JANUARY 7, 2026

Looking Ahead to Privacy (and Similar) Issues for 2026

by Tatum Andres , Meghan K. Farmer

Privacy law evolved at a dizzying pace in 2025. Regulators brought headline-making enforcement actions, courts continued to shape the boundaries of existing statutes, and state legislatures advanced new laws.

Much of that activity centered on familiar pressure points: privacy notices and opt-out mechanisms, telemarketing and text messaging practices, and the collection and use of sensitive data, particularly biometric information, health data (such as the Healthline CCPA enforcement), and children's and teens' personal information (including actions against Roku in multiple jurisdictions).

Newly effective laws echoed those same priorities. For example, Maryland's comprehensive privacy law and several children's privacy statutes in states like New York and Colorado place new limits on how children's data may be used for advertising and related purposes, while Colorado also expanded consent requirements for certain biometric processing affecting both consumers and employees. In parallel, changes at the federal level including the FCC's expanded revocation-of-consent rule, continued to reshape expectations around consumer choice and control.

We expect that momentum to carry into 2026. To help you keep track, we've pulled together the key privacy laws and regulatory developments to watch in the year ahead.

What Laws to Look Out for in 2026:

New Comprehensive State Privacy Laws and Regulations

- Comprehensive privacy laws will take effect in **Indiana, Kentucky**, and **Rhode Island** in 2026. Save a couple of exceptions under the Rhode Island law (see below), these statutes generally do not introduce material new obligations for companies that already take a national approach to complying with US privacy laws. The Rhode Island Data Transparency and Privacy Protection Act is somewhat unique in that the law does not have a cure period, requires disclosure of all third parties to whom data is sold or may be sold, and contains a separate notice requirement for companies that sell PII.
- New **California Consumer Privacy Act regulation**s took effect on January 1, 2026, introducing formal requirements related to risk assessments, expanded consumer rights, and cybersecurity audits. Covered businesses will be required to submit risk assessments and certifications of audit

completion to the California Privacy Protection Agency in the coming years.

Expanded Children's Privacy Protections

- Laws that impact children's privacy in **Nebraska** and **Arkansas** will take effect in 2026 and impose requirements that go beyond COPPA (Nebraska's law is the Age-Appropriate Design Code that took effect on January 1, 2026, but enforcement does not begin until July 1, 2026. While Arkansas' Children and Teens' Online Privacy Protection Act goes into effect on July 1, 2026). These laws introduce heightened protections for minors, although the Arkansas statute in particular may face legal challenges on federal preemption grounds.
- Recent amendments to the **Connecticut Data Privacy Act** impose additional restrictions related to minors. The law now includes **a blanket prohibition on the sale of personal data or targeted advertising to minors** when a controller has actual knowledge, or willfully disregards, that a user is a minor, **regardless of consent**. While certain profiling activities may still be permitted with consent, controllers must conduct a data protection impact assessment and implement risk mitigation measures where risks are identified.
- **Oregon** law now prohibits the sale of a consumer's personal data without consent where a controller knows or reasonably should know the consumer is under 16. The law also restricts the sale of precise geolocation data capable of identifying an individual or device within a 1,750-foot radius, subject to limited communications- and utility-related exceptions. In addition, **controllers may not process personal data for targeted advertising purposes where the consumer is under 16.** Similar to Oregon, **Delaware** now prohibits controllers from processing personal data for targeted advertising purposes where the consumer is under 18, unless the controller obtains consent.

Looking Back at Privacy Enforcement Actions and Litigation Trends in 2025:

To prepare for compliance in 2026, companies must look back on privacy enforcement actions and litigation in 2025. State regulators and courts are increasingly shaping the practical boundaries of U.S. privacy law. Enforcement activity in California, Connecticut, and Texas, along with ongoing litigation surrounding tracking technologies in states across the U.S., shows that state regulators and the courts are not only active, but willing to push the interpretations of existing statutes.

- **California:** California continued to set the pace in 2025. California regulators announced the

largest CCPA settlement to date, focused on failures to honor opt-out requests, including Global Privacy Control signals, using personal information and sensitive personal information in ways that went beyond what was disclosed to consumers, weak vendor contracts, and misleading cookie banners and consent tools. One notable aspect of the action was the inclusion of certain article titles (i.e., titles that imply a website visitor was interested in certain health conditions) within the scope of sensitive personal information as health data.

- **Connecticut:** Connecticut also made headlines in 2025 by imposing its first monetary penalty under the Connecticut Data Privacy Act. The settlement stemmed from deficiencies in the company's privacy notice and, more significantly, the company's failure to fix those issues during the law's cure period. The Attorney General also alleged that the company overstated its remediation efforts. Notably, the complaint described consumer rights mechanisms as misconfigured or inoperable, signaling that regulators are testing how these tools work in practice, not just whether they exist. The takeaway is clear: consumer rights and opt-out mechanisms need to operate exactly as described in privacy disclosures.

