A New Era of US Privacy Enforcement Has Only Just Begun: 2025 Trends and Outlook for 2026 and Beyond

JANUARY 21, 2026

D. REED FREEMAN JR., MICHELLE R. BOWLING, ANDREA M. GUMUSHIAN, JOHN M. KEBLISH

2025 was one of the most active years in recent memory for US state-level privacy enforcement. California and Texas led the way, and we anticipate Colorado, Connecticut, Maryland, Minnesota, Oregon, and New Jersey to emerge as active enforcers in 2026.

A growing, bipartisan group of state enforcers coordinated in 2025, notably on Global Privacy Control (GPC) sweeps. Looking ahead to 2026, we expect most 2025 trends to continue and expect states to enforce the signature issues highlighted in their new or amended privacy laws. This includes Maryland's rules on data minimization, Connecticut's new children's privacy regime, Colorado's new biometric rules, Minnesota's and Oregon's specific third-party disclosure requirements, , and New Jersey's focus on risk assessments and teens. Across states, the most prominent issues are likely to be opt-out compliance (especially GPC), children's privacy, sensitive data (health, location, biometric), risk assessments, vendor contract provisions, and compliant privacy policies.

2025 Enforcement Priorities: What Regulators Targeted

In 2025, state privacy enforcers prioritized user choice integrity (eliminating dark patterns and

friction), universal opt-out signal recognition, including the GPC across web and app ecosystems, data broker registration and governance under California's Delete Act, children's and teens' protections, and compliant privacy notices. The states making up the new privacy consortium entered into a memorandum of understanding to share expertise and to coordinate efforts to investigate and enforce violations collectively. This is reminiscent of the data breach enforcement framework in the 2010s, which resulted in significant multistate enforcement activity, and we expect the same to emerge for privacy now.

Below are the most notable areas of focus for regulators in 2025.

1. Dark Patterns

Dark patterns are user-interface designs that manipulate consent in data collection, tracking, or purchases. California's regulators brought first-of-kind California Consumer Privacy Act (CCPA) actions against "choice asymmetry," which is a type of dark pattern where the choice to opt-out is significantly more difficult than consenting. User interface design was a priority for regulators who scrutinized pre-ticked or allegedly visually biased toggles and alleged unnecessary friction in consumer rights workflows. Penalties and orders also required redesign of consent banners and workflows, parity of choices, and GPC honoring across channels. Two enforcement actions involving an automotive original equipment manufacturer and a clothing designer resulted in civil penalties of approximately $632,500 and $345,000, respectively, along with orders to redesign user-interfaces to provide choice parity.

2. Universal Opt-Out (GPC)

Regulators emphasized signal detection, cross-device and app honoring of GPC signals, and downstream acknowledgement of such preferences. Joint investigations reinforced states' position that deception can arise when banners falsely imply recognition of GPC opt-out signals. One settlement included a $1.55 million penalty and required cookie banner redesigns and documented honoring of GPC across properties.

3. Data Broker Registration and Delete Act Compliance

California's CPPA reviewed its data broker registry and initiated compliance sweeps that yielded fines and injunctions. Strict enforcement is likely to continue with the 2026 DROP workflows and penalties for unfulfilled deletion cycles. Recent enforcement actions included penalties of $55,800, $46,000, and $55,400 for alleged registration failures, and one order requiring a multi-year shutdown for persistent noncompliance. DROP compliance will be required beginning on August 1, and we expect enforcement to continue on registration and opt-out compliance throughout the year, with fines continuing to escalate. Note that the data broker registration deadline for 2025 activities is January 31.

4. Children's and Teens' Data and Purpose Limitation

States scrutinized consent in data collection of children under the age of 13 and new advertising and sales limitations on teens (13-17 years old). Many state statutes impose stricter compliance obligations (such as opt-in consent for selling or sharing teens' data, prohibitions or opt-in requirements for targeted advertising to minors, and age verification) than the baseline protections imposed by the Children's Online Privacy Protection Act. The attorney generals of California, Connecticut, and New York collectively imposed $5.1 million in penalties and mandated consent, data deletion, and data minimization controls on an ed-tech business for failing to employ reasonable and appropriate measures to protect personal information. The California Attorney General (AG) fined a gaming company $1.4 million for sharing and selling the data of children

between the age of 13 to 16 without the affirmative consent required by the CCPA.

5. Location, Biometrics, and ACR Devices

The Texas AG challenged alleged persistent and undisclosed location tracking, biometric capture without valid consent, and collection of TV viewing data using automated content recognition (ACR) on smart TVs as violations of Texas consumer protection law. This ACR enforcement action was the first since the Federal Trade Commission brought its case against a smart TV manufacturer in 2017, and we expect this new focus on smart TV data collection to continue in 2026 and beyond. While these smart TV cases are in active litigation, Texas' AG obtained a $1.4 billion settlement and temporary restraining orders halting certain tracking and data collection practices. Even states similarly scrutinized television providers for collecting personal data via ACR.

