

CALIFORNIA PRIVACY AGENCY CRACKS DOWN ON ANOTHER BUSINESS FOR DEFICIENT OPT-OUT PRACTICES: 3 ACTION STEPS FOR YOUR COMPANY

Insights
Mar 12, 2026

California Privacy Agency Cracks Down on Another Business For Deficient Opt-Out Practices: 3 Action Steps For Your Company

For the second time in a week, California privacy regulators announced a significant fine against a business for failing to satisfy California Consumer Privacy Act's (CCPA) "clear and conspicuous" opt-out requirements. The California Privacy Protection Agency fined Ford Motor Company \$375,000 fine on March 5, finding that the automaker's process for letting consumers opt out of having their personal information sold or shared created "unnecessary friction" in violation of the CCPA. These back-to-back enforcement actions should serve as a wake-up call for businesses to ensure their opt-out policies can withstand regulators' scrutiny. What happened in this matter, and what lessons can you learn from the fine?

What Happened?

The agency found that Ford's opt-out process required consumers to verify their email address prior to opting out of the sale and/or sharing of their personal information. If consumers did not complete the email verification step, Ford did not process their opt-out request.

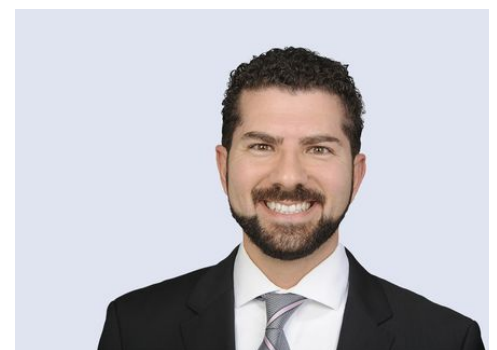
Per CalPrivacy, adding this additional step to the opt-out process runs afoul of the principle that "opting out is supposed to be easy." The fact that Ford inserted email

Related People



Logan S. Booth, CIPP/US
Of Counsel

720.644.2889



Usama Kahf, CIPP/US
Partner

949.798.2118

verification into the opt-out process was deemed to “discourage consumers from exercising their privacy rights.”

In [announcing the settlement agreement](#), CalPrivacy announced the following actions against Ford:

- **Levying a fine of \$375,703.**
- **Requiring Ford to change its practices** by ensuring opt-out processes have minimal steps.
- **Mandating that Ford audit its tracking technologies** and comply with opt-out preference signals.

CalPrivacy announced this fine not even a week after it announced a \$1.1 million settlement agreement with PlayOn Sports for having an inadequate opt-out mechanism. [You can read about that settlement here.](#)

3 Key Action Steps

CalPrivacy’s action against Ford is a reminder that the agency will continue to focus on opt-out requirements – and will take punitive action when a company’s processes run afoul of the CCPA. To comply with the law, companies should:

1. Examine your organization’s opt-out procedures: You should proactively review what is required for customers to opt-out of sharing their personal information and remove any steps that could be construed as unnecessary. The agency has demonstrated it will not tolerate unjustifiable or unwarranted roadblocks in the opt-out process.

2. Apply a business-oriented mindset: In highlighting the issues with Ford’s policy, CalPrivacy interestingly chose to couch its reasoning in commercial analogy. The Agency said that in the same way “unnecessary steps in the checkout process can discourage consumers from completing a purchase,” (which, obviously, no business would want), superfluous requirements in the opt-out process can impede consumers’ ability to protect their privacy. In short, if it’s a step that your business wouldn’t include to generate business, it likely will fail to meet the CCPA’s requirements in terms of promoting privacy rights.

Service Focus

Consumer Privacy Team

Privacy and Cyber

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

3. Account for the increased focus on connected technologies: As vehicles become more “connected,” auto manufacturers can obtain vast troves of data on their customers. In response, CalPrivacy has instructed the Enforcement Division to thoroughly review the data privacy practices of connected vehicle manufacturers, and has taken [similar actions](#) against other companies for violating the CCPA. While these recent actions have focused on automobiles, the same logic could be applied to any connected device – be it a smartwatch, fitness tracker, or cell phone – that gives businesses access to tracking or other personal information. If these technologies and capabilities apply to your organization, you should review your data protection and privacy policies to align with the CCPA’s requirements.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to [Fisher Phillips’ Insight System](#) to get the most up-to-date information direct to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our [Privacy and Cyber](#) team.