- **Texas:** Texas enforcement activity picked up momentum as well. In May, the Texas Attorney General issued multiple noncompliance notices under the Texas Data Privacy and Security Act, giving companies 30 days to cure potential violations. In January 2025, the Attorney General brought the first enforcement action under the TDPSA, alleging unlawful collection and sale of sensitive personal data through embedded mobile app software. One key allegation was the failure to provide a Texas-specific notice required when sensitive data was sold. This action serves as a reminder that while many states have fairly similar comprehensive privacy laws, the details matter, and state-specific notice and consent requirements cannot be overlooked in a national compliance program.

- **Tracking Technology Litigation:** On the litigation front, state wiretapping claims—particularly under California's Invasion of Privacy Act (CIPA)—continued to pose meaningful risk for businesses in 2025. Plaintiffs have alleged that cookies, session replay tools, chat features, and certain third-party pixels intercept website communications in real time, triggering CIPA's all-party consent requirements. Whether users implicitly consent to such tracking (thereby defeating the plaintiffs' claims) remains heavily contested in various state courts. Many companies have adopted prior-consent cookie banners to collect consent for the tracking as a litigation risk-management measure, separate from broader privacy compliance programs. What has emerged as a best practice is a banner that clearly explains tracking categories and purposes, offers users a genuine choice, records consent, and blocks nonessential tracking unless and until consent is affirmatively given. Courts evaluating these designs tend to focus on clarity, timing, and whether users can access the site without agreeing to nonessential tracking. Designs that permit continued site

access using only strictly necessary cookies (while gating advertising behind consent) have generally fared better than banners that enable tracking by default. At the same time, 2025 also delivered an important defense-side win. In a California federal case involving pixel-based tracking allegations against AddShoppers and Peet's Coffee, the court denied class certification under CIPA. The court found that the named plaintiffs failed to satisfy the typicality and adequacy requirements, emphasizing that CIPA liability turns on whether tracking occurred without consent. One plaintiff could not establish that he experienced the alleged harm at all, while the other undermined his claims by deleting relevant browsing data after discovery began. The ruling underscores that plaintiffs' credibility, data preservation, and individualized consent experiences are central to class certification analysis in tracking-technology cases. Courts are increasingly unwilling to certify classes where the named plaintiffs' claims are not representative of the proposed class. Therefore, companies facing CIPA or pixel-tracking litigation in 2026 should scrutinize standing and factual allegations early, including inconsistencies in plaintiffs' testimony or data, and maintain clear records documenting consent mechanisms, data flows, and marketing practices. These cases show that well-designed consent tools and a strong evidentiary record can materially improve a company's ability to defeat class certification at an early stage.

Privacy Risk Areas Companies Should Monitor in 2026

As we head into 2026, the privacy landscape keeps getting broader and more complex. Lawmakers and regulators are pushing forward on several fronts at once, with particular momentum around social media regulation, telemarketing and messaging practices, and the use of sensitive data (especially biometric information). These areas are changing quickly, often unevenly across states, and continue to draw enforcement and litigation attention. As a result, they are important areas for your company to keep a close eye on in the year ahead.

Social Media & Online Platform Laws.

State legislatures continue to advance laws regulating minors' access to social media and online services. These laws also remain largely unsettled, with several measures permanently enjoined (including in Ohio and Arkansas) and many others in states such as Georgia, Virginia, Mississippi, and California are temporarily blocked or under active litigation, primarily on First Amendment grounds.

Broadly, states have taken three overlapping approaches. First, a number of laws focus on age assurance and parental consent, requiring platforms to determine users' ages and obtain parental permission before minors may access social media accounts or certain features, as reflected in statutes adopted in Florida, Tennessee, and Utah. Florida's law, which is now permitted to take effect after the lifting of a preliminary injunction, prohibits children under 14 from maintaining social media accounts, perhaps requiring covered platforms to implement age-verification and parental consent mechanisms.

Users aged 14 and 15 can have accounts only with parental consent. Tennessee has taken a broader approach, extending its parental consent requirement to users under 18; however, minors may maintain accounts with parental consent, which parents retain the right to revoke.

Second, a growing number of states have focused on restrictions on personalized or "addictive" content and targeted advertising for minors, including laws in California, New York, Arkansas and Louisiana, many of which impose recordkeeping, audit, and notice obligations. For example, New York's Child Data Protection Act restricts targeted advertising to children and requires additional disclosures and alerts when children's data is collected. This law is subject to ongoing rule making by the New York AG. Similarly, an Arkansas law prohibits targeted advertising to minors and imposes obligations around collection, use, and disclosure of minors' data. California law prohibits platforms from providing an "addictive feed" to minors without verifiable parental consent. The California Attorney General is directed to issue implementing regulations on age assurance and consent by January 1, 2027.

