Navigating State Privacy Laws: Key Developments and What to Expect in 2026

January 22, 2026

Emma Blaser
Partner | ERBlaser@Venable.com

Arlyn Upshaw
Associate | AMUpshaw@Venable.com

Nana Abrefah
Associate | NAAbrefah@Venable.com

VENABLE LLP | 125 YEARS young

Agenda

- Update on CCPA Regulations
- Cookie Banners
- App Store Accountability Laws
- Update on California Delete Act Implementation
- Looking Ahead: Enforcement Priorities

VENABLE LLP | 125 YEARS young

Updates on CCPA Regulations

New and Amended Requirements

VENABLE LLP | 125 YEARS young

Updated CCPA Regulations

- Amendments to CCPA regulations include new obligations regarding:
  - **Risk assessments** for certain processing activities;
  - **Cybersecurity audits; and**
  - **Automated decisionmaking technology ("ADMT").**

- The amended regulations were effective as of January 1, but companies have additional time to comply with certain requirements, including related to the above new obligations.

- The amendments also clarified or changed existing rules, including rules regarding:
  - Confirming whether an opt-out has been processed;
  - Dark patterns, including what does not constitute sufficient consent or symmetry in design (e.g., for cookie banners, opt-outs, financial incentives); and
  - Provision of notices for information collected through connected devices.

VENABLE LLP | 125 YEARS young

When to Conduct CCPA Risk Assessments

- Risk assessments must be conducted if processing presents a "**significant risk to consumers' privacy**," which means:
  - Selling/sharing personal information;
  - Processing sensitive personal information;
  - Using ADMT for a significant decision concerning a consumer;
  - Using automated processing to infer or extrapolate certain characteristics of personnel and certain others;
  - Using automated processing to infer or extrapolate certain characteristics based on presence in a "sensitive location" (excluding use of personal information solely to deliver goods to or provide transportation for a consumer at a sensitive location); and
  - Processing personal information that is intended to be used to train ADMT for significant decisions or train facial recognition, emotion recognition, or identity verification technology.

- The first risk assessments (regarding processing prior to January 1, 2026, that continues after that date) must be completed by **December 31, 2027**.

VENABLE LLP | 125 YEARS young

CCPA Risk Assessments

- Risk assessments must describe **details of data processing** and identify **benefits** and "**negative impacts**" of processing as well as **safeguards** for the processing activities covered.

- Regulations require:
  - Short windows to update assessments following material changes in processing (45 days);
  - Submission to CalPrivacy of information about a company's risk assessments; and
    - A member of the executive management team must submit the information and certify the information's correctness under penalty of perjury.
  - CalPrivacy and the California AG can request a risk assessment report at any time (not just in connection with a CID or formal investigation).

VENABLE LLP | 125 YEARS young

CCPA Cybersecurity Audits

- Must be conducted if a business:
  - Derives 50% or more annual revenue from selling/sharing personal information; or
  - Has annual gross revenues > $26,625,000 and (1) processed personal information of 250K+ consumers/households in last calendar year, or (2) processed sensitive personal information of 50K+ consumers/households in last calendar year.

- First audits must be completed **by April 1, 2028, 2029, or 2030** depending on annual revenues ($100+, $50-100, and below $50 million, respectively). Then, annual audits are due by April 1 each year.

- The audit must assess how a cybersecurity program: (1) protects against unauthorized access, destruction, use, modification, or disclosure; and (2) protects against unauthorized activity resulting in the loss of availability of personal information. The regulations include detailed requirements for assessment scope.

- Certifications of completion must be submitted annually by a member of the executive team, who must attest to the certification's correctness under penalty of perjury.

VENABLE LLP | 125 YEARS young

Automated Decisionmaking Technology

- Amended CCPA regulations impose obligations on businesses that use ADMT for "significant decisions."
  - "ADMT" means "any technology that processes personal information and uses computation to **replace** human decisionmaking **or substantially replace** human decisionmaking."
  - A "**significant decision**" is "a decision that results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services."

