



PROGRAM MATERIALS

Program #36162

July 20, 2026

Protecting Kids Online: New Laws on Online Privacy and Safety for Minors

Copyright ©2026 by

- **Julia Jacobson, Esq. - Squire Patton Boggs**
- **Alan Friel, Esq. - Squire Patton Boggs**

**All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Protecting Kids Online: New Laws on Online Privacy and Safety for Minors

Celesq® Live Webinar
July 20, 2026 – 2:00pm ET

www.squirepattonboggs.com

Speakers



Alan L. Friel
Partner, Chair
Data Privacy, Cybersecurity &
Digital Assets
(Los Angeles)
alan.friel@squirepb.com



Julia Jacobson
Partner
Data Privacy, Cybersecurity &
Digital Assets
(New York)
julia.jacobson@squirepb.com

Key U.S. Laws: Minors Online

COPPA Updates

U.S. State
Consumer
Privacy Laws &
Minors

U.S. State Laws
- Online Safety
& Mental Health

Other U.S. Laws
with Age
Verification
Requirements

Minors and
Social Media -
State Law

Assessment and
Compliance

COPPA and State Consumer Privacy Laws

COPPA Rule Amendments – in force April 22, 2026 (except with respect to § 312.11(d)(1), (d)(4), and (g) (related to COPPA Safe Harbor))

- An official definition for “mixed audience”: an online service that is directed to children but “does not target children as its primary audience, and does not collect personal information from any visitor, other than for the limited purposes set forth in § 312.5(c), prior to collecting age information or using another means that is reasonably calculated, in light of available technology, to determine whether the visitor is a child.”
- Expanded Data Security Requirements that provide minimum requirements for the “reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children” (§ 312.8)” standard, including a written information security program that contains many of the same safeguards required under state cybersecurity laws, i.e., an accountable person, risk assessments, testing and monitoring, and vendor due diligence.
- Requires opt-in consent for targeted advertising and other disclosures to third parties.
 - Website and online service operators covered by COPPA will be required to obtain separate verifiable parental consent to disclose children’s personal information to third-party companies related to targeted advertising or other purposes.

2026 *Proposed* Children and Teens' Online Privacy Protection Act ("COPPA 2.0") - [Senate Bill 286](#) passed Senate on March 6, 2026 *but did not progress*

- Applies to teens
- New definition of "individual-specific advertising to children or teens", which is prohibited except (i) advertising or marketing to in response to the individual's specific request for information or feedback; (ii) contextual advertising when the advertisement appears and does not vary based on personal information related to the viewer; "(iii) processing personal information solely for measuring or reporting advertising or content performance, reach, or frequency, including independent measurement; (iv) advertising or marketing directed to a connected device used by both adult and child or teen members of a household where such advertising or marketing is directed to the profile of the adult user.
- Collect personal information only when consistent with the context of a particular transaction or service or the relationship of the child or teen.
- Store personal information in U.S. unless notice to child's parent or teen.
- Requires FTC to develop "common verifiable consent mechanism".

- Consumer under age 13: Obtain verifiable parental consent in accordance with the COPPA before collecting or processing personal data of a child.
- Consumer who is at least age 13 but under age 18:
 - Do obtain consent before collecting or processing personal data for:
 - (i) targeted advertising; (ii) the sale/sharing of personal data; and (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer; and
 - any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the minor's personal data or that is reasonably necessary for, and compatible with, the processing purpose that the controller disclosed at the time the controller collected the minor's personal data.
 - Do not:
 - Provide any consent mechanism that is designed to substantially subvert or impair or is manipulated with the effect of substantially subverting or impairing, user autonomy, decision-making or choice; or
 - Collect minor's precise geolocation data unless certain additional requirements are met (SCPLs of California, Connecticut, Montana, Virginia).

