JENNER & BLOCK

OOPS, we tracked you again! CalPrivacy announces nearly $3M CCPA settlement

Client Alerts

November 13, 2026
By: Madeleine Findley, Venus D. Johnson, Caroline Cease

On November 10, 2026, the California Privacy Protection Agency (CalPrivacy) announced a $2.975 million settlement with FedEx for alleged California Consumer Privacy Act (CCPA) violations. FedEx, the global transportation company that delivers millions of packages daily, allegedly shared personal information about website visitors with third parties for cross-context behavioral advertising without 1) disclosing that it sold or shared consumer personal information; 2) informing consumers of their opt-out rights; or 3) providing a compliant method for consumers to opt out of the sale or sharing of their personal information, including recognizing universal opt-out preference signals (OOPS). In addition to paying a fine, the company must scan its websites and apps every quarter to update its cookie inventory, maintain contracts with each third-party cookie provider, and configure its digital properties to honor consumer opt-out requests, among other things, for at least three years.

What happened?

In September 2025, CalPrivacy joined with the Attorneys General of California, Colorado, and Connecticut to announce a joint investigative sweep of potential noncompliance with requirements to honor the Global Privacy Control (GPC) the most widely deployed OOPS, a browser setting that automatically informs a business of a consumer's request to opt out of the sale or sharing of their personal information. The coalition of regulators contacted businesses about apparent noncompliance and, among other things, requested compliance.

What privacy rights are involved?

Right to Opt Out of Sale or Sharing of Personal Information to Third Parties

CalPrivacy alleged that although FedEx's privacy policy said that the company did not sell or share personal information, in practice, the company's website contained third-party tracking technology, including cookies and pixels, used for targeted advertising and cross-context behavioral advertising. These tracking technologies allowed consumers to be tracked across multiple websites and applications and enabled advertisers to build profiles to better target them. Although the company offered a cookie consent tool, it did not inform consumers of their right to opt out of the sale or sharing of their data, and it did not offer a "Do Not Sell or Share My Personal Information" or "Your

Privacy Choices" opt-out link on its websites. Additionally, the company's cookie consent tool did not control all of the tracking technologies on its sites.

What are the takeaways?

Be upfront and transparent about your data practices

Every state privacy law requires companies to describe their privacy practices. The CCPA requires companies to say whether they sell or share consumers' personal information to third parties for cross-context behavioral advertising. According to the settlement, the company's privacy policy during the relevant period said it did not sell or share personal information, when, in fact, it did. The order does not describe how this happened, but as data use and privacy practices evolve, a privacy policy needs to evolve as well. Adding a pixel to a website to track the effectiveness of an ad campaign can require a review of an entity's privacy policy, and regularly reviewing policies against practices is an important way to identify and close such gaps.

Method to Exercise Opt-Out Rights

Honor OOPS like GPC

The CCPA, like privacy laws in thirteen other states, requires covered businesses or entities to recognize and honor opt-out preference signals such as GPC and to describe how they handle such signals in their privacy policies. The company's privacy policy reportedly did not describe how it handled OOPS such as GPC. California's GPC requirement took effect in 2020, and although few browsers offered GPC functions to users at that time, other states quickly followed.

Provide opt-out methods in the number and form required

CalPrivacy alleged that the company failed to provide consumers with a compliant way to opt out of the sale or sharing of their personal information. The CCPA directs businesses to provide at least two methods for consumers to opt out of sale or sharing. If a business collects personal information online, those methods must include 1) recognition of an OOPS and 2) an interactive form accessible by clicking on a "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" link. Here, CalPrivacy alleged, the company's website offered neither of these methods.

Importantly, FedEx did offer an interactive form for consumers to exercise privacy rights, and that form even included an option labeled "Do Not Sell/Share My Information (Targeted Advertising)." But this was insufficient because the form specifically informed consumers that it did not opt consumers out of cookies or tracking technologies, and instead directed them to update their cookie preferences through the cookie consent manager.

Confirm that tools function as described and explain what they do

Regulators have been increasingly focused on how a business's privacy tools, including cookie consent managers, actually function. If a tool is not properly configured and tested before launch (and at intervals thereafter), it creates exposure for the business. CalPrivacy focused, in particular, on how FedEx's cookie consent manager worked, including, importantly, that tracking technologies continued to transmit personal information even after a website visitor turned off tracking cookies.

As a result, CalPrivacy concluded that the company failed to provide a functional method for consumers to opt out.

The settlement order underscores that cookie consent managers, by themselves, may not suffice as an opt-out method. CalPrivacy explained that even if the tool had controlled all the cookies, "it did not address how the cookie settings apply to the sale or sharing of personal information" and the company could not rely on it "as a method for opting out." In other words, if the cookie manager does not explain how its settings allow consumers to opt out of the sale/sharing of their personal information, it may not qualify as an opt-out method.

What should businesses be aware of?

The CalPrivacy settlement underscores the importance of regularly validating privacy disclosures, cookie consent tools, and opt-out mechanisms, particularly OOPS. As of July 1, 2026, fourteen states require businesses that sell or share personal information to honor OOPS, such as GPC, in at least some circumstances. The risk of noncompliance keeps increasing.

On January 1, 2027, California's Opt Me Out Act will require for the first time that all web browsers, including the most widely used browsers, must include built-in OOPS functionality. This has the potential to significantly increase the number of GPC signals and other automatic opt-out requests that a business must recognize and honor through its websites as consumers gain ready access to such signals. Businesses that are taking a wait-and-see approach or that have not already confirmed their ability to honor opt-out requests will be at risk: these are easy compliance gaps for consumers and regulators to spot.

Regulators, including CalPrivacy, have sent a strong message that businesses should be testing their privacy compliance, including consumer opt-out methods, and regularly updating their consumer-facing policies and tools. And regulators are testing these tools even if companies are not. Enforcement actions have moved from the *what*—what does a business say in its privacy policy and does that meet the applicable requirements—to the *how*—how does the business do what it says. Notices and opt-out tools are not set-and-forget but need to evolve with and be tested against the business's privacy practices on an ongoing basis. As privacy practitioners have experienced, a disclosure that was up to date in January may have gaps by December.

In multiple actions this year, regulators have penalized companies for offering consumers choices that did not function as claimed or that made opting out more difficult than opting in. More requirements are on the horizon, including potential CalPrivacy proposals to require companies to honor OOPS before setting any website cookies or tracking technologies.

What steps can businesses take?

As the year-end approaches, companies are planning for upcoming compliance needs. Among the steps to include, companies should consider:

- Scheduling regular audits of websites and apps to update cookie inventories
- Testing cookie consent managers to ensure they control all cookies as described
- Ensuring websites honor OOPS and considering the potential for increased volume in 2027
- Reviewing consumer opt-out methods to confirm they take the required form and function as expected
- Reviewing supply chain privacy risks to identify any new risks that have been introduced
- Reviewing privacy policies and notices and updating them to reflect current practices and comply with relevant state laws
- Monitoring regulatory developments, including proposals tightening practices around tracking technologies, and submitting comments in rulemakings

Related Lawyers



Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095



Venus D. Johnson
Special Counsel
vjohnson@jenner.com
+1 415 293 4833



Caroline Cease
Partner
ccease@jenner.com
+1 202 639 6056

Related Capabilities

Data Privacy and Cybersecurity

State Attorneys General

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →