished or deleted and honor these requests within 15 days. The AG is tasked with adopting rules prohibiting dark patterns.
- **Introduced Age-Appropriate Design Codes**: South Carolina (awaiting signature as of 1/21/26), Illinois

KEY THEMES

1. Duty to design products consistent with the **best interests** of children reasonably likely to access them.
2. Develop products and services with a **privacy-by-design** approach.
3. Complete **DPIAs** focused on children's risks.
4. Limits on **profiling**, **geolocation**, and **dark patterns**.
5. Age estimation v. verification.



05

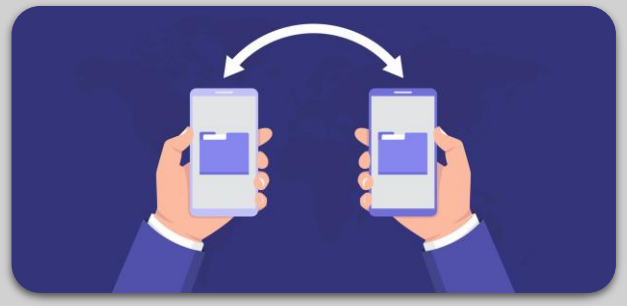
STATE AG ENFORCEMENT AND LITIGATION

ENFORCEMENT THEMES FROM STATE ATTORNEYS GENERAL

Social Media & Design Features

Focus on “addictive” or manipulative design

Scrutiny of teen engagement features and transparency failures



Third-Party Data Sharing and SDKs

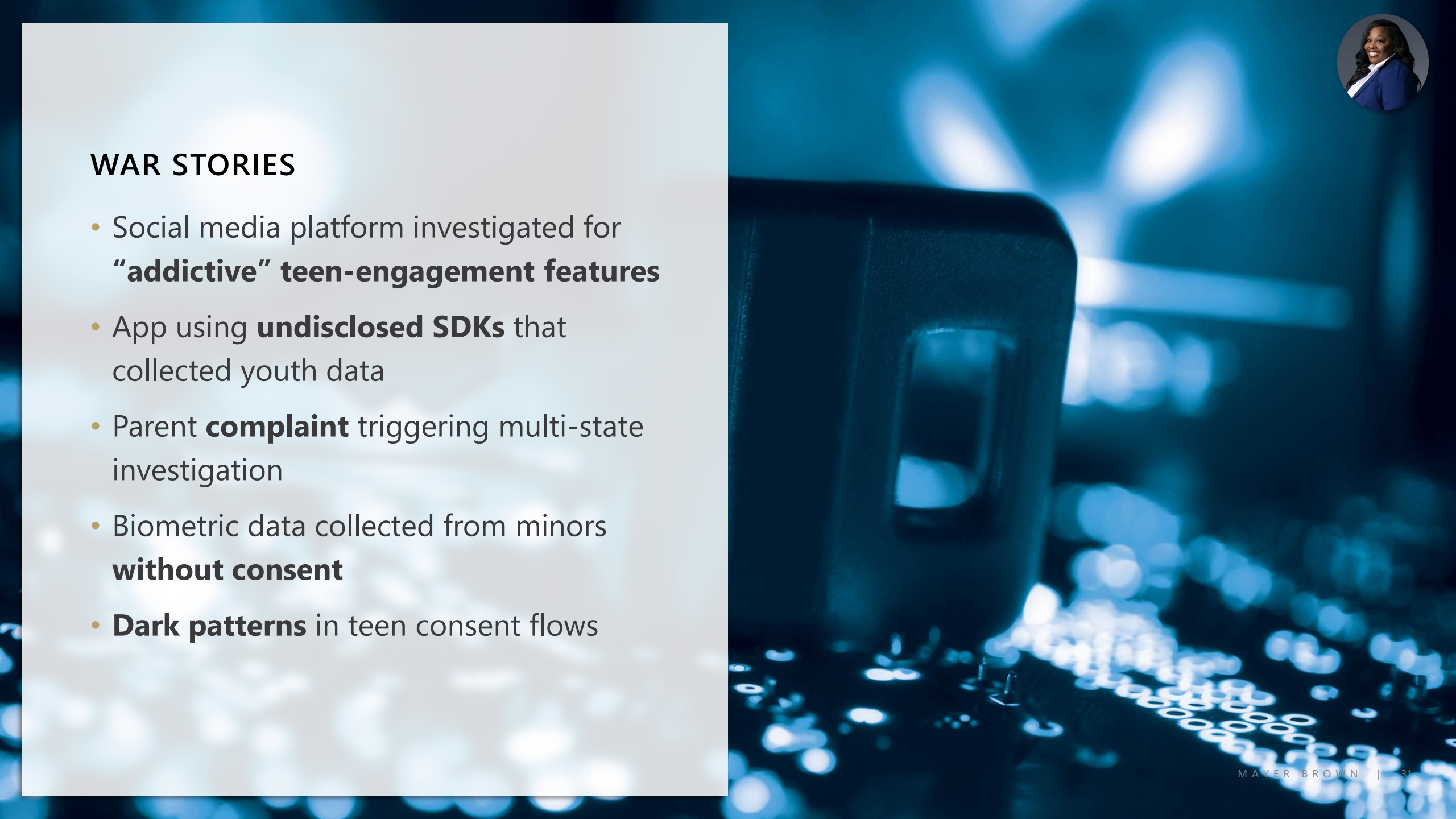
Undisclosed SDKs, pixels, and tags collecting youth data