U.S. wide high-water mark approach to minors’ personal data processing limits options because, for example:

- “minor” is defined as at least age 13 but younger than either age 16, 17 or 18
- Per Maryland SCPL: no use of personal data for targeted advertising or sale if consumer is under age 18.
- Per Connecticut SCPL:
 - no use of personal data for targeted advertising or sale (+ **profiling effective July 1, 2026**) if a controller has actual knowledge, or willfully disregards, that the consumer is at least age 13 but under age 18.
 - **effective July 1, 2026**, online service product or feature cannot collect geolocation from minors (< age 18) unless strictly necessary plus prohibitions related to direct messaging and addictive design.
- Per Oregon SCPL: no use of personal data for targeted advertising or profiling in furtherance of decisions that produce legal effects or effects of similar significance if a controller has actual knowledge, or willfully disregards, that the consumer is under age 16.
- Per Vermont SPCL: no use of personal data for targeted advertising or sale if controller has actual knowledge, and willfully disregards, that a consumer is at least 13 years of age but younger than 18.
- SCPL of Alabama, Minnesota, Montana, and New Hampshire require consent for targeted advertising or sale if a controller has actual knowledge, or willfully disregards, consumer is under age 16.

SCPLs of Colorado, Connecticut, and Montana:

- “Online service, product, or feature” means any service, product, or feature that is provided online (***online service***).
- “Minor” means any consumer who is under the age of 18.
- The controller must: (a) use reasonable care to avoid heightened risk of harm to minors; and (b) conduct a data protection assessment if there is a heightened risk of harm to minors.
- If the minor is younger than age 13, the consent must be acquired from the minor's parent or legal guardian.
 - A controller that complies with the verifiable parental consent requirements in COPPA has satisfied any requirement to obtain parental consent.
- Unless a controller has obtained consent, a controller that offers any online service to a consumer whom the controller actually knows or willfully disregards is a minor must not process a minor's personal data:
 - (Excluding Connecticut, which effective July 1, 2026, prohibits) for the purposes of (i) targeted advertising; (ii) the sale of personal data; or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer;
 - For any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the minor's personal data or that is reasonably necessary for, and compatible with, the processing purpose that the controller disclosed at the time the controller collected the minor's personal data; or

- Unless a controller has obtained consent, a controller that offers any online service to a consumer whom the controller actually knows or willfully disregards is a minor must not:
 - process a minor's personal data for longer than is reasonably necessary to provide the online service.
 - collect a minor's precise geolocation data unless:
 - Such precise geolocation data “is reasonably” / “are strictly” necessary for the controller to provide the online service and, if the data is necessary to provide the online service, such controller may only collect such data for the time necessary to provide such online service; and
 - The controller provides the minor a signal indicating that the controller is collecting precise geolocation data, that signal must be available to the minor for the entire duration of collection.
 - Specific exclusions apply in the SCPLs of Montana and Colorado.
 - use a feature to significantly increase, sustain, or extend a minor’s use of the service, product, or feature.

Global Privacy Enforcement Network audit [published March 2026](#) conducted by 27 global data protection authorities (including California) reported an overall increase in age assurance practices in the last 10 years but "the sole use of self declaration (or lack of age assurance altogether) is concerning for websites and apps identified as having inappropriate content or high-risk data processing and design features for children."

Summary of findings

- **Age Verification:** For 72 percent of the websites and mobile applications assessed, participants were able to bypass age verification mechanisms – most often through age self-declaration mechanisms to restrict access.
- **Collection of personal information about children:** Overall increase in information compared to the 2015 survey.
- **Privacy and control features:** 71 percent of websites and mobile applications did not have privacy information and privacy settings tailored to children.
- **Account deletion:** 36 percent of websites and mobile applications did not have an accessible way to delete accounts.
- **Inappropriate content and high-risk design:** Only 35 percent of the services considered to have inappropriate content or high-risk design towards children stated how they processed personal data.

■ Arkansas Children and Teens Online Privacy Act (**ACTOPA**)

- In force on July 1, 2026
- “Child” is defined as under 13 + in Arkansas
- “Teen” is age 13 – 16
- Privacy rights:
 - Deletion of account, content, or information submitted by the *child* or deletion of personal information *collected from a teen* or content *submitted by a teen*
 - excludes operators of “an interactive gaming platform that complies with the requirements of COPPA” (§ 4-88-1502(9)).

