Westlaw Today

2026 privacy developments to watch

By Libbie Canter, Esq., Jayne Ponder, Esq., Jenna Zhang, Esq., and Clare Mathias, Esq., Covington & Burling LLP

MARCH 5, 2026

2025 was a busy year for privacy, with new federal proposals, several amendments to state comprehensive privacy laws, and many new sector-specific privacy laws. As 2026 gets started, we share several areas that we are watching for this coming year.

Enforcement trends

State AG Guidance on Enforcement Priorities. Several states previewed priorities that will guide their enforcement activity and areas of focus for 2026. For example, the California Attorney General released a list of seven areas of focus for 2026 (https://bit.ly/40C3Sfh), which includes risk assessments, opt-out rights, rights to know and correct personal information, and an expanded definition of sensitive personal information.

Regulators are likely to continue to focus on how opt-out options are presented to consumers, including whether such choices contain so-called "dark patterns."

Likewise, the Indiana Attorney General released (https://bit.ly/402kZ9Z) guidance called the "Data Consumer Bill of Rights," which could preview the regulator's focus on consumer rights. Additionally, earlier in the year, both Oregon (https://bit.ly/3Pbo4lD) and Connecticut (https://bit.ly/3N1kbPz) released enforcement reports detailing their office's enforcement actions, both of which reveal a focus on consumer rights (particularly where rights diverge from other state privacy laws), reviews of privacy notice disclosures, and minor's data.

Opt-Out Rights Enforcement. Regulators are likely to continue to focus on how optout options are presented to consumers, including whether such choices contain so-called "dark patterns." This focus could echo recent enforcement, such as Sling TV's 2025 voluntary settlement (https://bit.ly/3OFHgrL) with the California Attorney General, in which the company agreed to provide consumers with an easy-to-use opt-out mechanism, including through a QR code on the screen if an opt-out wasn't commercially practical on the device.

Additionally, the Connecticut Attorney General's enforcement report (https://bit.ly/4cYjO2N) also emphasizes the regulator's focus on what it calls "problematic opt-out mechanisms" and dark patterns, such as in cookie banners, which could preview a priority area for the regulator in 2026.

Data Brokers. 2026 may also bring increased attention to data brokers, particularly in California. CalPrivacy launched a Delete and Request Opt-out Platform (DROP) (https://bit.ly/46BSzXZ) mechanism that allows consumers to opt-out of data brokers' use of personal data. In November, CalPrivacy announced a "data broker enforcement strike force" (https://bit.ly/4l8ukXt) that will investigate violations of the Delete Act and CCPA.

In December, the agency issued Enforcement Advisory No. 2025-01 (https://bit.ly/3OL5BfF), which provides CalPrivacy's interpretation of requirements for data broker registration for trade names, parent and subsidiary relationships, and other scenarios. It is likely that data brokers will be a focal area for California regulatory attention, which could encourage other states to focus on this issue.

In November, CalPrivacy announced a 'data broker enforcement strike force' that will investigate violations of the Delete Act and CCPA.

Coordinated State Enforcement. 2026 will likely see a continued increase in coordinated inquiries from regulators in the recently formed Consortium of Privacy Regulators (https://bit.ly/47i4L0c), which includes privacy regulators from 10 states. For example, in September, California, Colorado, and Connecticut announced (https://bit.ly/3OUL9ce) a joint investigative sweep focused on businesses' compliance with Global Privacy Control, and it is likely we will see continued coordination in 2026.

Litigation trends

In 2025, plaintiffs increasingly brought requests and arbitration demands under California's "Shine the Light" statute, which provides a private right of action and allows consumers to request disclosures regarding personal information shared for third-party direct marketing purposes (defined to include mail, telephone, and email). Additionally, the plaintiffs' bar brought several privacy class actions in 2025, with continued emphasis on bringing claims under the California Invasion of Privacy Act ("CIPA").

Following New York's lead in passing an algorithmic pricing disclosure requirement into law in 2025, other legislatures could focus on targeting algorithmic pricing.

For example, a class action complaint filed (https://bit.ly/3NeXVSt) in October alleges the entertainment franchise Dave & Buster's Entertainment Inc. violated CIPA by allegedly continuing to use third party cookies on its website after users selected a "Reject All" option on the site's cookie banner, and plaintiffs brought (https://bit.ly/3N1kKc9) a similar proposed class action in December against the retailer Kohler Co. alleging analogous CIPA violations.

