HINSHAW

Alerts

Fall 2025 Regulatory Roundup: Top U.S. Privacy and AI Developments for Businesses to Track

September 23, 2025
Privacy, Cyber & AI Decoded

Welcome to our early Fall 2025 edition of Hinshaw's *Privacy, Cybersecurity, & AI Decoded*.

In this edition, we highlight key privacy enforcement actions, regulatory changes, and new AI laws and policies.

Federal AI Action Plan

The Trump Administration's AI Action Plan (the "Plan") was released by the White House on July 23, 2025, with the goal of providing a national strategy to increase the development of AI in the United States.

The Plan consists of over 90 policy recommendations for federal agencies to consider, which are organized under three pillars:

1. Accelerating AI Innovation;
2. Building American AI Infrastructure; and
3. International AI Diplomacy and Security.

Under The Plan, the following items will be critical for businesses to monitor:

- the further development of national standards for AI governance under the National Institute of Standards and Technology (NIST);
- the establishment of regulatory sandboxes or AI Centers of Excellence around the country, where researchers, startups, and established enterprises can rapidly deploy and test AI tools while committing to open sharing of data and results; and
- the creation of an AI cybersecurity threat information sharing program.

Attorneys

Kelechi Ajoku

Sabrina Janeiro

Cathy Mulrow-Peattie

Claire Standish

Service Areas

Privacy, Security & Artificial Intelligence

California: Privacy Developments

California Announces Joint Enforcement Action on Global Privacy Control

On September 9, 2025, California Attorney General Rob Bonta, the California Privacy Protection Agency (CPPA), and the attorneys general of Colorado and Connecticut announced a joint investigative action involving potential noncompliance with the Global Privacy Control (GPC).

GPC is a browser setting or extension that automatically signals to businesses a consumer's request to stop selling or sharing their personal information to third parties. This action reiterates the enforcement priorities of California, Colorado, and Connecticut to require the implementation of GPC and other consumer opt-out and data subject rights requirements of state privacy laws and their promise on collective privacy actions.

People of the State of California vs. Healthline

On July 1, 2025, the California Attorney General's Office announced a record-setting $1.55 million settlement with Healthline Media, a provider of health and wellness information and operator of Healthline.com, a website where consumers can read informational articles about medical and health topics.

The Attorney General alleged that Healthline.com violated the California Consumer Privacy Act (CCPA) and the California Unfair Competition Law by sharing personal health data of consumers and failing to properly implement opt-out mechanisms for targeted advertising to third-party advertisers.

The settlement marks the first major privacy enforcement in the healthcare space that focuses on the law's purpose-limitation requirement. The Attorney General's office emphasized that businesses must ensure their privacy practices accurately align with their disclosures, that their opt-out mechanisms work consistently, and that any secondary use of personal data must align with the "reasonable expectations of the consumer" to satisfy the CCPA's purpose limitation requirement.

While this settlement specifically impacts businesses in the healthcare field, other businesses subject to the CCPA and similar state privacy laws should also take note of this settlement as an example of how state regulators may enforce violations of such laws.

California's Continued Enforcement Against Data Brokers

The CPPA is aggressively enforcing the Delete Act's data broker registration requirements, having already initiated eight enforcement actions. Recently, a Washington-based company was fined $55,400 and subjected to injunctive relief for failing to register as a data broker and pay the annual fee. This enforcement follows several data broker actions by the CPPA this year.

Critically, the amended data broker regulations, approved in December 2024, broaden the definition of **"data broker"** to include businesses that collect and sell a consumer's personal information to third parties who did not intend to interact with the business.

The amendments further clarify that a business remains a data broker even when it maintains a direct relationship with the consumer, but also sells personal information about that consumer that the business did not acquire directly from the consumer. Many brands and companies in advertising could fall within this definition.

Companies that collect, use, or sell a consumer's personal information should promptly assess whether it qualifies as a data broker and ensure full compliance with the Delete Act to avoid costly fines. These violations could include penalties of up to $200 per day, in addition to the costs of registration and the CPPA's investigation and enforcement efforts, and reputational damage by registering in California's Data Broker Registry and complying with all requirements under the Delete Act.

Several New California AI Bills

The California legislature has approved several AI bills related to transparency, healthcare, chatbots, and employment, which are currently before Governor Newsom for review. Governor Newsom has vetoed and approved various AI bills in the past. We will update readers on those bills once the Governor has taken action.

Colorado: Automated Decision-Making Technology and High-Risk AI

On August 28, 2025, Governor Polis (D) signed SB-4, a bill to delay implementation of the Colorado AI Act by five months, moving the effective date back from February to **June 30, 2026.**

Companies that are deployers or developers of AI and that are subject to the requirements of the Colorado AI Act should continue to move forward with compliance efforts, but now have more time to do so.

Maryland, Oklahoma, and Oregon: Regulatory Happenings

Maryland's Online Data Protection Act

As a reminder, the Maryland Online Data Protection Act goes into effect on **October 1, 2025**. Read more about the law as discussed in this September 2024 alert.

Oklahoma's Request for Proposal

On September 12, 2025, Oklahoma's Attorney General issued a request for outside counsel to investigate Temu's transfer of Oklahoma residents' personal data to China as a deceptive trade practice. Temu, a mobile application and website, allows users to purchase low-cost goods manufactured in China.

Ultimately, Temu is owned by a Chinese company, PDD Holdings, Inc., commonly known as Pinduodo Inc. This action extends regulatory concerns over the transfer of sensitive data to China to the state level. Read more about the federal bulk sensitive data rules as discussed in our July 2025 alert.

Oregon Consumer Privacy Act

On July 1, 2025, the Oregon Consumer Privacy Act (OCPA) went into effect for 501(c) (3) organizations.

On September 28, 2025, with the passage of HB 3875, the OCPA will now apply to motor vehicle manufacturers and their affiliates that control or process personal data from a consumer's use of a vehicle or its components in Oregon.

As a reminder, Oregon's 30-day cure period sunsets, and universal opt-out requirements begin on **January 1, 2026**. This may impact dealerships and other related entities in Oregon, which should review their privacy notices, contracts, and training materials to ensure compliance with the OCPA.

We also note that the Oregon Attorney General's August 2025 enforcement report states that they investigated 90 consumer complaints in the law's first year of enforcement. Many of the complaints claimed a violation of the OCPA provision, which allows consumers to request a list of entities to which their personal data was disclosed, including sales of consumer data. This means companies failing under the OCPA should update their data inventory and related service provider/third-party contracts to respond to these requests.