■ New York Child Data Protection Act (**NYCDPA**)

- In force as of June 20, 2025
- “Child” has the same meaning as COPPA – per the NY Attorney General’s guidance (issued on May 19, 2025); “Minor” is under age 18
- Age flags – an operator is required to treat a user as minor or child if the user's device “communicates or signals that the user is or shall be treated as a minor, including through a browser plug-in or privacy setting, device setting, or other mechanism” that complies **with the Attorney General’s regulations. (§ 899-ii)**

State Privacy Laws Specific to Minors

	Arkansas	New York
Effective Dates	July 1, 2026	June 20, 2025
Applies to operator of online service directed at children or with actual knowledge of collecting personal data of child	Yes Excludes interactive gaming platform[s] that comply with COPPA.	Yes
Obtain Consent	For the collection, use, or disclosure of personal data from a teen.	When processing a covered user’s personal data is not strictly necessary, unless processing of child personal data is COPPA compliant.
Notice	Provide notice including personal data collected and purpose, rights, categories of personal data shared with third parties, and categories of such third parties.	Request for informed consent that is separate from other transaction , does not use subverting mechanism, describes processing, and includes option to refuse consent. May only be requested once a calendar year.
Targeted Advertising	Prohibited.	Prohibits “activities related to marketing, advertising, research and development, providing products or services to third parties.”
Sale	N/A	Prohibited.
Age Gating or Verification Functionality	Not required to implement.	N/A

State Privacy Laws Specific to Minors

	Arkansas	New York
Age Flags	N/A	Browser plug-in, privacy setting, device setting, or other mechanism that complies with regulations can communicate user is a minor and consent to processing.
Consumer Rights	• Right to delete account or information of child and refuse further use • Right to correct personal data of child by parent • Right to obtain copy of personal data of child by parent • Right to delete personal data of teen by teen or parent • Right to correct personal data of teen by teen or parent • Right to obtain copy of personal data of teen by teen or parent	N/A Once an operator becomes aware that a user is a minor, they must delete the minor’s personal data within 30 days, unless (i) processing is permitted under COPPA , (ii) is strictly necessary, or (iii) the operator has informed consent.
Data Minimization	Limit collection to what is necessary for service.	Limit collection to what is necessary for service.
DPA’s	N/A	DPAs required for all third parties and service providers.

State Minors-Specific Laws

Age Appropriate Design Laws

Key Considerations

- Definition of “child” and “minor”
- Notice and Consent
- Privacy by Design or Default
- Parental Controls
- Age Verification or Age Determination
- Assessment Requirements
- Targeted Advertising Restrictions
- Privacy Rights
- Data Minimization
- Prohibited Practices

South Carolina Age-Appropriate Code Design - effective as of February 5, 2026

- “Child,” not defined
- “Minor” = under age 18
- Applies to a “covered online service” that is reasonably likely to be accessed by minors and meets certain thresholds.
- Prohibits features that encourage excessive use (e.g., infinite scrolling, auto-playing videos, push notifications). (§ 39-80-30)
- Audit reports must be prepared by an independent third-party auditor and the public report must be submitted annually on or before July 1 to the Attorney General who shall post it in a prominent place on his internet website. Audit reports must include:
 - the purpose of the covered online service;
 - the extent to which the covered online service is likely to be accessed by minors;
 - whether, how, and for what purpose the minors' personal data is collected or processed;
 - the design safety and the privacy protections for minors, and the parental tools adopted;
 - whether and how covered designed features are used;
 - the process for handling data access, deletion, and correction requests for a minor's data;
 - age verification or estimation methods used; and
 - a description of algorithms used by the covered online service.

California Age-Appropriate Design Code Act (CAADCA) – Effective as of July 1, 2024*

(*Certain provisions remain enjoined)

- Applies to a business that provides an online service, product, or feature “likely to be accessed by children”
- “Child” = under age 18
- Age assurance is required – “A business that provides an online service, product, or feature likely to be accessed by children shall estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers.” (§ 1798.99.31(a)(5).)
- A business that collects precise geolocation data must provide an obvious sign to the child for the duration of the collection or if the child is being monitored or tracked through the service by a parent/guardian.

As of March 12, 2026, the U.S. Court of Appeals for the Ninth Circuit decision vacated the CAADCA injunction except for:

- Data Protection Impact Assessment requirements
- Prohibitions on
 - features the operator knows/should know are “materially detrimental to the physical health, mental health, or well-being of a child”
 - data processing unless operator can demonstrate that processing is in “the best interests of children likely to access the online service, product, or feature”
 - profiling
 - dark patterns

All other CAADCA provisions are enforceable.