- By **January 1, 2027**, businesses using ADMT for significant decisions must:
  - Provide consumers **notice** that includes the rights to opt out of ADMT processing and to access ADMT and information about how the ADMT works, among other specified disclosures;
  - Allow consumers (or their authorized agents) to **opt out of the use of ADMT** for significant decisions, subject to exceptions; and
  - Disclose information about use of ADMT in response to consumers' **requests to access** regarding ADMT.

VENABLE LLP | 125 YEARS young

Cookie Banners

Litigation Considerations and State Law Opt-Out Rights

VENABLE LLP | 125 YEARS young

Background on Cookie Banners and Wiretap Litigation

- **Recent litigation has leveraged wiretapping/eavesdropping statutes** to target collection, use, and sharing of personal information via third-party cookies.
  - For example, cases have commonly been brought under the California Information Privacy Act and Pennsylvania's Wiretapping and Electronic Surveillance Control Act.

- U.S. law does not expressly require cookie banners, but banners may reduce litigation risk.
  - Cookie banners may help to establish **express or implied consent** to data processing by third-party cookies. This consent may serve as a defense to wiretapping claims.
    - ***Express consent*** requires an affirmative action by the consumer (such as an "I agree" button), so it involves more friction.
    - ***Implied consent*** occurs when the consumer receives a meaningful advance notice and subsequently proceeds with the communication — such as when the consumer hears a notice about call recording and continues with the call anyway.

Cookie Banners and State Law Opt-Out Rights

- Implementing a cookie banner does not obviate the need to offer an opt-out to consumers under the state omnibus privacy laws, but may impact the design of, and options available on, any cookie banner the business chooses to implement.

- State regulators increasingly expect **symmetry of choice** in cookie banners, so companies should consider offering a "Reject All" option if an "Accept All" option is presented.
  - However, companies should also be careful not to overstate the scope of the rejection option.

- If using an implied consent banner, this consent does not override previous sales/sharing/targeted advertising opt-outs from the consumer.

VENABLE LLP | 125 YEARS young

Compliance Considerations for Cookie Banners

- **Express or implied.** Consider which consent approach to adopt for cookie banners.
  - If using implied consent, a separate opt-out for sales/sharing is likely required.
  - If using express consent, balance litigation concerns with opt-out/consent requirements.

- **Determine cookie-based sales/sharing.** Examine whether your business sells, shares, or processes personal information for targeted advertising through any means other than cookies.
  - If no, consider designing cookie preference tools to align with state law opt-out requirements.
  - If non-cookie-based sales exist, a cookie banner (and any cookie notices) should avoid representing that the cookie banner is a complete state law opt-out method.

- **Ensure consistency among notices.** Review disclosures in the privacy policy and the cookie banner to ensure they are aligned.

VENABLE LLP | 125 YEARS young

App Store Accountability Laws

Overview and Compliance Requirements for App Developers

VENABLE LLP | 125 YEARS young

App Store Accountability Laws: Overview

- New "app store accountability" laws enacted last year in **California, Louisiana, Texas, and Utah** include broad, novel obligations on app stores and app developers related to age verification and parental consent.
  - Texas's law was slated to go into effect this month, but a federal judge paused enforcement on First Amendment grounds.
  - The other three laws are set to take effect over the next year, barring similar injunctions.

- In general, app stores will need to verify a user's age when creating an account and obtain parental consent for app downloads and purchases by **any user under 18**.

VENABLE LLP | 125 YEARS young

App Developer Compliance Obligations

- All app developers — not just developers of apps directed to minors — should prepare for compliance.
  - In certain states, app developers will be required to request age category and parental consent information from app stores for each app download and purchase.
  - App developers will need to have systems in place to appropriately handle any age category and parental consent information received from app stores.

- Additionally, developers should prepare to use age category information to comply with age-related requirements under other privacy laws, such as:
  - Obtaining verifiable parental consent under the Children's Online Privacy Protection Act ("COPPA") for users under 13;
  - Obtaining consent from teens for targeted advertising (or ceasing sales of teen data or processing teen data for targeted advertising) under certain state privacy laws; and
  - Applying necessary restrictions and protections to any data collected from children and teens to comply with COPPA and state privacy laws.

