

OOPS! What Website Owners Need to Know about Opt-Out Preference Signals + 4 Compliance Steps

Insights

7.28.25

Businesses should be aware of recent public outreach in California – and other states with consumer privacy laws – signaling that increased enforcement activity is on the horizon. For instance, the California Privacy Protection Agency (CPPA) is now promoting awareness to consumers on how to use opt-out preference signals (OOPS), following a recent compliance campaign aimed at businesses subject to the California Consumer Privacy Act. Beyond California, a growing number of states with consumer privacy laws have enacted similar protections that require covered businesses to implement OOPS (although some states refer to this universal opt-out mechanism as a UOOM). Here is what you need to know about OOPS and UOOMs, and four steps to help your business stay compliant.

What are **OOPS** and **UOOM** ?

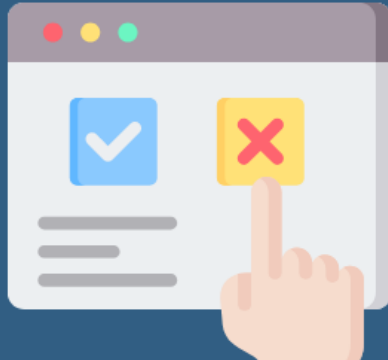

OOPS

opt-out preference signals

UOOM

universal opt-out mechanism

OOPS and **UOOMs** give individuals a simple, automatic way to tell websites to not share or sell their personal data.

What are OOPS and UOOM?

OOPS and UOOMs give individuals a simple, automatic way to tell websites to not share or sell their personal data. Instead of website users having to click through each website's settings, individuals

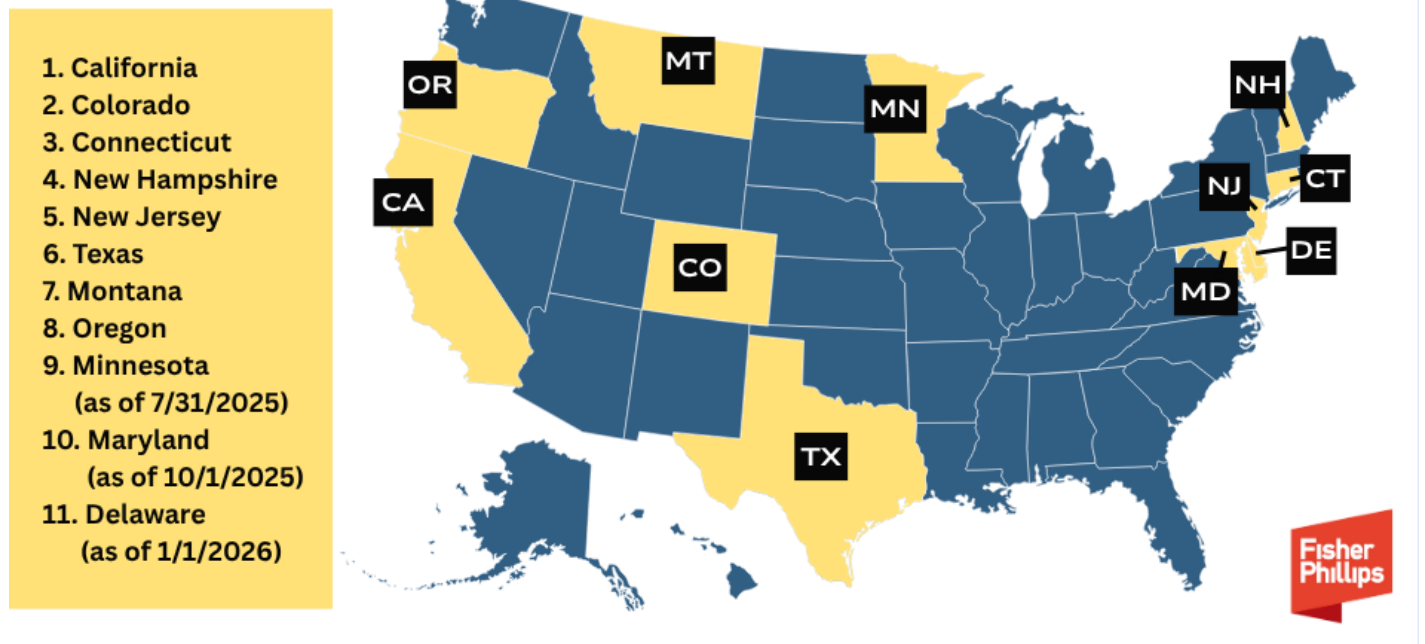
can use a special browser or extension that sends an opt-out signal. The point of OOPS and UOOMs is to further push for a frictionless opt-out process.