Misrepresentations in privacy notices

Geolocation & Sensitive Data

Enforcement around precise geolocation for minors

Biometric identifiers (face, voice, fingerprints) under heightened scrutiny



WAR STORIES

- Social media platform investigated for **“addictive” teen-engagement features**
- App using **undisclosed SDKs** that collected youth data
- Parent **complaint** triggering multi-state investigation
- Biometric data collected from minors **without consent**
- **Dark patterns** in teen consent flows

MULTI-STATE AG COALITIONS

- Joint investigations led by 3–10 AG offices.
- Shared subpoenas and coordinated CID (civil investigative demand) templates.
- Cross-state working groups on youth safety, dark patterns, and geolocation.
- Increasing collaboration with federal agencies (FTC, CFPB).
- Coalitions often target:
  - Social media platforms
  - EdTech providers
  - Location-based services
  - Apps with youth-heavy user bases
- State AGs increasingly file joint briefs supporting each other's youth-safety and privacy laws.

Coalition of 43 States Urges FTC To Strengthen Online Privacy and Safety Protections for America's Youth

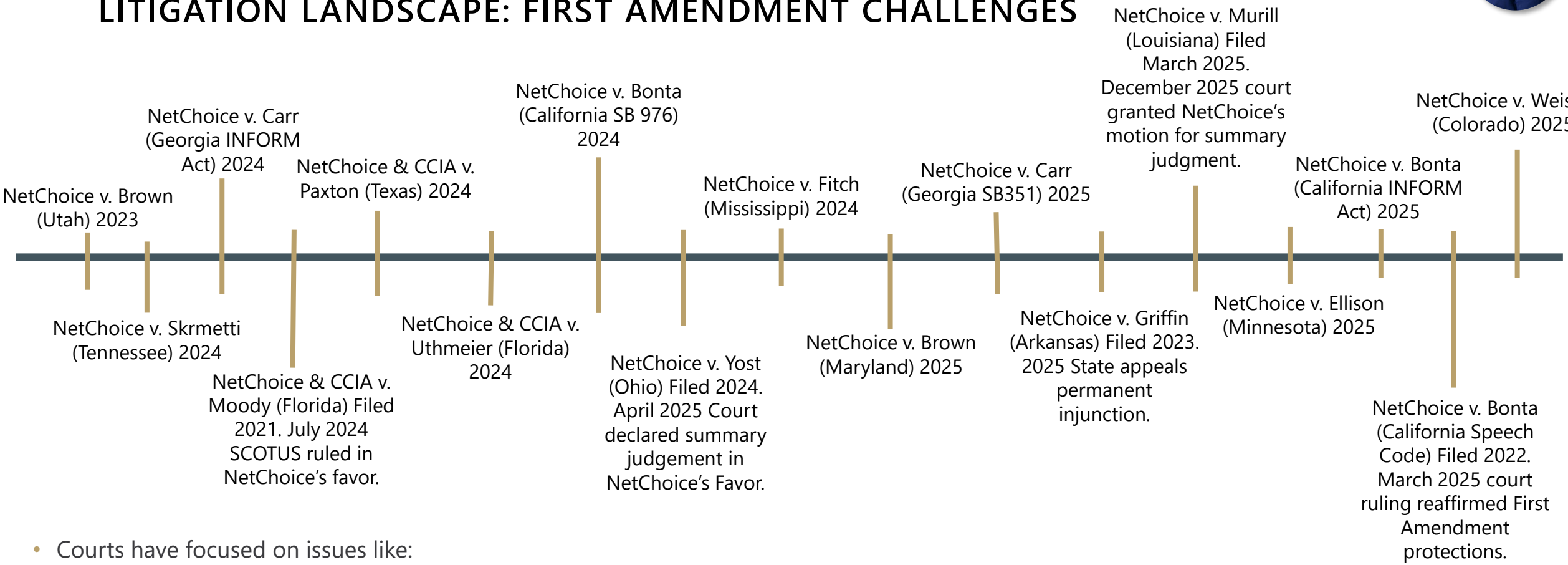
AG Campbell Joins Multistate Coalition Urging Congress To Pass Kids Online Safety Act