Maryland Age-Appropriate Design Code Act, effective as of October 1, 2024

(*Also, under challenge)

- “Child” = under age 18
- Applies to a “covered entity” that offers online products reasonably likely to be accessed by children in Maryland.
- Similar to the CAADCA, if the child’s precise geolocation data is being processed, an obvious signal must be displayed to the child for the duration of the processing.
- A business may not use dark patterns to: (I) *cause* a child to provide personal data beyond what is reasonably expected to provide the online product; (II) *circumvent privacy protections*; or (III) *take any action that the business knows, or has reason to know, is not in the best interests* of children who access or are reasonably likely to access the online product. (§ 14-4606(A)(7).)
 - A similar provision in the CAAADCA is enjoined.

Vermont Age-Appropriate Design Code Act – In force on **January 1, 2027**.

- “Child,” not defined but for purposes of determining whether an online product, service or feature is “reasonably likely to be accessed by a covered minor,” the term “child” is under age 13 as per the COPPA.
- “Minor” = under age 18
- Applies to a “covered business” whose online products, services, or features are reasonably likely to be accessed by a minor and “generates a majority of its annual revenue from online services,” among other thresholds.
- Restrictions on design features that encourage compulsive usage (e.g., auto-play, infinite scroll), dark patterns, and push notification restrictions. (§ 2449d(1).)
- A covered minor has the right to request that the covered minor’s account on a social media platform be unpublished or deleted from a “*social media platform*” *within 15 days after the covered business receives the request*. The covered business must provide a “prominent and accessible tool” for the covered minor to submit the deletion request. (§ 2449d(b).)
- The Vermont Attorney General is in the process of adopting rules identifying commercially reasonable and technically feasible methods for covered businesses and processors to determine if a user is a covered minor, including a review process for users appealing their age designations, and additional privacy protections for age assurance data as needed and expects the rules to be completed by the time the law is in effect.

Nebraska Age-Appropriate Online Design Code – In force on January 1, 2026, amendment effective July 17, 2026

- “Child” = under age 13
- “Minor” = under age 18
- Applies to a “covered online service” that generates a majority of its annual revenue from online services, determines the purpose of processing, and either (i) exceeds \$25 million in gross annual revenue; (ii) annually processes the personal data of 50,000 or more consumers. (§ 2(5).)
- Prohibits targeted advertising to a covered minor (§ 6(4)) and restricts the use of “dark patterns.” (§ 9(2).)
- Push notification restrictions. (§ 6(6).)
- Tools must be provided to allow minors to opt into chronological feeds rather than algorithmic feeds, block unwanted contact, and restrict the sharing of precise geolocation. (§ 5(1).)

AI and Minors' Online Safety

State laws regulating Minors Use of AI Companions (aka Companion Chatbots): California, Colorado, Connecticut, Georgia, Idaho, Iowa, Nebraska, New York, Oregon, Washington

- **Transparency & Notice Requirements** - not minor specific in all laws
 - Reasonable Person Standard – notification required if a reasonable person interacting with an AI companion would believe that the person is interacting with a human; some laws also require measures to prevent AI companion from generating statements that would lead a reasonable person to believe that the person is interacting with another natural person; initial and recurring notices
 - Timing of Recurring Notices – every 3 hours or every 1 hour during continuous interaction – minor specific in some states
 - [Hawaii](#): “If an operator has actual knowledge or reasonable certainty that a user is a minor, the operator shall clearly and conspicuously disclose to the user that the user is interacting with artificial intelligence: (1) As a persistent visible disclaimer; or (2) Both: (A) At the beginning of each session; and (B) Appearing at least once per hour in a continuous AI companion interaction that reminds the user to take a break from the chat and that the conversation is artificially generated and not with a human.” (other states are 3 hours – see, e.g., [Colorado](#), [Idaho](#))
 - [New York](#): “An operator shall provide a notification to a user at the beginning of any AI companion interaction and at least every three hours for continuing AI companion interactions thereafter, which states either verbally or in bold and capitalized letters of at least sixteen point type, the following: ‘THE AI COMPANION (OR NAME OF THE AI COMPANION) IS A COMPUTER PROGRAM AND NOT A HUMAN BEING. IT IS UNABLE TO FEEL HUMAN EMOTION.’” [not specific to minors]
 - [California](#) – An operator shall “[p]rovide by default a clear and conspicuous notification to the user at least every three hours for continuing companion chatbot interactions that reminds the user to take a break and that the companion chatbot is artificially generated and not human.”

