CLIENT ALERTS & INSIGHTS

California, Colorado, and Connecticut Announce Coordinated Investigative Sweep to Enforce Compliance with the Global Privacy Control Signal

SEPTEMBER 23, 2025

Key Takeaways

- California, Colorado, and Connecticut have launched a coordinated investigation targeting businesses that fail to honor Global Privacy Control (GPC) signals, which are browser-level settings allowing consumers to opt out of the sale or sharing of their personal information for targeted advertising.
- This enforcement sweep highlights a growing business risk: regulators are increasing their scrutiny of online data collection and targeted advertising practices, and non-compliance with GPC requirements can lead to regulatory action and reputational harm.
- Businesses should promptly assess and update their websites to ensure they detect and process GPC signals, review privacy notices for accurate disclosures, and regularly monitor third-party cookie management tools to confirm ongoing compliance with state data protection laws.

States continue to focus on targeted advertising opt-out rights under continued and coordinated enforcement of U.S. state data protection laws.

In early September, California (through the California Attorney General and the California Privacy Protection Agency), Colorado, and Connecticut announced a joint investigative sweep targeting businesses for alleged failures to honor consumer targeted advertising opt-out requests. The investigative sweep will specifically be looking for failures to honor Global Privacy Control signals.

The Global Privacy Control is a user-enabled, browser-level setting designed to allow consumers to automatically communicate their request to opt-out of the selling or sharing of their personal information for targeted advertising purposes.

The tri-state initiative signals a deepening commitment among U.S. state data protection regulators to cooperate and coordinate on data protection law investigations and enforcement. This trend signals increasing scrutiny that regulators are placing on online data collection practices as U.S. state data protection laws mature.

This follows the early summer announcement of the “Consortium of Privacy Regulators” among a handful of U.S. states and a trend of increased data protection enforcement activity. One of the early-but consistent-trends is a focus on targeted advertising and online tracking technologies. See our previous coverage of emerging enforcement trends here.

Global Privacy Control Requirements

The Global Privacy Control (GPC) is an opt-out preference signal that provides consumers with a browser-level setting enabling them to automatically assert their right to opt-out of the selling or sharing of their personal information for targeted advertising purposes. This is in lieu of the consumer having to manually submit opt-out requests or change their preferences on a website-by-website basis.

Well over half of the U.S. state data protection laws in effect or coming into effect require businesses to adhere to GPCs. California, Colorado, and Connecticut have been at the forefront of this requirement, providing specific guidance and regulations on GPC compliance. For example, in early 2024, Colorado was first in line to provide specific regulations on GPC signals.

With respect to GPC signals, businesses subject to U.S. state data protection laws are required to:

1. Detect and process GPC signals as legally binding opt-out requests; and
2. Immediately opt such consumers out of the selling and sharing of their personal information for targeted advertising purposes once the GPC signal is received.

Considerations and Next Steps

Businesses subject to U.S. state data protection laws-especially those with e-commerce and retail websites-need to evaluate their current technical posture to ensure their websites and applications are compliant with GPC requirements. To conduct this evaluation, businesses should consider:

1. Evaluating whether their websites and applications are currently and correctly detecting and processing GPC signals.
2. Reviewing their privacy notices to ensure it contains accurate disclosures on consumer opt-out rights and adherence to GPC signals.
3. Reviewing any in-scope third-party cookie management and consent tools to ensure they are configured to adhere to GPC signals.

It is important to note that reliance on, and use of, third-party plug-ins and cookie management tools is not a silver bullet. Businesses need to continue monitoring those tools and applicable configurations to ensure compliance with GPC and opt-out requirements.

This was perhaps best exemplified in the California Privacy Protection Agency's (CPPA) recent enforcement action against the retailer Todd Synder.

The CPPA noted that, like many businesses, Todd Synder utilized third-party cookies for analytical and targeted advertising purposes. To effectuate consumer requests to opt out of such selling and sharing, Todd Synder directed consumers to utilize the GPC or utilize a cookie settings preference center.

However, for a period of 40 days, when a consumer clicked on the cookie settings preference center link, a cookie banner appeared but then instantly disappeared-preventing the consumer from

exercising their right to opt out. Relatedly, the Todd Synder website was not adhering to GPC signals.

The CPPA appeared critical of businesses that rely solely on third-party cookie management and data subject rights request tools, noting that "*Todd Synder would have known that Consumers could not exercise their CPPA rights if the company had been monitoring its Website, but Todd Synder instead deferred to third-party privacy management tools without knowing their limitations or validating their operation.*"

The Benesch Data Protection team is committed to staying at the forefront of these recent developments to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel is a Managing Associate in Benesch's Data Protection Group. He can be reached at 312.212.4977 or lschaetzel@beneschlaw.com.