Why does it matter? As a general rule, states with consumer privacy laws have created mechanisms for users to opt-out of the sale of personal information and/or the use of their personal data for targeted advertising. How this right is formulated and operationalized can differ from state to state, but a number of states (including California) require that covered businesses honor OOPS and UOOMs to effect that right. Currently, the OOPS and UOOM that states expect business to honor is the Global Privacy Control (GPC).

The following states' consumer privacy laws require compliance with OOPS/UOOM:

1. California
2. Colorado
3. Connecticut
4. New Hampshire
5. New Jersey
6. Texas
7. Montana
8. Oregon
9. Minnesota (as of 7/31/2025)
10. Maryland (as of 10/1/2025)
11. Delaware (as of 1/1/2026)

State Consumer Privacy Laws Requiring Compliance With OOPS/UOOM



California just released [guidance](#) this month for consumers on how to implement OOPS – and the Colorado and Connecticut Attorneys General posted a [video](#) explaining how consumers can opt out from ad tracking. This type of guidance could signal that additional enforcement actions are coming and that opt-out preference signals are a high priority.

4 Steps Businesses Should Consider Taking Now

1. Become Compliant with OOPS and UOOMs

Compliance takes more than just posting a policy. You'll also want to do the technical work on the back end of the website to ensure that GPCs (the most common OOPS and UOOM) are detected and honored. For businesses that work with consent management platforms, such platforms should have mechanisms to honor GPCs. Additionally, there are a lot of technical resources available for website developers to assist with the implementation of OOPS/UOOM. The GPC [website](#) provides the proposed specification and back-end implementation instructions.

Additionally, recognize that a cookie banner with consent management capabilities is not the same as or a substitute for OOPS or UOOMs. The California Consumer Privacy Act's and other consumer privacy laws' requirement for an OOPS or UOOM is an independent requirement.

2. Make Sure the OOPS or UOOM is Working as Intended

Be aware of common problems that result in OOPS or UOOM not working as intended. For example, a tracking technology on a website may not be properly classified (or classified at all). It is up to you to ensure that the OOPS or UOOM knows what technologies should be blocked. Relatedly, the way a tracking technology is set up may result in unintended data leakages.

If your OOPS or UOOM is not working correctly, it could be considered an unfair business practice in addition to a violation of opt-out rights under relevant consumer privacy laws. Notably, [Healthline](#) recently paid \$1.55 million to resolve allegations brought by the California Attorney General that it was violating the California Privacy Protection Act and engaged in deceptive business practices for allegedly allowing consumers to opt-out of tracking cookies but not effecting that consent. If your privacy notices or disclosures make affirmative representations that you honor any types of OOPS or UOOMs (like a GPC) and the opt-out is not complete, you may be engaging in an unfair business practice.

3. Consider Hiring a Third Party to Test Opt-Out Technology

At the end of the day, your business is responsible for ensuring that the OOPS and UOOM is working correctly. As such, you should not rely solely on your website host or consent management platform to guarantee that you are getting it right. Consider hiring a third-party vendor to regularly test and assess whether the opt-out technology is operating as intended.

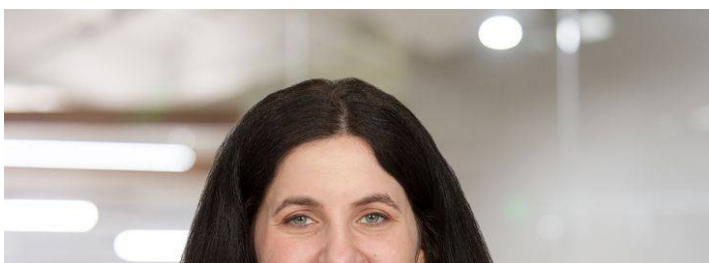
4. Stay Informed on Future Legislation Expanding the Use of OOPS Signals

A pending California bill, [AB-566](#), would require all browsers to include OOPS. If passed, there will likely be a significant increase in individuals utilizing OOPS.

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](#).

Related People





Darcey M. Groden, CIPP/US

Associate

858.597.9627

Email



Usama Kahf, CIPP/US

Partner

949.798.2118

Email



Jillian Seifrit, CIPP/US

Associate

610.230.6129

Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills