AN A.S. PRATT PUBLICATION
FEBRUARY 2026
VOL. 12 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 2** **February 2026**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Navigating Minors' Privacy and Online Safety Laws: A Strategic Guide for Businesses

By Maki DePalo and Hyun Jai Oh*

In this article, the authors explain that recent bipartisan privacy and online safety initiatives reflect growing concern over youth mental health, online exploitation, and manipulative digital design. The authors outline how companies can stay ahead by integrating privacy-by-design principles, implementing age-appropriate features, and mitigating risks of harm to minors.

Businesses offering online services to minors face a rapidly expanding and fragmented legal landscape. As new state and federal laws take effect, companies face a need to revisit their business strategies and reassess the business value of serving minors against growing compliance complexity and potential liability. The federal Children's Online Privacy Protection Act of 1998 (COPPA) remains the foundation of privacy and online safety regulation, but businesses now face a new wave of state-level laws. This evolving patchwork creates new operational challenges with nuanced applicability criteria, obligations, and remedies.

Terminology across minors' privacy and online safety laws is far from uniform. One statute may define a "child" as someone under 13, while another uses the same term for anyone under 18. To avoid confusion, this advisory designates "children" as individuals under 13, "teens" as 13 to 17, "minors" as under 18, and "adults" as 18 or older.

SOCIETAL IMPERATIVE FUELING LEGISLATIVE ACTION

The legislative momentum around minors' privacy and online safety reflects growing societal concern over the pervasive influence of digital platforms on youth mental health, autonomy, safety, and well-being. High-profile incidents involving online exploitation, exposure to harmful content, and manipulative design features have galvanized public discourse and prompted policymakers' attention. Parents, educators, and youth advocacy groups have increasingly demanded stronger safeguards, prompting state laws aimed at creating safer digital environments for minors.

* Maki DePalo, a partner in the Atlanta office of Alston & Bird LLP, may be contacted at maki.depalo@alston.com. Hyun Jai Oh, an associate in the firm's office in Atlanta, may be contacted at hyunjai.oh@alston.com.

CATEGORIES OF MINORS' PRIVACY AND ONLINE SAFETY LAWS

Minors' privacy and online safety laws vary widely in age thresholds, scope, and obligations. With state legislatures introducing bills at a rapid pace, it can be challenging to understand these statutes, navigate their nuances, and establish workable compliance strategies.

One practical way to address this challenge is to categorize relevant laws. Minors' privacy and online safety laws fall into the following five categories:

1. Laws that require consent for processing minors' data;
2. Comprehensive privacy laws that impose minor-specific requirements;
3. Age-appropriate design codes;
4. Laws establishing age-range signals; and
5. Social media laws.

CATEGORY 1: LAWS THAT REQUIRE CONSENT FOR PROCESSING MINORS' DATA

Federal Children's Online Privacy Protection Act of 1998

COPPA applies to operators of websites or online services that target children or knowingly collect personal information from them. Operators subject to COPPA must post an online children's privacy policy, provide direct parental notice, and obtain verifiable parental consent before collecting, using, or disclosing children's personal information. COPPA also requires operators to maintain reasonable measures to protect the confidentiality, security, and integrity of personal information collected from children.

The Federal Trade Commission (FTC) has rulemaking authority under COPPA. In April 2025, the FTC amended the Children's Online Privacy Protection Rule (COPPA Rule) to add new operator obligations, including written information security program and written data retention policy for children's personal information. The FTC, often working with state regulators, has remained active in enforcement, bringing more than a dozen public COPPA enforcement actions in the past two years, some resulting in multimillion-dollar settlements.

Arkansas Children and Teens' Online Privacy Protection Act

Effective July 1, 2026, the Arkansas Children and Teens' Online Privacy Protection Act (Arkansas CTOPPA) extends COPPA-like protections to Arkansas teens under 17. Operators of websites or online services with actual knowledge that they collect personal

information from these users must obtain the teen's consent before doing so. Arkansas CTOPPA also mandates data minimization and security measures, compliant privacy notices, and privacy rights for both teens and their parents.

