CLIENT ALERTS & INSIGHTS

California Keeps Its Foot on the Gas: CalPrivacy and Minnesota Announce Parallel Settlements from Joint Privacy Consortium Investigation

NOVEMBER 24, 2026

Authors: Ryan T. Sulkin, Jacob “Jake” Bennett

Featured Practices: Data Privacy & Cybersecurity, State Attorneys General Investigations & Enforcement, Litigation, Intellectual Property

Key Takeaways

- On November 19, 2026, the California Privacy Protection Agency (“CalPrivacy”) and the Minnesota Attorney General announced coordinated settlements with Polaris Industries, Inc. (“Polaris”) totaling more than $1 million, the first enforcement action arising from a joint investigation by members of the Consortium of Privacy Regulators.
- Polaris is one of four CCPA enforcement actions CalPrivacy announced in November alone, each centered on consumers’ right to opt out of the sale of their personal information or its sharing for cross-context behavioral advertising (i.e., targeted advertising based on activity across other websites), including through opt-out preference signals (“OOPS”), such as the Global Privacy Control (“GPC”), which are browser settings that automatically tell every website a consumer visits not to sell or share their data.
- With CalPrivacy also advancing new OOPS regulations that generally clarify existing obligations, businesses should expect additional multistate collaboration and settlements and should test their opt-out mechanisms now.

The Polaris Settlement: The Consortium’s First Joint Result

CalPrivacy’s Board issued a Decision and Stipulated Final Order requiring Polaris to pay an administrative fine of $910,986 and change its business practices to resolve alleged violations of the California Consumer Privacy Act (“CCPA”). In a parallel action, the Minnesota Attorney General reached a $150,000 settlement with Polaris under the Minnesota Consumer Data Privacy Act (“MCDPA”), marking Minnesota’s first enforcement action under the MCDPA since it took effect in July 2025. Both regulators are members of the Consortium of Privacy Regulators and have confirmed that they worked on the investigation together.[1]

According to the regulators, Polaris (i) required consumers to verify their identity by email before processing opt-out requests and denied requests when consumers did not respond, (ii) offered a "Decline All" button in its "Your Privacy Choices" pop-up that did not stop all sales and sharing through tracking technologies (in one instance, clicking it fired the Meta pixel), (iii) deployed certain tracking technologies that were not configured to process OOPS, such as GPC, and (iv) maintained a privacy policy that did not explain how it processes OOPS. Notably, the CCPA regulations prohibit requiring a verifiable consumer request to opt out, and the MCDPA similarly requires controllers to comply with opt-out requests upon receipt without additional steps. CalPrivacy also emphasized how quickly these failures compound, finding that Polaris committed at least five violations each time an opted-out consumer visited its website.

Minnesota also alleged that Polaris lacked formal written data privacy and protection assessments before April 2026, and that even after Polaris told the Minnesota Attorney General it had cured the issues identified in a November 2025 warning letter, subsequent testing uncovered continuing errors in how Polaris handled opt-out requests. In addition to paying the fines, Polaris must make its opt-out methods easy to use and require minimal steps, maintain a "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" link, and update its privacy policy to address OOPS. Polaris also agreed to adopt an internal approval process for new tracking technologies, conduct quarterly scans of its tracking technologies for three years to ensure it honors opt-out requests, engage a technical specialist, conduct employee training, and, under the California order, provide annual officer-certified compliance reports for three years.

A Busy November for CalPrivacy

Polaris caps a particularly active month for CalPrivacy as the year wraps up. On November 10, CalPrivacy announced a $2.975 million fine against Federal Express Corporation for, among other things, stating it did not sell or share personal information while engaging in cross-context behavioral advertising, failing to provide a "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" link, failing to honor OOPS (an obligation CalPrivacy noted has been in place since 2020) or explain in its privacy policy how it processed them, offering a webform for CCPA requests that listed "Do Not Sell" as an option but did not apply to online tracking technologies, and maintaining cookie controls that did not address sales or sharing and did not stop all data flows. The FedEx order also imposes ongoing testing, monitoring, and risk-mitigation obligations for at least three years, including quarterly inventories of online tracking technologies with a review process for any new tracking technology before it is added.

