FEBRUARY 27, 2026

Plaintiffs Are Quietly Creating a "Private Right of Action" Under the CCPA - Even Though the Law Doesn't Allow One

by Meghan K. Farmer , Tatum Andres

Takeaway: After years of suing companies under wiretap laws for using third-party website tracking tools, plaintiffs' firms are now advancing a new theory. Instead of arguing that tracking itself is unlawful, they are claiming that companies are breaking their promises about opt-outs. In doing so, they are effectively creating a private enforcement mechanism for the California Consumer Privacy Act (CCPA), even though the statute does not provide one outside of certain data breach scenarios.

Most customer-facing websites and apps use cookies, which are small text files stored on a user's device. These cookies help analyze behavior, personalize content, enable social media features, and serve targeted ads. Some cookies are first-party, meaning they are used by the website itself. Others are third-party, meaning outside vendors can collect data across multiple sites.

For years, plaintiffs' firms focused on bringing lawsuits under state wiretap laws, especially the California Invasion of Privacy Act (CIPA). The theory was that when a website uses third-party tracking tools without proper notice and implied consent, it is allowing a third party to "listen in" on user communications. Because CIPA allows private lawsuits and statutory damages, it became a powerful tool for the plaintiffs' bar.

In response, companies invested heavily in compliance. They updated privacy policies. They built detailed cookie banners. They implemented clear "Accept All" and "Reject All" options. The goal was to provide notice and obtain consent to reduce litigation risk.

But plaintiffs' firms evolved their strategy in response.

Reframing CCPA Failures as Other Legal Violations

Under the CCPA, businesses must allow consumers to opt out of "cross-context behavioral advertising," which essentially means targeted ads based on a person's activity across different websites.

To comply, companies that use third-party tracking tools typically rely on cookie banners that let users accept or reject certain types of tracking. If those opt-out tools do not function properly, the company risks regulatory enforcement by state authorities.

Plaintiffs are now attempting to sidestep the lack of a private right of action under the CCPA by repackaging alleged opt-out failures as: (a) wiretap violations under statutes like CIPA; (b) invasion of privacy claims; and (c) unfair and deceptive practices under consumer protection laws/

Here is how this theory works in practice. A website displays a cookie banner stating that users can reject non-essential cookies, including analytics and advertising cookies. A user clicks “Reject All.” However, in these new class action lawsuits, plaintiffs allege that even after they opt out, third-party tracking technologies continue transmitting data to vendors anyway.

Plaintiffs then argue: (1) the company represented that users could opt out; (2) the user relied on that representation; (3) the company continued collecting and transmitting data; and (4) that conduct constitutes a deceptive practice or invasion of privacy. Thus, rather than addressing only whether cookies were disclosed, the claims now dispute whether the company did what it promised.

This is where the shift becomes significant. Historically, if a cookie banner did not function properly or failed to fully implement an opt-out, the primary enforcement risk came from regulators. Under the CCPA, only regulators could bring enforcement actions for opt-out violations. And regulators bring a limited number of cases each year, often focusing on broader compliance issues rather than technical banner misfires.

But as courts begin accepting the theory described above, plaintiffs are effectively gaining a private enforcement mechanism for CCPA-style opt-out obligations, even though the statute expressly denies one.

Why This Theory Is Gaining Attention in Courts

Ordinarily, information such as browsing history, website interactions, device identifiers, session data, and general geolocation may not automatically create a strong privacy claim in court.

But plaintiffs are reframing the issue. They argue that once a company explicitly tells users that they can reject tracking, users develop a reasonable expectation that tracking will stop. The focus shifts away from the sensitivity of the data and toward the mismatch between what the company said and what technically occurred.

Some courts have allowed these claims to move past early dismissal stages, which has encouraged more filings. The practical effect is that plaintiffs are using traditional privacy and consumer protection theories to enforce what looks very similar to CCPA opt-out obligations.

The Next Area of Risk May Be Global Privacy Control Signals

This same reasoning could extend to Global Privacy Control signals. Several state privacy laws permit

consumers to exercise opt-out rights through browser-enabled signals. If a company indicates that their website respects these signals, but the website fails to properly detect or honor a valid GPC signal, plaintiffs may argue that: (1) the failure constitutes deceptive conduct; (2) continued tracking amounts to unlawful interception; and (3) the company ignored a legally recognized opt-out request. Thus, even without an express private right of action, technical consent failures may become the next major litigation trigger.

What This Means for Businesses

Cookie compliance is not limited to including the correct language in a company's privacy policy. Companies must also make sure their technology actually does what the disclosures promise.

In other words, Plaintiffs are no longer focused only on whether companies provided notice. They are testing instead whether an opt-out mechanisms function correctly in real time. If a "Reject All" button does not truly stop analytics and advertising cookies, that gap between promise and performance may be actionable in litigation.

To reduce risk, businesses should consider the following steps:

- First, conduct regular technical audits of cookie and tracking deployments. Do not rely solely on vendor assurances. Validate that cookies and third-party tags are blocked when a user opts out, including across different browsers and devices.
- Second, test "Reject All" and Global Privacy Control workflows periodically. Confirm that signals are detected and honored as designed. Small configuration errors or tag sequencing issues can create significant exposure.
- Third, align disclosures with actual practices. Avoid broad or absolute statements that tracking will "stop" unless you are confident the system fully supports that representation. Precision in language can help narrow risk.
- Finally, ensure cross-functional coordination. Legal, privacy, data engineering, and marketing teams should be aligned on how consent tools operate in practice. Litigation in this space often turns on technical details that legal teams may not see without data engineering input.

For companies with customer-facing websites and apps, the safest assumption is this: if you promise users they can opt out, plaintiffs will expect that promise to be honored down to the last line of code.