GOODWIN

ALERT · SEPTEMBER 12, 2025

Multistate Privacy Enforcement Sweep Puts Global Privacy Control in the Spotlight

BY Omer Tene Jacqueline Klosek Jonathan Ng Gabe Maldoff

Recent enforcement actions and announcements from the California Privacy Protection Agency (CPPA) and state Attorneys-General (AGs) in California, Colorado and Connecticut, and a California bill that passed the state legislature, signal a new phase of heightened enforcement, focused on honoring consumers' opt out requests, including through cookie banners and the Global Privacy Control (GPC).

Two critical developments stand out from our review of these actions and announcements: a crackdown on non-functional opt-out tools, highlighted by a multi-million dollar settlement and a multi-state investigative sweep; and a renewed emphasis on mandatory risk assessments for data "selling" and "sharing," including for online advertising practices that are commonplace.

Key Takeaways

- Recent enforcement actions, including a record-setting settlement with Healthline Media, demonstrate that the California AG and the CPPA are closely scrutinizing whether companies' technical implementations of cookie banners and universal opt-out mechanisms (UOOMs) actually work as advertised.
- Beginning January 1, 2026, businesses that sell or share personal information for cross-context behavioral advertising, a widespread industry practice, will be required to conduct and document a risk assessment, adding a new layer of compliance requirements.
- Companies should act immediately to test their UOOMS and other opt-out signal processing and begin to develop a framework for conducting and documenting risk assessments.

Regulators Demand Functional UOOMs and Opt-Out Tools

On September 9, 2025, California's AG General Rob Bonta and the CPPA's Executive Director, Tom Kemp, in coordination with the AG of Colorado, Phil Weiser and the AG of Connecticut, William Tong, announced a joint investigative sweep focused on enforcing the obligation to honor UOOMs, notably through implementation of the GPC.

A UOOM is a signal sent by a platform, technology or other mechanism that is designed to communicate a consumer's intention to opt out of the sale or sharing of personal information, or targeted advertising. Under the CCPA and several state privacy laws, businesses must recognize and act on a consumer's UOOM signal where the UOOM has been recognized and approved by the relevant state regulator. On September 11, 2025, the California legislature passed a bill that, if signed by the governor, will require all web browsers to offer UOOMs to consumers.

GPC is a UOOM that has been approved in California, Colorado, Connecticut and other states. When enabled in a browser, GPC allows users to communicate a legally binding preference to opt out of selling, sharing, and targeted advertising to websites they visit. . The coordinated enforcement effort signals that regulators nationwide are now placing GPC compliance as a top priority.

The joint announcement expands on previous enforcement actions that focused on UOOM signals, beginning with the 2022 Sephora settlement in California. As part of the investigative sweep, the AGs have already sent letters to businesses that do not appear to be processing consumer opt-out via UOOMs, requesting that those businesses come into immediate compliance.

While consent management solutions, such as cookie banners, can be configured to recognize GPC signals, regulators have alleged that these solutions often are not configured properly, leading to personal information being sold or shared, or used for targeted advertising, despite consumer opt outs. For example, in a recent $1.55 million settlement, the California AG alleged that Healthline, a health information website, failed to honor consumer opt-outs submitted via its cookie banner, its "*Do Not Sell or Share My Personal Information*" link, and the GPC signal. We previously covered this settlement in depth here.

This issue has also drawn the attention of plaintiffs' firms, which have sent demand letters to businesses alleging that their use of third-party cookies or pixels "intercepted" or "wiretapped" communications without consent where such businesses' cookie banners did not honor consumer requests to opt out.

New Required Confirmation of Compliance with UOOM Signal

Adding another layer to these compliance obligations to respond to UOOMs, the updated CCPA regulations will mandate that businesses provide an explicit, user-facing confirmation that a UOOM signal has been honored beginning January 1, 2026.

Per the updated regulations, it is no longer sufficient to simply process an opt-out signal in the background. Businesses must visually confirm compliance to the consumer. The amended regulations provide examples of acceptable notification methods, such as displaying a message on the website stating, "*Opt-Out Preference Signal Honored*," or showing a pre-selected toggle or radio button within a privacy menu that indicates the user has opted out. This requirement for affirmative feedback places a new burden on businesses to ensure their technical infrastructure not only correctly interprets and complies with UOOM signals but also communicates this action back to the consumer in real-time.

Don't Forget About Risk Assessments for Selling or "Sharing"

Those watching the privacy regulatory space are well aware of the upcoming CCPA risk assessment requirements for cybersecurity and automated decision-making technologies. Beginning January 1, 2026, nested within the list of processing activities that the CCPA's updated regulations consider a "significant risk" and therefore require a risk assessment, are the selling and sharing of personal information, including for targeted advertising. This means that common advertising practices, such as deploying third-party advertising cookies or pixels on a website, will soon require businesses to perform and document a risk assessment.

The regulations contain detailed requirements regarding the content of and procedure for conducting a risk assessment. Specifically, risks assessments must:

- Explain the activity and its purpose in granular detail, including: the specific categories of personal information required (and, in support of data minimization requirements, the minimum categories of personal information necessary to achieve the intended purpose); the method of collecting, using, and sharing personal information; the intended retention period for each category of personal information; and all transparency disclosures provided to consumers.
- Identify the purported benefits and potential negative impacts of the proposed activity. Negative impacts may include unauthorized access to or use of personal information, discrimination, loss of control over personal information, coercion, or economic, physical, psychological, or reputational harms.

- Describe the safeguards that will be implemented to manage potential negative impacts (e.g., technical safeguards, policies or procedures, notifications or consents).

While the regulations do not require businesses to submit their risk assessments to the CPPA for approval, they must be made available to the agency upon request.

What Should Businesses Do Now?

- **Test and Retest Regularly:** Regularly audit and test all opt-out mechanisms, including GPC and other UOOM signal processing, cookie banners, and "*Do Not Sell or Share My Personal Information*" links, to ensure they are functioning as intended.
- **Inventory Data Flows:** Identify all instances where personal information is shared for cross-context behavioral advertising or otherwise processed in a manner that may trigger opt out or risk assessment requirements.
- **Tell Consumers When Honoring UOOM Signals:** Businesses that sell or share personal information, including for targeted advertising, will need to indicate on their websites when they have recognized and honored a consumer's request to opt out via a UOOM.
- **Vendor Management:** Review contracts with partners to ensure they include CCPA-mandated provisions and that these partners are capable of honoring consumer opt-out requests.
- **Develop a Risk Assessment Framework:** Create a standardized process and template for conducting and documenting risk assessments that align with the CCPA's requirements.

As the regulatory landscape for data privacy in California and other states continues to evolve, the latest enforcement actions, new regulations, and priority statements from the AG demonstrate that the bar for compliance is rising sharply and rapidly.

CONTACTS

Omer Tene
Partner

otene@goodwinlaw.com
Boston | +1 617 570 1094

Jacqueline Klosek
Partner

jklosek@goodwinlaw.com
New York | +1 212 459 7464

Jonathan Ng
Associate

jonathanng@goodwinlaw.com
Silicon Valley | +1 650 752 3246

Gabe Maldoff
Associate

gmaldoff@goodwinlaw.com
Washington, DC | +1 202 346 4317