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

STATE AG "CHECKLIST": WHAT THEY ASK FOR FIRST

- ✓**Data Maps**: How youth data flows across products, vendors, and SDKs
- ✓**Consent Records**: Parental consent logs, teen opt-in evidence
- ✓**Design Documentation**: UX flows, dark-pattern testing, A/B experiments
- ✓**Risk Assessments**: DPIAs for minors, profiling, targeted ads
- ✓**Third-Party Controls**: Contracts, monitoring, and SDK governance

LITIGATION LANDSCAPE: FIRST AMENDMENT CHALLENGES



- Courts have focused on issues like:
  - Compelled speech
  - Overbreadth
  - Vagueness
- Outcomes have varied. We have seen some provisions enjoined and others allowed to proceed…all contributing to our Patchwork Problem.

LITIGATION LANDSCAPE: AGE VERIFICATION

- **Adult Content Age Verification**
  - Post-Texas HB 1181 ruling
    - Texas's age-verification law for adult content triggered a wave of similar legislation in other states.
    - Courts have split on whether mandatory age-verification:
      - Impermissibly burdens access to lawful adult content
      - Violates anonymity rights
      - Is justified by compelling state interests in protecting minors
- **The Texas ruling has become a reference point for other states drafting or defending similar laws.**

06

ROADMAP FOR 2026

WHAT TO EXPECT IN 2026

1. More Youth-Focused Laws & Design Codes

- More states expected to adopt CA-style design codes (and many will face immediate constitutional challenges)
- Expansion of teen-specific opt-in requirements

2. Increased AG Scrutiny of Product Design

- "Addictive" features, infinite scroll, autoplay, and algorithmic feeds
- Expect deeper dives into internal research and UX testing

3. Litigation Will Shape the Boundaries

- First Amendment challenges will determine how far states can go
- Age-verification laws likely to proliferate, with mixed court outcomes

RECOMMENDATIONS

For businesses:

- ✓ Determine applicability early.
- ✓ Understand and map data flows of children's data and classify such data as sensitive in your systems.
- ✓ Prioritize privacy-by-design for children by setting high-privacy defaults, limiting profiling and geolocation, and avoiding dark patterns.
- ✓ Anticipate AG scrutiny of design choices, undisclosed SDKs and pixels, and sensitive data, such as biometrics and precise geolocation.

For parents:

- ✓ Use parental consent and supervision tools thoughtfully.
- ✓ Review teen account settings and monitor connected-app permissions.
- ✓ Opt into stricter privacy and communication controls when available.


Q&A