Third, several states have moved toward age-appropriate design code frameworks, regulating default settings, profiling, and risk assessments for services accessed by or likely to be accessed by minors, with notable examples in Nebraska, Maryland, and Vermont which impose expansive default-privacy, design, notification, and data-minimization requirements, including limits on profiling, push notifications, and algorithmic recommendations for minors.

Telephone & Telemarketing Laws

As we enter 2026, the regulatory environment for telemarketing and text messaging is undergoing its most significant transformation in decades. For years, businesses relied on Federal Communications Commission (FCC) orders as the "final word" on Telephone Consumer Protection Act (TCPA) compliance. However, a landmark Supreme Court decision (*McLaughlin v. McKesson*) and a wave of appellate rulings have fundamentally shifted the balance of power from federal regulators to federal judges.

The impact of this judicial independence is already visible. In 2023, the FCC attempted to implement strict new rules for "lead generating" telemarketers, requiring them to obtain separate consent for every individual party on whose behalf a message was sent. However, after the Eleventh Circuit Court of Appeals struck down the rule as an overreach of agency authority in ***Insurance Marketing Coalition Ltd. v. FCC***, the agency officially abandoned the rulemaking. In late 2025, the FCC reinstated its prior, less restrictive regulatory language, signaling a retreat from aggressive new mandates.

Perhaps the most surprising development for 2026 is the growing divide over whether text messages are even covered by certain parts of the TCPA. Despite decades of FCC guidance stating that a text is a "call," at least two federal courts—including the Seventh Circuit in ***Steidinger v. Blackstone Medical Services***—have recently found that text messages do not constitute "calls" under specific provisions of the Act. These conflicting rulings inject meaningful uncertainty for businesses that rely on text messaging, as plaintiffs may increasingly seek out jurisdictions with more favorable interpretations. Until appellate courts or Congress resolve the issue, companies will need to pay close attention to where

TCPA claims are filed and be prepared for divergent outcomes.

Adding to that complexity, the FCC adopted a new revocation-of-consent rule effective April 2025 that expands how consumers may opt out of receiving messages. Under the rule, consent is deemed revoked if a consumer responds with commonly understood phrases such as "stop," "quit," "end," "revoke," "opt out," "cancel," or "unsubscribe," as well as substantially similar responses. The rule also prohibits businesses from requiring consumers to use a single, exclusive opt-out method and instead requires honoring revocation requests expressed in any reasonable manner. Where consumers use nonstandard or ambiguous language, the reasonableness of the revocation is assessed based on the totality of the circumstances and, in the event of a dispute, the burden may fall on the sender to show that the consumer's message was not a reasonable request to revoke consent.

Biometric Privacy Laws

The use of biometrics continues to present legal risk, particularly class action exposure under Illinois' BIPA and Washington's MHMD law. That risk is underscored by recent enforcement activity. In 2025, the Texas Attorney General, acting under the state's biometric privacy law (commonly referred to as CUBI), secured a $1 billion settlement with Google. The settlement resolved allegations that Google tracked users' location data even when settings suggested otherwise, misrepresented the privacy protections of its "Incognito" browsing mode, and collected biometric identifiers, including voiceprints and facial geometry data, without obtaining proper consent.

At the same time, states are taking increasingly divergent approaches to biometric regulation. Texas has amended CUBI for 2026 to exempt certain AI systems from notice and consent requirements where those systems are developed or deployed to prevent security incidents, identity theft, fraud, or other illegal activity. This amendment brings Texas more closely in line with other state frameworks that provide broad carve-outs for safety and fraud-prevention use cases.

By contrast, Colorado has moved in the opposite direction. Recent amendments to the Colorado Privacy Act, which took effect on July 1, 2025, significantly expanded the scope of regulated biometric information by introducing a broad "biometric identifiers" category alongside a narrower "biometric data" subset, and by extending notice and consent obligations beyond what many other state laws require. As a result, biometric use cases that may fall outside other state regimes could still trigger compliance obligations in Colorado.

Conclusion

As privacy laws continue to evolve, 2026 is shaping up to be a year of contrasts. For many organizations that already take a nationwide approach to privacy compliance, newly effective comprehensive state laws may feel familiar and largely incremental. At the same time, other areas (particularly social media, children's privacy, telemarketing and biometrics) are becoming more complex, with laws that go beyond

notice and consent and instead place real limits on how data can be used.

Companies should expect regulators and courts to remain focused on sensitive data, minors, and "high-risk technologies." Staying compliant in this environment will require more than just tracking new statutes, it will also mean paying close attention to how existing laws are interpreted and enforced as businesses and technologies continue to change.

We will keep monitoring these developments and share updates as enforcement actions and litigation provide greater clarity on privacy risk in 2026.