VENABLE LLP

State Quick Hits: California Enacts New Privacy Laws as Other States Expand Data Privacy Regulations and Enforcement Focus

October 09, 2025

Michael A. Signorelli, Allaire Monticollo and Rob Hartwell

California Governor Gavin Newsom (D) has signed into law several bills imposing new privacy obligations on businesses that handle personal information. These measures, together with the ever-growing patchwork of state privacy laws across the country, including the California Consumer Privacy Act (CCPA), show that the pace of new requirements will not slow down anytime soon.

California's New Privacy Requirements

Three recently enacted California privacy laws impose distinct obligations on businesses handling personal information.

- **AB 566**: **Opt-Out Preference Signals.** Starting January 1, 2027, all web browsers will need to include functionality for Californians to send an opt-out preference signal to businesses they visit online through the browser. This law follows the California Privacy Protection Agency (CPPA) announcement of a joint investigative sweep with privacy enforcers in Colorado and Connecticut to investigate potential noncompliance with the Global Privacy Control.
- **SB 361: Expanded Data Broker Disclosures.** Effective January 1, 2026, data brokers will be required to disclose in their annual registration with the state whether they collect certain data elements, such as MAIDs, CTV IDs, and VINs. The law also requires data brokers to disclose whether they have shared or sold data to a foreign actor, the federal government, other state governments, or a developer of a GenAI system or model in the past year.
- **AB 45: Geofencing and Health-Related Location Privacy.** Also effective January 1, 2026, under AB 45 it will be unlawful to collect, use, disclose, sell, share, or retain personal information about individuals physically located at, or within 1,850 feet of, a family planning center, except when necessary to provide requested services. The law also prohibits geofencing locations that provide in-person healthcare services to identify, track, or collect personal information from the person seeking services, from sending advertisements related to a person's health or personal information, or sending notifications about the individual's personal information or health services.

Evolving State Privacy Law Landscape

California's new requirements emerge within an accelerating and increasingly complex state privacy environment. The Maryland Online Data Privacy Act (MODPA), for example, took effect on October 1, 2025, granting Maryland residents new privacy rights imposing novel data-minimization obligations on controllers operating in the state. In addition, beginning January 1, 2026, omnibus privacy laws in Rhode Island, Indiana, and Kentucky will take effect, while Connecticut, Montana, and Oregon have amended existing statutes this year to expand consumer rights and add more compliance duties. Separately, Virginia has amended its Consumer Protection Act to prohibit the use or disclosure of personally identifiable reproductive or sexual health information without consent, with a private right of action available for violations.

These developments come in the wake of a recent announcement that state attorneys general in Minnesota and New Hampshire have joined the Consortium of Privacy Regulators (Consortium), a multistate initiative first unveiled in April 2025 to coordinate state enforcers' efforts to investigate potential violations of applicable privacy laws. Other members of the Consortium include the CPPA and state attorneys general of California, Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon. State regulators are coordinating, so while California has been the most active enforcer so far, the others are likely not far behind.

Key Takeaways for Businesses

- **Plan for Universal Opt-Out Signals:** Businesses should ensure they are able to recognize and honor browser-based opt-out preference signals where required.
- **Consider New Data Broker Registration Requirements:** Data brokers in California should prepare to disclose new information about their data collection practices when registering in 2026. California has a broader definition of "data broker" than any other state, so businesses should determine whether these requirements cover their activity.
- **Prepare for Multi-State Compliance:** With Maryland's law in effect and more states coming online in 2026, a unified, scalable compliance framework is increasingly essential.
- **Monitor Enforcement Risk:** Increased coordination among state privacy enforcers, Virginia's new reproductive data protections with a private right of action, and California's recent enforcement actions heighten potential exposure for businesses operating nationwide.

Businesses should move quickly to update privacy compliance programs and adopt adaptable strategies for an increasingly complex patchwork of state privacy laws. If you need assistance reviewing or developing a privacy compliance program, contact the authors or visit Venable's Privacy and Data Security center to help ensure your organization is prepared.