New York Child Data Protection Act

Effective June 20, 2025, the New York Child Data Protection Act (NYCDPA) applies to operators of websites or online services that primarily target minors or knowingly collect their personal information. Covered operators that process minors' personal information must obtain consent from the minor (if a teen) or the parent (if a child) unless processing is strictly necessary for specified "permissible purposes," including:

- Providing and maintaining requested products or services;
- Identifying and repairing technical errors;
- Protecting against malicious, fraudulent, or illegal activity; and
- Complying with law or legal process.

CATEGORY 2: COMPREHENSIVE PRIVACY LAWS WITH MINOR-SPECIFIC REQUIREMENTS

Nineteen states – California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Minnesota, Maryland, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia – have enacted comprehensive privacy laws (CPLs) protecting residents' personal information and imposing additional obligations when processing minors' personal information.

Sensitive Personal Information

All but one CPL – the California Consumer Privacy Act (CCPA) – classify personal information collected from known children as sensitive personal information. Businesses processing this data must apply heightened security measures appropriate to its sensitivity. Of those non-California CPLs, two (Iowa and Utah) allow individuals to opt out of businesses' processing of sensitive personal information, while the remaining 16 require consent and a formal data protection assessment before processing it.

CCPA regulations were recently amended to expand the definition of sensitive personal information to include personal information of individuals known to be under 16. Effective January 1, 2026, businesses must maintain enhanced security measures for processing personal information of individuals known to be under 16. While consent is not required, businesses processing such data must provide individuals with the right to limit processing and, effective January 1, 2026, conduct a formal risk assessment to evaluate the risks and benefits of processing.

Restrictions on personal information sale, targeted advertising, and automated decisions

Several states require businesses to obtain consent before selling personal information or using it for targeted advertising involving individuals known to be under 16 (California, Minnesota, New Hampshire, Oregon), 17 (New Jersey), or 18 (Colorado, Connecticut, Delaware, Montana). In Maryland, businesses are prohibited from selling personal information of known minors or using it for targeted advertising.

Consent is also required in certain states to use personal information of individuals known to be under 16 (Oregon), 17 (New Jersey), or 18 (Colorado and Connecticut) when making automated decisions that have significant impacts on individuals such as approving or denying financing, health care services, or education opportunities.

Duty of Care

In Colorado and Connecticut, CPLs impose a duty of care on businesses offering online products to known minors. Covered entities must exercise reasonable care to avoid a heightened risk of privacy harm to minors, which includes:

- Conducting a formal data protection impact assessment (DPIA) to evaluate the online product's benefits and risks to minors;
- Implementing data minimization measures;
- Restricting direct messaging from adults to minors through the online product; and
- Avoiding design features that encourage addictive or manipulative use.

CATEGORY 3: AGE-APPROPRIATE DESIGN CODES

Age-appropriate design codes (AADCs) require businesses to proactively design online services that are safe and appropriate for minors. They mark a significant shift from the traditional U.S. framework focused on notice and consent, prohibiting processing activities or design features that create unmitigated risks of material harm to minors. Neither minors nor their parents can consent to those activities or features.

California became the first state to enact an AADC in 2022. Modeled on the UK's version, California's law applies to businesses subject to the CCPA that operate online services "likely to be accessed" by minors. Key requirements include:

- Conducting a formal DPIA to evaluate the online service's potential harm to minors and identify timed mitigation measures;
- Refraining from using minors' personal information in ways the business knows or should know are materially detrimental to minors' health or well-being;

- Limiting processing of minors' personal information to what is necessary for online services with which minors actively and knowingly engage;
- Configuring a protective default privacy settings for minor; and
- Presenting online terms, such as terms of service and privacy policies, in clear, age-appropriate language.

Although the California AADC is preliminarily enjoined on First Amendment grounds, Maryland, Arkansas, and Nebraska have enacted similar statutes incorporating many of the same requirements.

