JENNER & BLOCK

State Consumer Privacy Enforcement Update: Fall 2025

Client Alerts

October 31, 2025
By: Madeleine Findley, Xinyue Lu, Joshua Petersen

With federal privacy enforcement increasingly limited, state regulators have stepped forward as consumer privacy enforcers. This year may have offered a reprieve from the rapid adoption of new state consumer privacy laws seen in 2023 and 2024, but privacy enforcement activity has accelerated steadily and is poised to grow even more. In fact, yesterday the California Attorney General announced a $530,000 settlement with Sling TV arising from an investigative sweep into compliance with California's requirements to provide consumers with a way to opt out of the sale of their personal information. In this article, we review the latest in state consumer privacy protection enforcement, particularly the emphasis on coordination and collaboration among states, and discuss other emerging trends as companies work to navigate this changing compliance landscape.

States Are Formalizing Joint Efforts in Privacy Enforcement

This year has marked a notable new development in state privacy enforcement: formal coordination between regulators across the country. Although state regulators have long shared information and coordinated on a more or less informal basis, particularly in connection with large-scale data breaches, this year marked a shift to formal privacy enforcement collaboration. In April 2025, regulators from California, Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon formed the Consortium of Privacy Regulators to share expertise and resources and coordinate enforcement. In October, Minnesota and New Hampshire joined the consortium, meaning almost half the states with comprehensive consumer data privacy laws are formally working together. This consortium marks a significant milestone in cross-state regulatory coordination and collaboration.

Opt-Out Rights Continue to Be a Top Priority, with a Renewed Focus on Universal Opt-Out Signals

Empowering consumers to exercise control over how their personal data is used—and particularly how it is used in advertising targeted to them—has been a driving force in state consumer privacy laws since the genesis of the California Consumer Privacy Act. This year has continued that effort. For example, in March, Oregon reported that within the first six months of the Oregon Consumer Privacy Act taking effect, it had issued 21 cure notices asking companies to correct alleged privacy notice deficiencies, including due to insufficient or absent opt-out mechanisms. In April,

Connecticut announced that it had conducted three "privacy notice sweeps" asking companies to, among other things, "bolster[], or fix[] consumer rights request mechanisms, including adding clear and conspicuous links to opt out of targeted advertising and the sale of personal data." And in July, Connecticut reached an $85,000 settlement with an online ticket marketplace after the company failed to cure multiple alleged violations, including privacy right mechanisms "that were misconfigured or inoperable."

In September, the California Privacy Protection Agency (CPPA) announced a $1.35 million settlement with Tractor Supply Company to resolve various alleged violations of the CCPA. The settlement alleged that Tractor Supply had failed to properly disclose consumers' California privacy rights in its privacy notice and failed to implement required privacy terms in contracts with its service providers. Notably, the settlement also alleged that Tractor Supply Company's opt-out mechanism on its website did not actually effectuate the opt-outs—underscoring the importance for companies of verifying that their systems are in fact operating as intended. Moreover, Tractor Supply Company's website allegedly failed to process opt-out preference signals, such as the Global Privacy Control (GPC). Finally, the CPPA asserted that Tractor Supply failed to notify job applicants of their privacy rights, a reminder that California does not exempt employee or job applicant personal information from the scope of the CCPA. On October 30, the California Attorney General announced a proposed settlement with Sling TV regarding the right to opt out. Specifically, the complaint and settlement alleged that Sling TV provided a confusing and difficult-to-access opt-out framework that did not in fact opt users out of sales of their information, made confusing disclosures, and required consumers to take multiple, burdensome steps to exercise their privacy rights.

Companies are seeing the effects of the new trend of joint enforcement discussed above collide with the prioritization of opt-out rights. In September, California, Colorado, and Connecticut announced a coordinated investigative sweep targeting businesses who have not implemented universal opt-out preference signals on their websites. Currently, GPC is the primary form of these types of signals. GPC is a technical standard that is available as a browser feature or extension, which allows a consumer to automatically send a request to websites they visit to opt out of selling or sharing personal information. While some websites have begun implementing GPC recognition, many businesses have not affirmatively adopted this standard. In fact, some companies have explicitly stated in their privacy policies that they do not recognize GPC. While some businesses have disclosed in their policies that they do not currently process such signals, this latest sweep suggests that at least these three states will begin pursuing enforcement on this specific issue more directly. And California recently upped the ante for businesses, passing the California Opt Me Out Act (AB 566), which will require browser developers to include an easy-to-find function enabling consumers to send an opt-out preference signal to businesses through their browsers.

