Insights, News & Events

MULTI-STATE SWEEP PUTS GLOBAL PRIVACY CONTROL IN THE SPOTLIGHT: 5 STEPS FOR BUSINESSES IN CA, CO, CT, AND ELSEWHERE

Insights
Sep 11, 2025

Officials from California, Colorado, and Connecticut just announced a coordinated investigative sweep targeting companies whose websites may be ignoring automatic opt-out preference signals that users can configure in their browsers. What does this September 9 announcement mean? If your business has been slow to honor Global Privacy Control (GPC) signals, regardless of the state in which your business is based, consider yourself to be officially on notice after this week's big development. If you've implemented GPC compliance, you need to double-check your process actually works. If you haven't implemented GPC compliance, make it a top priority today. Here's a quick summary and some guidance to take the next steps regardless of what you've done to date.

What Happened?

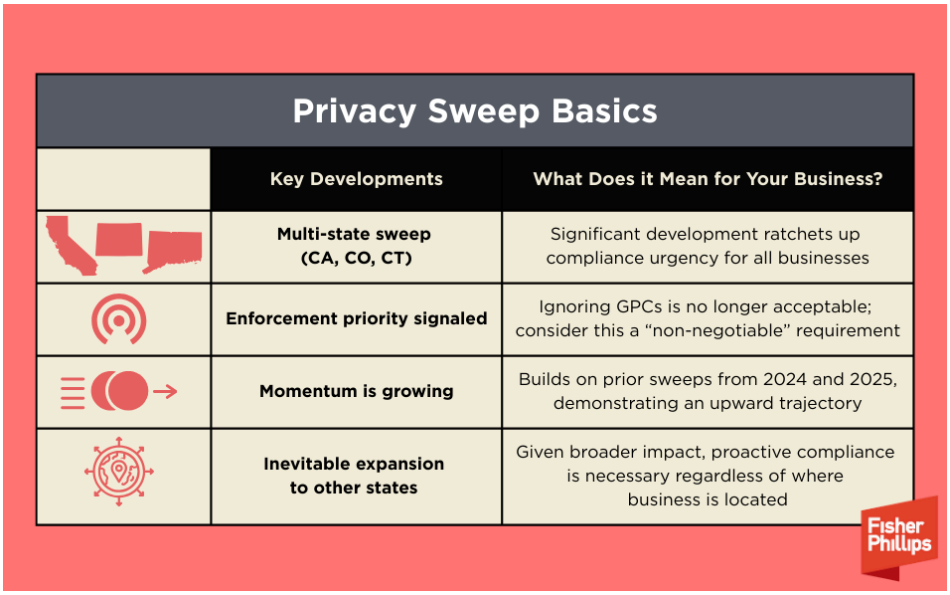
- **Joint Sweep:** The California Privacy Protection Agency (CPPA) and the AGs of CA, CO, and CT issued investigative letters on September 9 to businesses that appear to be failing to honor Global Privacy Control (GPC) signals.
- **What's at Stake:** These signals communicate a consumer's decision to opt out of the sale or sharing of personal data, including the use of personal information for targeted advertising, through cookies and other tracking technology on a website. State consumer privacy laws in California, Colorado, and Connecticut require businesses to ensure that their websites process these signals.

Related People

Darcey M. Groden, CIPP/US
Partner
858.597.9627

Usama Kahf, CIPP/US
Partner
949.798.2118

- **Enforcement Priority:** Regulators stressed that ignoring GPCs is no longer acceptable. As Connecticut's AG William Tong put it, honoring these signals is a *"non-negotiable"* requirement of modern privacy law.
- **Bigger Picture:** This action builds on prior sweeps, such as the CPPA's investigation of registered data brokers last year and earlier this year. Together, these moves show a consistent enforcement trajectory.



Why It Matters to Your Business – Regardless of Where You're Located

There are three big reasons why this news should be a wake-up call for your business, whether you operate in the three affected states or not.