On November 17, CalPrivacy announced a $1.55 million fine against The Hertz Corporation (including its Dollar and Thrifty brands) for failing to process OOPS (an obligation CalPrivacy again noted has been in place since 2020), failing to explain how it processed them, and adding unnecessary friction to the opt-out process. Specifically, the cookie manager on the Dollar and Thrifty websites displayed advertising cookies as already toggled off, but if a consumer closed the window rather than clicking "Save Changes," the settings reverted to allow advertising cookies. In addition to the fine, Hertz must comply for three years with quarterly testing, monitoring, and risk-mitigation requirements, including testing its methods for submitting CCPA requests, inventorying tracking technologies and reviewing any new tracking technology before it is deployed,

and testing opt-out compliance across staging and production environments, browsers, mobile device platforms, and tag management containers.

The same day, CalPrivacy also announced an order requiring retailer Filson to stop online sales and sharing of personal information pending certification of compliance, based on allegations that Filson failed to provide a "Do Not Sell or Share My Personal Information" link, failed to honor OOPS, and directed consumers to three methods for exercising their privacy rights (phone, email, and a web link), none of which worked. CalPrivacy explained that it reduced Filson's fine to $217,987 from what would otherwise have been a multimillion-dollar fine because Filson provided confidential financial information demonstrating its inability to pay.

This enforcement activity coincides with CalPrivacy's regulatory focus on the same issues. At its November 6, 2026, meeting, the CalPrivacy Board voted to commence formal rulemaking on proposed amendments to the CCPA regulations regarding OOPS.

The proposed amendments would, among other things, expressly identify GPC as an OOPS, add examples addressing cookie syncing and pseudonymous profiles, clarify that, to meet the CCPA's timing requirements, a business must determine whether it has received an OOPS before setting cookies or other tracking technologies that facilitate the sale or sharing of personal information, and expand the public metrics reporting requirements currently imposed on businesses that handle the personal information of 10 million or more consumers to also cover businesses subject to the CCPA's cybersecurity audit requirements. CalPrivacy has characterized the amendments as generally clarifying, rather than creating, obligations already required by statute and regulation, signaling that it views the core OOPS requirements as enforceable today.

Looking Forward

California remains the most active state privacy regulator, and the Polaris settlement shows that the Consortium of Privacy Regulators is now producing results. We expect further collaboration among Consortium members and additional joint or parallel settlements, particularly as state regulators increasingly coordinate investigations around shared enforcement priorities such as opt-out rights and OOPS. Coming roughly a year after the Consortium's September 2025 GPC investigative sweep, the Polaris settlement signals that this coordination is now translating into formal enforcement. Notably, cooperation and remediation did not prevent seven-figure fines in at least two of the November actions, and several of the orders reflect that the violations stemmed from websites and tracking technologies that were not properly configured to honor opt-outs, rather than from intentional practices.

Given these developments, businesses should work with privacy counsel to evaluate their opt-out practices before they become the subject of a regulatory inquiry. In particular, we recommend that businesses (i) confirm that their websites and apps detect and honor OOPS, including GPC, across all tracking technologies and tag management containers, (ii) remove verification or other unnecessary friction from opt-out workflows, (iii) test cookie banners and preference centers to confirm that opt-out selections actually stop sales and sharing, (iv) update privacy policies to explain how OOPS are processed, and (v) ensure that required assessments are documented and can be produced upon regulator request.

Ryan Sulkin is Team Lead of Benesch's Data Privacy & Cybersecurity Practice Group. He can be reached at 312.624.6398 or rsulkin@beneschlaw.com.

Jake Bennett is an Associate in Benesch's Data Privacy & Cybersecurity Practice Group. He can be reached at 312.517.9561 or jbennett@beneschlaw.com.

---

[1] Announced in April 2025, the Consortium is a bipartisan group of state privacy regulators that collaborates on implementing and enforcing state privacy laws, including by sharing information to conduct enforcement across jurisdictions. With Vermont joining in August 2026, the Consortium has grown to twelve regulators: CalPrivacy and the Attorneys General of California, Colorado, Connecticut, Delaware, Indiana, Maryland, Minnesota, New Hampshire, New Jersey, Oregon, and Vermont. Although Consortium members previously coordinated on a September 2025 investigative sweep focused on GPC compliance, the Polaris settlement is the first joint settlement we have seen arise from the Consortium.