States Regulators Have Focused on Dark Patterns in Interface Design

States also have shown increasing enforcement interest in website design features that are perceived to manipulate or undermine consumer choice, also known as "dark patterns." For

example, following its initial privacy notice sweeps, Connecticut has expanded its enforcement focus to include cookie banners and has issued cure notices regarding cookie banners that "undermine or even override consumers' ability to make important privacy choices, including the right to opt out of targeted advertising or the sale of their personal data through the use of tracking technologies." And Texas has brought claims under the Texas Deceptive Trade Practices-Consumer Protection Act against both an auto manufacturer and an auto insurance company, in the wake of a broader inquiry into the industry, relating to allegedly insufficient notices about their data collection and disclosure practices. Finally, California's CPPA imposed a $632,500 fine earlier this year on Honda Motor Co. for violations of the consumer's right to opt out based on the allegedly asymmetric nature of Honda's opt-out mechanism. California regulators took issue with the fact that Honda allegedly made opting out more difficult than sharing the data in the first place.

States Are Also Using Their UDAP Laws to Protect Consumer Privacy

Regulators in states, including those that have not enacted comprehensive consumer privacy statutes, are increasingly leveraging their existing unfair and deceptive trade practices laws to pursue actions regarding companies' allegedly insufficient data practices. For instance, in the last year, New York has settled or brought suit against four major auto insurance companies for alleged data privacy violations through its omnibus consumer protection law. Michigan filed a lawsuit in April against Roku, alleging that the streaming service provider collected and monetized personal data without consent. In July, Nebraska also filed a lawsuit against an auto manufacturer for allegedly mistreating sensitive data. And tying back to the deceptive or confusing interface prioritization, New York has signaled that if a website interface or default setting thwarts consumers' attempt to limit data processing, that could be deemed an unfair practice under its consumer protection law.

A New Frontier For Enforcement Through Purpose Limitations

Finally, California has begun examining compliance with the "purpose limitation" provision in the CCPA. This principle, analogous versions of which are also found in the Colorado Privacy Act and the Maryland Online Data Privacy Act, among others, requires that a business limit its use of personal information to the purposes for which the information initially was collected or processed or to another disclosed, compatible purpose "consistent with the reasonable expectations of the consumer." In July, California announced a $1.55 million settlement with Healthline Media LLC regarding its processing of health information. Of note, the complaint against Healthline alleged that its use of personal data for targeted advertising violated the purpose limitation provision of the CCPA. California claimed that Healthline violated this requirement by sharing that consumers had viewed article titles suggesting possible medical diagnosis—such as "The Ultimate Guide to MS for the Newly Diagnosed"—with "unseen advertisers and their vendors" while Healthline's privacy notice only "discussed targeted advertising briefly" and "never mentioned sharing article titles."

Key Takeaways:

As the year comes to a close, the latest data privacy regulatory actions have demonstrated a continued effort in key enforcement patterns and the emergence of new trends. Companies therefore should consider the following:

1. The recent formalization of coordination across states emphasizes the need for a considered and coordinated approach in responding to regulators. Companies should ensure that they take a harmonized approach to engaging with regulators and assume that states will collaborate and coordinate.

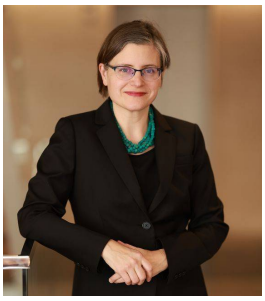
2. The focus on opt-out rights remains a top priority for regulators, and companies should regularly review their compliance mechanisms to ensure they function as intended. And given the renewed focus on universal opt-out preference signals, companies should be ensuring they are able to process such signals to avoid regulatory scrutiny.

3. Having a cookie consent manager can be a helpful tool in a privacy compliance program, but like any other opt-out tools, it is not foolproof and should not be used as the sole means of effectuating opt-outs. Moreover, companies should consider whether their cookie controls are understandable to consumers and ensure that they do not contain erroneous, confusing, or misleading representations or instructions. Recent enforcement actions illustrate that such mechanisms should be easy for consumers to access and should offer “symmetrical” choices for accepting or declining cookies.

4. Even in states that do not have comprehensive data privacy laws, companies should ensure their privacy notices remain consistent with their data practices. States have used general consumer protection laws as the basis for enforcement actions against companies for allegedly using and processing personal information out of step with what has been disclosed.

5. While there is convenience in using broad phrasing for required data processing disclosures in a company's privacy notice, doing so may be risky. As the recent Healthline settlement illustrates, overly generalized descriptions of processing purposes that omit details of specific processing activities risk a regulator determining that such activities were outside of the scope of the disclosure.

Related Attorneys



Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095

Xinyue Lu
Associate
xlu@jenner.com
+1 202 637 6376

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →