Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

March 9, 2026

California Privacy Protection Agency v. Ford Motor Company

Opt-Out Friction in Connected Vehicles: What Every Business Must Know Now

By Amy S. Mushahwar and Tricia Y. Wagner CIPP/US, CISSP, CISA

The California Privacy Protection Agency (CalPrivacy) recently issued a $375,703 enforcement order against Ford Motor Company, requiring it to change its opt-out practices and undergo an audit of its tracking technologies. The action is the second enforcement decision to emerge from CalPrivacy's ongoing investigative sweep of connected vehicle manufacturers, following a similar action against American Honda Motor Co. in 2025. This alert provides a detailed analysis of the enforcement findings, explains why email verification as a condition of opt-out is a widespread and urgent compliance risk, and connects this action to the framework we introduced in our prior client alert on the California Attorney General's (AG) record $2.75 million settlement with The Walt Disney Company.

KEY FACTS AT A GLANCE

Fine: $375,703
Regulator: California Privacy Protection Agency (CalPrivacy)
Violation Period: July 2023-March 2024
Violation: Email verification required before processing opt-out requests; prohibited under the California Consumer Privacy Act (CCPA)
Context: Second enforcement action (following Honda) from CalPrivacy's connected vehicle investigative sweep
Remediation Required: Easy opt-out methods, minimal steps, audit of tracking technologies, Global Privacy Control (GPC) compliance

1. The Core Violation: Email Verification as Opt-Out Friction

Ford required consumers to verify their email address before it would process requests to opt out of the sale and sharing of personal information collected through its digital properties and connected vehicle services. If a consumer did not complete the email verification step, Ford did not process the opt-out request, which is a common practice among brands.

The Rule CalPrivacy Applied

Under the CCPA, businesses may require identity verification for requests to delete, know, or correct personal information, but may not require verification for requests to opt out of the sale or sharing of personal information to a greater degree than is required for opt-in processes. Opt-out requests must be processed with operational parity to opt-in processes.

This distinction is fundamental. The CCPA intentionally treats opt-out rights differently from data access and deletion rights. The latter involve retrieving or destroying records tied to a specific individual, creating a legitimate basis for identity confirmation. Opt-out requests, by contrast, are prospective instructions to stop a practice; they do not require the business to locate or act upon historical records. Requiring email verification in this context adds a barrier that the law does not permit.

⚠ URGENT: Email Verification Is a Widespread Compliance Gap

Email verification before opt-out processing is not an edge case–it is a default configuration in many widely deployed consent management platforms (CMPs) and vendor tools. Many businesses have unknowingly inherited this violation through off-the-shelf products that treat all consumer rights requests as verifiable.

If your organization uses a third-party CMP, a privacy rights management platform, or any vendor-provided opt-out workflow, you should treat your current configuration as presumptively noncompliant until you verify otherwise. The Ford settlement makes clear that CalPrivacy does not view reliance on vendor defaults as a mitigating factor.

This risk is not limited to automotive or connected device companies. It applies to any business operating under the CCPA, including retailers, publishers, streaming platforms, financial services firms, health care companies, and software-as-a-service providers.

2. Connected Vehicles: A Sector Under Active Scrutiny

The Ford settlement is not an isolated incident. CalPrivacy announced in 2023 that it was conducting an investigative sweep of connected vehicle manufacturers, and the Honda and Ford actions represent its public enforcement outputs from that sweep. The agency has signaled that this sector will continue to receive targeted scrutiny.

The connected vehicle context adds particular complexity because data collection is pervasive, often continuous, and tied to multiple individuals–drivers, passengers, and registered owners–who may have different relationships with the vehicle and different expectations about data use. Ford's digital properties and connected vehicle services collect data across multiple touchpoints, creating an environment where opt-out architecture must be carefully designed and technically verified.

CalPrivacy's order also requires Ford to conduct an audit of tracking technologies on its website and to ensure compliance with opt-out preference signals, including the GPC. This reflects a recurring enforcement theme: Regulators are not merely looking at whether an opt-out button exists, but also evaluating whether the opt-out propagates through the technical stack and downstream data flows.

CalPrivacy's Publicly Announced Enforcement Priorities

CalPrivacy and the California AG have identified active areas of focus that should inform compliance triage: surveillance pricing, location data, GPC compliance, streaming services and connected televisions, employee and job applicant data, mobile apps, financial incentive and loyalty programs, and–as the Ford and Honda actions confirm–connected vehicles. If your business operates in any of these sectors, you should treat enforcement risk as elevated.

3. The Identity Symmetry Connection: From Disney to Ford

In our prior client alert analyzing the California AG's $2.75 million settlement with The Walt Disney Company, the largest CCPA enforcement action to date, we introduced the concept of Identity Symmetry as the organizing principle of California's evolving enforcement posture.

Identity Symmetry

If a business has built the capability to recognize, track, and link consumers across devices, services, or environments for monetization or analytics purposes, it must honor opt-out rights of that same operational scope. The architecture of consumer rights must match the architecture of data collection.

The Disney settlement applied Identity Symmetry to cross-device opt-out propagation, holding that a company capable of linking a single consumer across platforms for advertising purposes must suppress that consumer's data across the same linked systems when they opt out.

The Ford action reveals a second dimension of the same principle: the friction asymmetry problem. Ford's vehicle and digital services had no difficulty collecting, linking, and monetizing data from connected vehicles without requiring users to verify their identity at the point of data collection. Yet when consumers sought to exercise their right to opt out, Ford imposed a verification barrier, creating an asymmetry in the operational ease of data collection versus the operational difficulty of exercising opt-out rights.