■ Minor Safety

- Minor: Operator “knows is, or is reasonably certain is, under eighteen years of age” ([Iowa](#); see also [Georgia](#), [Idaho](#)); variations include “knows or has reason to believe” ([Connecticut](#), [Oregon](#)); “operators knows is a minor” ([California](#))
 - Age Verification – operator must use “commercially reasonable methods or generally accepted methods to estimate the age of account holders or users” ([Colorado](#))
 - [New York Safe By Design Act](#): “the Attorney General may promulgate rules and regulations identifying methods for reasonable and technically feasible age assurance...”
- Parental Controls – “No operator shall provide an artificial intelligence companion to a user, or operate an artificial intelligence companion for a user, if the operator knows, or has reason to believe, that the user is younger than eighteen years of age, unless the operator has made available to minor users and their parents or legal guardians tools to manage minor users’ screen time and account settings.” ([Connecticut](#)); “For accounts known to belong to minor users, an operator shall offer reasonable tools to a minor or parent to manage the minor's screen time and account settings...” ([Georgia](#); also [New York Safe By Design Act](#))
- Measures for preventing manipulative engagement techniques to engage/prolong emotional relationship with a minor.
 - [Iowa](#): “An operator shall not provide a minor user with points or similar rewards at unpredictable intervals with the intent to encourage increased engagement”
 - [Georgia](#): An operator shall adopt reasonable measures to prevent an AI companion chatbot to use the following techniques directed to a minor (1) Reminding or prompting the minor to return for companionship or emotional support; (2) Excessive praise designed to deepen emotional attachment or prolong use; (3) Statements designed to discourage breaks or suggest frequent return is necessary; (4) Soliciting gifts, premium purchases, or expenditures framed as necessary to maintain the relationship; or (5) Variable or unpredictable rewards intended to increase engagement
 - Also [Connecticut](#)

- **Measures for self harm prevention**

- Colorado: “a protocol for a conversational artificial intelligence service to respond to a user prompt regarding suicidal ideation or self-harm, which protocol must include user referral to a crisis service provider such as a suicide hotline, a crisis text line, or another appropriate crisis service, but not including a law enforcement agency, and escalation procedures for repeated or severe crisis indicators.”
- California: “An operator shall prevent a companion chatbot on its companion chatbot platform from engaging with users unless the operator maintains a protocol for preventing the production of suicidal ideation, suicide, or self-harm content to the user, including, but not limited to, by providing a notification to the user that refers the user to crisis service providers, including a suicide hotline or crisis text line, if the user expresses suicidal ideation, suicide, or self-harm.”

- **Harmful Content Controls**

- Reasonable measures to prevent the companion chatbot from “producing visual depiction of sexually explicit material” or “stating the minor should engage in sexually explicit conduct” (Iowa; also [Nebraska](#), [New Hampshire](#) (among others))
- Disclose on its platform that companion chatbots may not be suitable for some minors (California)

App Store Accountability Laws

- Five laws
 - Alabama - App Store Accountability Act
 - Louisiana - Online Protections for Minors
 - Texas - App Store Accountability Act
 - Utah - App Store Accountability Act
 - California - Digital Age Assurance Act
- Require both the app store providers/owners *and* developers to meet certain obligations related to minors.
- Google Play and the Apple App Store have guidelines for developers:
 - Google Play - [Changes to Google Play for upcoming app store bills for users in applicable US states](#)
 - Apple Store - [Age assurance frameworks Q&A](#)

- Texas App Store Accountability Act (SB 2420)
 - Lawsuits by the Computer & Communications Industry Association and the Students Engaged in Advancing Texas allege violations of First Amendment (free speech protections for users, app stores, and app developers) and Fourteenth Amendment (due process violated by vagueness).
 - December 23, 2025 – Texas federal judge enjoined enforcement.
 - June 2, 2026 – Fifth Circuit stayed the injunction
 - July 6, 2026 – [SCOTUS](#) did not vacate the Fifth Circuit stay
- Other app store accountability laws are not currently enjoined.
 - [Alabama](#) (signed on February 17, 2026 and in force January 1, 2027)
 - Louisiana (in force July 1, 2027)
 - Utah (in force May 6, 2027)
 - [California](#) (in force January 1, 2027)