- **Compliance Is No Longer Optional** – Your business can no longer wait for a lawsuit or regulatory letter to know what's required of it. As our firm noted in our recent publication **"What Website Owners Need to Know About Opt-Out Preference Signals"** (FP Insights, July 2025), the writing was already on the wall: honoring GPCs was always going to be a compliance priority. This multi-state sweep proves that point.
- **Multi-State Trend** – While California, Colorado, and Connecticut are leading this initiative, other states – including Texas, Oregon, Maryland, and Minnesota – have laws on the books that also require (or soon will require) recognition of universal opt-out mechanisms for businesses subject to their consumer privacy laws.

Service Focus

Consumer Privacy Team

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

Denver

Businesses that take a wait-and-see approach risk being caught flat-footed when enforcement inevitably spreads.

What Your Business Should Do Now

We previously outlined four compliance steps, and these remain essential. In light of the enforcement sweep, here's how you can turn those steps into an immediate action plan:

1. Implement GPC Detection Without Delay

Work with your website and app developers to ensure your systems can detect and honor GPC signals. Confirm your consent management platform (CMP) or privacy vendor supports universal opt-out mechanisms.

2. Audit and Test Your Systems

Don't assume they work and that all your tracking technologies are properly classified – test your website regularly. Regulators and advocacy groups may run their own checks. Consider cross browser testing to ensure GPC signals are recognized across common platforms. We recommend independent testing, meaning do not rely on the same vendor that develops or runs your website or that manages your cookie consent mechanism to self-test and self-validate their own tools. Additionally, this testing should be done regularly, not once in a blue moon or just once at the outset of a website launch.

3. Document and Verify Compliance

Keep records of your testing and configuration, as independent verification or third-party audits can demonstrate good-faith compliance if regulators come calling.

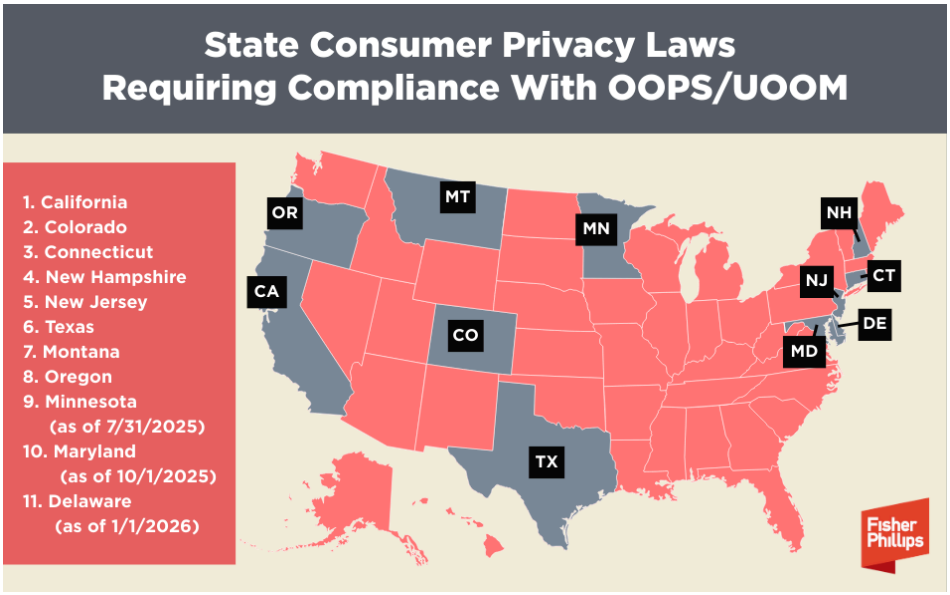
4. Update Policies and Disclosures

Make sure your privacy policy clearly states how you handle opt-out preference signals. Ensure your internal workflows (marketing, sales, IT, compliance) align with what your policy promises.

5. Monitor the Multi-State Landscape

Track developments in other states that are members of the Consortium of Privacy Regulators. Anticipate that additional AGs will join the sweep, expanding enforcement

exposure. The best way to monitor developments in this area is to subscribe to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.



Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. You can also visit FP's US Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group or Consumer Privacy Team.