CATEGORY 4: LAWS ESTABLISHING STANDARDIZED AGE-RANGE SIGNALS

App Store Accountability Acts

Louisiana, Texas, and Utah have enacted app store accountability acts (ASAAs) requiring app store providers and developers to implement measures to protect minors. While most ASAA requirements fall on app store providers, app developers must also comply with certain obligations, including:

- Verifying users' age category – "child" (under 13), "younger teenager" (13 to 15), "older teenager" (16 to 17), or "adult" (18 or older) – and using this classification to enforce the developer's age restrictions, comply with applicable law, and implement age-based safety features;
- Requiring that minors' accounts are linked to a parent's app store account and obtaining parental consent before a minor downloads an app, purchases an app, or makes in-app purchases;
- Notifying app store providers of any significant changes to the app's terms or privacy policy that materially affect the app's functionality, user information, or personal information processing; and
- Providing accurate information about the app's age rating and personal information processing practices to app store providers so it can in turn be made available to parents.

ASAAs reflect an emerging legislative trend toward requiring businesses to affirmatively verify the age of platform users. By contrast, minors' privacy requirements under COPPA, Arkansas CTOPPA, NYCDPA, and CPLs only arise when a business knowingly processes minors' personal information or intentionally targets minors. Likewise, AADCs also do not mandate age verification, although businesses are permitted to do so to provide age-appropriate services to different age groups. Under ASAAs, however, age verification is a requirement.

California Digital Age Assurance Act

Effective January 1, 2027, California's Digital Age Assurance Act (DAAA) introduces a device-based age-verification system. DAAA requires operating system providers to collect users' age information during device setup and transmit age-range signals to developers through a real-time API. These signals – under 13, 13 to 15, 16 to 17, or 18 and over – enable developers to tailor privacy and online safety features without collecting additional personal information.

The law aims to standardize age assurance across platforms, reducing friction and compliance burdens for developers. It also has significant implications under other privacy laws: Developers receiving age-range signals may be deemed to have actual knowledge of a user's age, triggering obligations under COPPA, CCPA, and AADCs.

CATEGORY 5: SOCIAL MEDIA LAWS

Fifteen states – Arkansas, California, Connecticut, Florida, Georgia, Louisiana, Minnesota, Mississippi, Nebraska, New York, Ohio, Tennessee, Texas, Utah, and Virginia – have enacted laws regulating minors' use of social media platforms. Several define social media platforms broadly enough to apply to online services with community-oriented features.

For example, the Texas Securing Children Online Through Parental Empowerment Act applies to operators of online services that allow individuals to socially interact, create public or semi-public profiles, and create or post content viewable by others.

Key requirements include:

- Requiring users to verify age and, for minors below the threshold, obtaining parental consent before granting them access;
- Providing parents with tools to view, understand, and restrict minors' activity on the platform;
- Configuring a protective default privacy and online safety for minors; and
- Avoiding sending notifications during sleep or school hours or using features that foster compulsive use.

Many of these laws face First Amendment challenges, some resulting in preliminary or permanent injunctions. Nevertheless, state legislatures continue to propose similar restrictions on minors' social media use.

COMPLIANCE STRATEGIES

The evolving landscape of minors' privacy and online safety laws requires businesses to adopt proactive, scalable compliance strategies. Practical steps include:

- *Assess the Business Case for Serving Minors*

  Determine whether to offer the online service to minors based on audience relevance and compliance risk. If minors are a target group, implement measures to comply with applicable requirements.

- *Monitor Legislation and Litigation*

  Track amendments and court challenges; categorize laws to identify new requirements and maintain a responsive compliance posture.

- *Choose an Appropriate Compliance Framework*

  Decide whether to implement a jurisdiction-specific framework, unified framework across all jurisdictions, or hybrid framework whose high-impact requirements are implemented only in relevant states.

- *Apply Privacy-by-Design and Document Good-Faith Efforts*

  Integrate privacy-by-design principles, record compliance efforts, and monitor regulatory development for guidance.