> ### The Ford Corollary to Identity Symmetry
> The ease of exercising privacy rights must match the ease of data collection. If your systems collect data without friction, whether passively, continuously, or automatically, your opt-out process cannot introduce friction that data collection does not require. Regulators are measuring the effort consumers must expend to opt out against the effort businesses expend to collect data.

Together, Disney and Ford define a comprehensive enforcement framework in which California regulators evaluate opt-out compliance across two axes: (i) scope–do opt-outs propagate across all environments in which data is collected and monetized? and (ii) friction–does the opt-out process impose burdens that data collection does not? Businesses must now assess their compliance posture on both dimensions.

4. What the Ford Order Requires and What It Signals

In addition to the monetary penalty, Ford must take the following steps:

- Provide consumers with easy methods to submit opt-out requests with minimal steps for both digital properties and connected vehicle services.
- Process opt-out requests without requiring email verification or other identity confirmation steps that are not permitted under the CCPA.
- Conduct a comprehensive audit of tracking technologies deployed on its website.
- Implement and honor GPC signals as a valid opt-out mechanism.

The GPC requirement deserves particular attention. The GPC is a browser- and device-level signal that consumers can activate to communicate their opt-out preference automatically without taking action on each individual website or platform. CalPrivacy has consistently treated GPC compliance as a nonnegotiable requirement–and the Ford order reaffirms that businesses must technically implement GPC recognition, not merely disclose an intent to do so.

5. Broader Enforcement Trajectory: What CalPrivacy Is Building

The Ford and Honda actions are not ad hoc responses to individual complaints; they are outputs of a structured enforcement sweep, which means CalPrivacy appears to have done the i
nvestigative work on connected vehicle manufacturers and is in a position to bring additional actions rapidly. More broadly, CalPrivacy has demonstrated a clear enforcement methodology: It announces sector-specific investigatory sweeps publicly, conducts systematic reviews, and then brings enforcement actions sequentially. This approach gives the agency both deterrence value (putting entire sectors on notice) and enforcement efficiency (applying the same legal analysis to multiple companies).

Businesses in the sectors CalPrivacy has identified, such as connected vehicles, streaming, mobile, loyalty programs, surveillance pricing, and employee data, should treat the public sweep announcements as the functional equivalent of a preliminary investigation notice. Waiting for an individual enforcement action to begin before conducting internal compliance reviews is not a defensible posture.

6. Immediate Action Items for Your Organization

1	Audit Your Opt-Out Verification Requirements Review every consumer-facing opt-out workflow, including those managed by third-party CMPs or vendor platforms, to confirm that email verification, account login, or other identity confirmation steps are not required before opt-out requests are processed. Vendor defaults may be noncompliant; do not assume otherwise.
2	Confirm Opt-Out and Verification Request Types Are Technically Separated Your consumer rights platform must be configured to distinguish between verifiable requests (delete, know, correct) and unverifiable requests (opt out of sale/sharing). If your system processes all requests through the same verification workflow, this is likely a CCPA violation requiring immediate remediation.
3	Implement and Technically Verify Global Privacy Control Compliance GPC recognition must be implemented in a technically meaningful way, not merely disclosed in a privacy policy. Test whether GPC signals received by your website or application actually suppress downstream data transmission, including to advertising partners, analytics providers, and data brokers.
4	Map Opt-Out Propagation Against Your Data Collection Architecture Apply the Identity Symmetry framework from our Disney alert wherever your systems collect or share consumer data across devices, platforms, services, or advertising ecosystems, by confirming that a single opt-out request propagates to all of those environments. Scope gaps are a principal enforcement risk.
5	Apply Heightened Scrutiny to Connected or Internet of Things Products If your business offers connected vehicles, smart devices, wearables, or any product that collects data passively or continuously, conduct a specific opt-out architecture review for those products. CalPrivacy has signaled that connected product data collection is a priority enforcement area.
6	Audit Tracking Technologies and AdTech Integrations Ford was required to audit its tracking technologies as part of the settlement. Proactively conduct this audit now, documenting all tracking pixels, SDKs, cookies, and third-party integrations deployed on your digital properties, and confirm that opt-out signals suppress data transmission across all of them.
7	Review Your CMP Configuration With Your Vendor Many CMP vendors offer customizable opt-out flows but default to configurations that may require verification steps. Contact your CMP vendor specifically to confirm that opt-out requests are configured to process without verification, and to obtain written documentation of the configuration.

7. Some Operational Perspective

The Ford action reinforces a theme that has defined California privacy enforcement across the past several enforcement cycles: Procedural architecture matters as much as substantive compliance. CalPrivacy and the California AG are not primarily asking whether a business has a privacy policy or even whether it has an opt-out

button; they are asking whether the opt-out actually works technically, operationally, and at the same level of sophistication as the data collection it is designed to address.

This is precisely the enforcement environment in which we are designed to operate. Our team includes former chief information security officers, certified privacy engineers, and technical practitioners who evaluate opt-out architecture at the engineering layer, not merely at the legal documentation layer. We can help your organization conduct the kind of technical opt-out audit that CalPrivacy is now functionally requiring and position you to demonstrate good-faith compliance before enforcement attention arrives.

For context on the systemic Identity Symmetry framework underlying these enforcement actions, we encourage you to review our prior client alert California Attorney General Secures Record CCPA Settlement: Cross-Device Opt-Outs Now a System-Level Obligation.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data Privacy, Security, Safety & Risk Management
T: 202.753.3825 / 703.283.3515
amushahwar@lowenstein.com

TRICIA Y. WAGNER CIPP/US, CISSP, CISA
Counsel
T: 202.753.3658 / 916.201.7657
twagner@lowenstein.com