New legislation and regulations

Minors' Privacy. Minors' privacy was a major focus (https://bit.ly/4un8KTt) of regulations and legislative proposals in 2025, and we expect significant activity in this area will continue in 2026. At the state level, states enacted over a dozen new minors' online privacy and safety laws in 2025 on a range of issues, including app store age verification requirements, mental health warning labels, and AI chatbots.

Nebraska and Vermont have both proposed new age-appropriate design codes. And, as discussed above, the updated CCPA regulations consider the personal information of consumers under 16 as "sensitive." Colorado also completed rulemaking in connection with minor-related provisions of the CPA, and New York has an active rulemaking for the SAFE for Kids Act.

At the federal level, there are several bills currently pending in Congress aimed at addressing minors' privacy, including the Children and Teens' Online Privacy Protection Act ("COPPA 2.0") (https://bit.ly/473FXJm) and Kids Online Safety Act ("KOSA") (https://bit.ly/4l2rIdL), along with a set of minors-related bills currently being considered by the House Subcommittee on Commerce, Manufacturing, and Trade.

Foreign Transfers of Personal Data. As a continuation of the U.S. Department of Justice's (DOJ) Data Security Program Rule, which took effect (https://bit.ly/40EYMio) in 2025, it is possible that privacy regulators will continue to scrutinize transfers of personal data — particularly sensitive data — outside of the United States. The FTC has also indicated it plans to increase enforcement of the Protecting Americans' Data from Foreign Adversaries Act of 2024 (https://bit.ly/4aLZHUj), which prohibits sale of personally identifiable sensitive data to certain recipients.

New State Comprehensive Privacy Laws and Regulations. A number of state legislatures have carried over bills from the prior legislative session or introduced new comprehensive privacy laws early in 2026, including Maine, Massachusetts, Mississippi, and South Carolina. Some of these bills propose models that are similar to existing state privacy statutes.

However, others include notable and different obligations, such as South Carolina's proposed novel portability requirements for social media services. It is also likely that the 2025 trend to amend existing privacy laws will continue into 2026 as states incorporate changes to existing laws to mirror frameworks in effect.

Algorithmic Pricing. Following New York's lead in passing an algorithmic pricing disclosure requirement (https://bit.ly/3N8ZSQm) into law in 2025, other legislatures could focus on targeting algorithmic pricing. For example, Kentucky has already introduced (https://bit.ly/4rWx6S0) an amendment to its comprehensive privacy statute that would include heightened requirements for "surveillance pricing," and Maryland (https://bit.ly/3MU5myo) is looking at this issue as well. It is likely that other states continue to propose legislation and make algorithmic pricing a focus in 2026.

Sensitive Data. Lawmakers may continue to focus on the sale or disclosure of sensitive data in passing or amending privacy statutes in 2026. Already this year, legislatures have introduced proposals to limit the use and disclosure of sensitive data. For example, California Assembly Member Chris Ward has introduced AB 1542 (https://bit.ly/4aNLAxO), which would amend the CCPA to add that "[a] business, service provider, or contractor shall not sell or share sensitive personal information to a third party."

It is possible that the emphasis on sensitive data could be mirrored at the federal level, as the FTC announced (https://bit.ly/4u61cE6) a settlement with General Motors early this year to resolve allegations that precise geolocation and car driving data was collected and used without adequate consent.

California's Updated CCPA Regulations. Several updates (https://bit.ly/4u5RPVc) to the California Consumer Privacy Act (CCPA) took effect January 1st. For example, businesses must confirm consumer opt-out requests, including those submitted through preference signals like Global Privacy Control, by providing clear indicators such as confirmation messages or toggles in privacy settings.

Consumers are also now able to request access to personal information retained for more than 12 months, dating back to January 1, 2022, and when correcting data obtained from other sources, businesses must disclose the source and ensure corrections remain accurate.

About the authors




(L-R) **Libbie Canter** is vice chair of **Covington& Burling LLP**'s data privacy and cybersecurity practice. She can be reached at ecanter@cov.com. **Jayne Ponder** is an associate in the firm's data privacy and cybersecurity practice. She can be reached at jponder@cov.com. **Jenna Zhang** is an associate in the data privacy and cybersecurity practice at the firm. She can be reached at jzhang@cov.com. **Clare Mathias** is an associate in the data privacy and cybersecurity practice group at the firm. She can be reached at cmathias@cov.com. Canter and Ponder are based in Washington, D.C., Zhang is based in San Francisco, and Mathias is based in Boston. The authors would like to thank partner Lindsey Tonsager for contributing to this article.

This article was first published on Westlaw Today on March 5, 2026.