6. Privacy Notices and Rights Mechanisms

Investigations focused on whether disclosures actually map to processing (including third-party sharing and targeted advertising), whether "do not sell/share" toggles are obvious and accurate, and whether appeals to access, correct, or delete requests are functional and timely. One enforcement action imposed an $85,000 penalty and required remediation of privacy notices and consumer rights pathways. Another enforcement action alleged that a retailer failed to inform California consumers of their privacy rights in their privacy policy, resulting in a $1.35 million settlement.

7. Vendor Contracts

Contractual oversight with third parties remains a focus. The CCPA and every other state comprehensive privacy law require businesses that share data with third parties to have several explicit provisions to ensure consumer protection. The California AG and CalPrivacy alleged that entities failed to craft contracts that meet the CCPA's requirements, resulting in settlements of $1.35 million and $1.55 million.

Early 2026 Priorities: State-By-State Focus Areas

We expect 2025 enforcement topics to continue in 2026. In addition, we expect the state 2026 enforcement priorities to include the following:

- **California:** Expect aggressive audits and inquiries around GPC, manual opt-outs, adequate service provider contracts, the sale of children's data, and data broker registration, vendor contract compliance, and Delete Act and DROP compliance. The AG and CalPrivacy stated they are pursuing hundreds of open investigations. Multistate GPC sweeps will continue. Regulators are actively using website scanning technology to police compliance.

- **Colorado:** Colorado amended its privacy law last year to include strict new notice, consent, retention, deletion, and breach response rules for biometric data, and we expect aggressive enforcement on these requirements in 2026. Enforcement always follows new regulations, and we see no reason to doubt that here. Expect Colorado to also continue to lead the charge on identifying acceptable universal opt-out mechanisms beyond the GPC, and to focus on enforcement around honoring their signals.

- **Connecticut:** The Connecticut AG has also suggested that legislators enhance the state's data minimization standard, citing that in many cases, "serious privacy and data security

concerns could have been offset, if not fully alleviated, if companies had properly minimized the data they collected and maintained." Additionally, universal opt-out signal recognition started this month, so expect regulators to scrutinize how these technologies are implemented and how they function on your website. Connecticut updated its privacy laws to add significant new protections for minors, including stricter consent requirements and new limits on how companies can process or target the personal data of teens aged 13-17. Enforcement will follow.

— **Maryland:** Maryland's new comprehensive privacy law, effective October 2025 and applicable for data collected beginning April 2026, is among the strictest, prohibiting the sale of sensitive personal information, barring the sale of personal data and targeted advertising to minors under 18 when the business knows or should know the consumer's age, and imposing strict data minimization requirements. We expect data minimization inquiries and scrutiny of how and when businesses collect personal data from minors, or other sensitive personal data, to increase this spring.

— **Minnesota and Oregon:** Minnesota and Oregon require controllers to disclose lists of specific third parties to whom personal data have been disclosed, upon request. These requirements are unique to these states, and we expect enforcement on them. Right-to-cure sunsets hit this year on January 1 for Oregon and January 31 for Minnesota, allowing enforcement to proceed. Oregon's GPC requirement also took effect on January 1 this year. We expect regulators in these states to look for low hanging fruit and scrutinize website disclosures and technical compliance with GPC requirements.

— **New Jersey:** Draft regulations are expected to be finalized sometime this year, although there may be delays given the change in the state's administration. We expect new final regulations to address automated decision-making and risk assessments, among other things. We think enforcement will begin later this year, with an emphasis on ADMT transparency and consent design.

— **Texas:** Texas will almost certainly continue aggressive enforcement in 2026, with a focus on location data, biometric data, and connected ACR tied to broader national security narratives. The Texas AG will likely continue to focus on online advertising and tracking, connected vehicles, and precise geolocation, including automotive-adjacent data broker channels.

For more information or help on a particular matter, please reach out to your AFS contact or a member of the **Privacy and Data Security** team.

Additional research and writing from Perry Jackson, law clerk in ArentFox Schiff's Washington, DC, office.

Contacts

D. Reed Freeman Jr.

PARTNER

Michelle R. Bowling

SENIOR ASSOCIATE

Andrea M. Gumushian
ASSOCIATE

John M. Keblish
ASSOCIATE

Related Practices

Privacy & Data Security

Continue Reading

PRIVACY COUNSEL

New Year, New Privacy Obligations

DECEMBER 19, 2025 | D. REED FREEMAN JR., MICHELLE R. BOWLING, ANDREA M. GUMUSHIAN, JOHN M. KEBLISH

PRIVACY COUNSEL

New State Privacy Laws – Second Half of 2025

JULY 29, 2025 | D. REED FREEMAN JR., ANDREA M. GUMUSHIAN, MICHELLE R. BOWLING

23andMe and the Role of Privacy in Bankruptcy Law

MAY 21, 2025 | D. REED FREEMAN JR., CAROLYN INDELICATO