- A lawsuit filed on February 5, 2026, was voluntarily dropped on April 21, 2026, after [HB 498](#) (amendment) was signed on March 18, 2026
- Key Changes
 - State enforcement removed; only enforceable by private right of action
 - No rulemaking
 - In-app purchases defined
 - Refines requirements for pre-installed applications – now excludes “(i) operating system functions; (ii) essential device drivers; and (iii) apps necessary for basic device operations” (e.g., phone, settings, emergency services, security, or system maintenance)
 - The term “significant change” excludes changes to user experience and functionality and includes “in-app purchases” and “advertisements” if they previously were not “previously present in the app”
 - Adds that a developer may request an app store provider prevent minor accounts from downloading the developer's app
 - Clarifies that “commercially available methods that are reasonably designed to ensure accuracy” for a minor include affirmative age attestation by a parent together with other age information collected as part of the creation or use of an account

- [HB 977](#) passed on May 5, 2026, replacing the original law enacted June 30, 2025
 - Similar to Utah's amendment, Louisiana now extends its coverage to pre-loaded applications
 - A developer may rely on app store age signals unless developer has actual knowledge that its own data is more accurate
 - A developer may rely on app store parental consent signals
 - Adds "family account application" requirements for age range defaults and associations with subaccounts

Key Considerations

- Applicability – App Store Provider vs. Operating System Provider
 - Identify account holder's age information and/or verify account holder's age information and/or assign an age category to the account holder
 - Parental consent
 - Affiliate minor account with parental account
 - Notification requirements for revocation of consent
 - Data minimization
 - Data Protection
 - Prohibitions
- App developer requirements
 - Verify minor account holder's age category and parental consent
 - Notification of significant changes to the app
 - Enforce in-app age category restrictions
 - App age rating
 - Prohibitions

Social Media Parental Consent Laws

Social Media Parental Control Laws – Many Proposed, Few Survived

- Temporarily enjoined laws:
 - Utah Social Media Regulation Act
 - Texas Securing Children Online through Parental Empowerment Act
 - Florida An Act Relating to Online Protections for Minors
 - Mississippi Walker Montgomery Protecting Children Online Act.
 - Georgia Protecting Georgia's Children on Social Media Act
 - Minnesota Prohibiting Social Media Manipulation Act
 - Colorado Protections for Youth Using Social Media Act
 - California Protecting Our Kids from Social Media Act
- Ohio Parental Notification by Social Media Operators Act - June 18, 2026, [opinion](#) lifted previous injunction
- Permanently enjoined laws:
 - Arkansas Social Media Safety Act
 - Louisiana Secure Online Child Interaction and Age Limitation Act

- Idaho Stop Harms from Addictive Social Media Act ([HB 542](#)) signed April 2, 2026, and effective July 1, 2026
 - Applies to “covered social media platform,” which means the social media platform has generated at least one billion dollars (\$1,000,000,000) in advertising revenues worldwide in one (1) or more of the preceding three (3) years.
 - “Child” means age 16 or younger; “Minor” means under age 18
 - “If a covered social media platform is able to conclude with eighty percent (80%) confidence or higher that the account holder is older than sixteen (16) years of age, the covered social media platform may treat the account holder to be other than a child for the purposes of this chapter. Otherwise, the covered social media platform shall treat the account holder as a child for the purposes of this chapter.”
 - Requires verifiable parental consent for children and higher default privacy settings
 - Prohibits targeted advertising and “addictive interface features”

Assessment and Compliance

1. Conduct a minor's data assessment
 - Consider Audience – child, minor and/or adult
 - Consider Content
 - Consider Advertising
 - Consider Data Disclosures
2. Determine compliance approach: state by state, U.S. wide, international
3. Update/prepare online notices, parental notice, and consent systems
4. Implement content detection and management systems
5. Assess what “good faith” compliance efforts look like
6. Establish monitoring efforts to anticipate emerging legislative and enforcement activity

Key Contacts



Alan L. Friel
Partner, Chair
Data Privacy, Cybersecurity &
Digital Assets
(Los Angeles)
alan.friel@squirepb.com



Julia Jacobson
Partner
Data Privacy, Cybersecurity &
Digital Assets
(New York)
julia.jacobson@squirepb.com