VENABLE LLP | 125 YEARS young

Compliance Steps for App Developers

- **Assess applicability** of app store accountability laws and determine whether any mobile or online apps may be subject to the new requirements.
- **Evaluate applicable obligations** in each relevant state. Note that there are variations in specific developer obligations across the four states.
- **Implement infrastructure** to receive age category and parental consent information from app stores. App stores have released age-signal APIs that can make this information available to developers.
- **Update internal processes** to prepare for verification requirements and, when necessary, implement age-related protections for users who are identified as under 18.

VENABLE LLP | 125 YEARS young

Update on California Delete Act Implementation

Requirements for California Data Brokers

Background on the California Delete Act

- The California Delete Act directs the California Privacy Protection Agency ("CalPrivacy") to create a centralized deletion mechanism, allowing California consumers to submit data deletion requests to all registered data brokers.

- Under California law, a "data broker" is defined broadly as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.

- Starting **August 2026**, data brokers will need to access the Delete Request and Opt-out Platform ("DROP") established by CalPrivacy and process consumer deletion requests every 45 days.
  - The DROP is expected to contain lists of consumer-provided information, including names, DOBs, zip codes, email addresses, phone numbers, mobile advertising IDs, connected TV IDs, and vehicle identification numbers.

- CalPrivacy has signaled that it intends to be active and aggressive in enforcing the Delete Act, launching a "Data Broker Enforcement Strike Force" to investigate potential violations of data broker requirements.

VENABLE LLP | 125 YEARS young

Update on Delete Act Implementation

- In late 2025, CalPrivacy adopted implementing regulations addressing the accessible deletion mechanism and requirements for data brokers.

- Key obligations imposed under the regulations include:
  - Accessing the DROP and downloading new consumer deletion lists every 45 days;
  - Standardizing and hashing information in the data broker's records in accordance with specific guidelines, and then comparing with consumer requests submitted through the DROP;
  - Deleting non-exempt matched records and associated personal information;
  - Applying sales opt-outs to certain data (such as when a matched identifier is associated with multiple consumers); and
  - Reporting the status of consumer requests as "deleted," "opted out of sale," "exempted," or "not found."

- This month, the DROP became available to California consumers to begin submitting requests ahead of the August 1, 2026, compliance date for data brokers.

VENABLE LLP | 125 YEARS young

Looking Ahead: Enforcement Priorities

What to Expect in 2026

What to Expect from Enforcement in 2026

- **Continued coordination among regulators**
  - As more state laws have gone into effect, and regulators seek to enforce while balancing resource constraints, regulators build on each others' work.
  - Last year, privacy regulators in nine states announced the creation of a bipartisan consortium to coordinate efforts to investigate potential privacy violations.
  - California, Colorado, and Connecticut regulators launched a joint privacy sweep focused on state privacy compliance and honoring consumer opt-out requests.

- Continued focus on **consumer rights**, including opt-out rights and cookie banners
  - Public-facing issues often garner initial scrutiny and can lead regulators to look "under the hood." For example, a faulty opt-out mechanism that relies in part on a vendor may encourage regulators to review a business's contracts.
  - California regulators have been particularly active on this topic, and we expect them to continue to enforce in this space.

VENABLE LLP | 125 YEARS young

What to Expect from Enforcement in 2026

- **Children's privacy**
  - Remains a priority for state and federal stakeholders, and we have seen some state regulators (e.g., Kentucky and Utah) kick off public enforcement of their privacy laws with children's privacy-focused actions.

- **"Sensitive" data and differing approaches**
  - Health and location data remain focal points.
  - California enforcement has focused on health-related data without expressly applying standards applicable to sensitive health data.
  - States like Maryland have also taken different approaches to sensitive data requirements. We may see regulators flesh out how they will treat such data under their respective laws.

VENABLE LLP | 125 YEARS young

What to Expect from State and Federal Enforcement in 2026

- **AI and automated decision-making**
  - New laws and regulations are in effect (e.g., California and Texas).
  - AI use can intersect with other priority enforcement areas, such as children's privacy and use of sensitive data.
  - On December 11, 2025, President Trump issued an Executive Order titled "Ensuring a National Policy Framework for Artificial Intelligence," which calls for development of a "uniform Federal regulatory framework for AI" and an evaluation of existing state law requirements (among other items).

VENABLE LLP | 125 YEARS young