Insights, News & Events

SLING TV SETTLES CALIFORNIA PRIVACY ALLEGATIONS FOR $530K AS ENFORCEMENT EXPANDS: 6 STEPS TO AVOID SIMILAR PENALTIES

Insights
Nov 7, 2025

California's Attorney General has been taking swift action against businesses that make it difficult for consumers to opt-out of data collection practices. In a lawsuit filed last week, the AG claimed that streaming service Sling TV violated the California Consumer Privacy Act (CCPA) by failing to provide consumers with an easy opt-out method to prevent the company from selling and sharing their personal information. Additionally, the AG claimed that the company failed to implement adequate protocols aimed at protecting children's data. Sling TV recently paid a $530,000 settlement and agreed to implement changes to resolve those allegations. Here's what businesses need to know about this lawsuit and settlement and six steps you can take to avoid similar enforcement actions.

Breakdown of the Lawsuit and Settlement

Here are the key facts in *People v. Sling TV*, according to California Attorney General Rob Bonta's October 30 complaint, and the recent settlement.

- Sling TV offers paid subscription plans and a free ad-supported streaming service for live and on-demand sports, movies, and shows. Advertising is included across both the paid and free versions.
- Sling TV collects first-party data directly from its customers and sells or shares it with third parties for targeted advertising purposes. It also purchases data about its customers and their households from various third parties, including information such as location,

Related People

Vivian Isaboke, CIPP/US, CIPM
Associate
908.516.1028

Usama Kahf, CIPP/US
Partner
949.798.2118

interests, and detailed demographic and psychographic attributes.

- Sling TV combines both the first-party and third-party customer data to create an enhanced data set for targeted advertising purposes, a process also known as cross-context behavioral advertising.
- As a result, Sling TV is able to maximize its advertising profits by providing advertisers with opportunities to precisely target consumers on Sling TV's platform.

The Alleged CCPA Violations

Sling TV's website and app design choices allegedly made it difficult for consumers to exercise their CCPA opt-out right, which allows consumers to direct a business not to sell or share their personal information for targeted advertising. Specifically:

- Instead of a direct "Do Not Sell My Personal Information" link, Sling TV provided a "Your Privacy Choices" link that led users to cookie preferences, which do not constitute a valid CCPA opt-out from the sale and sharing of consumers' personal information.
- Consumers who wanted to fully opt out were unnecessarily burdened with a multi-step process and confusing forms. The company also allegedly used deceptive controls or "dark patterns" that misled consumers into believing their personal information was no longer being shared when it actually was.
- Sling TV also allegedly failed to provide sufficient privacy protection for children, including giving parents adequate information and tools to protect their children's personal information.

The Settlement

Sling TV agreed to pay a $530,000 settlement and implement changes. The company agreed to:

- Cease sending consumers to cookie preferences when they are attempting to exercise opt-out rights.
- Not require logged-in customers to submit information already available to the business.

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT

Associate

858.964.1582

Service Focus

Consumer Privacy Team

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

- Provide opt-out on “living-room devices” and not require consumers to visit Sling TV’s website to opt-out.
- Allow parents to create a “kid’s profile” with sale and sharing turned off by default.

Provide clear disclosures and tools to parents so they can protect their children’s privacy.

6 Steps to Avoid Penalties Under the CCPA

To help ensure CCPA compliance requirements are met, businesses should consider taking the following six steps:

1. Provide a Clear Opt-Out Mechanism. Make it easy for consumers to opt-out from selling or sharing their personal information. A link to general cookie preferences is not enough under the CCPA. As AG Bonta emphasized, “businesses should not bury the CCPA opt out with other choices, like cookie preferences, that do not provide the same broad directive to stop selling or sharing data.”

2. Minimize the Steps to Opt-Out. In this case, the California Attorney General alleged that consumers who wanted to fully opt out were unnecessarily burdened with a multi-step process and confusing forms.

3. Evaluate Your Practices for Dark Patterns. One key issue under the CCPA is “dark patterns.” A dark pattern is a design that effects to substantially subvert or impair user autonomy, decision making, or choice. Practices that are thought to make it even marginally harder for a consumer to exercise privacy rights or which are meant to prod consumers in a particular direction can be in the crosshairs.

4. Ensure Proper Controls to Protect Minors’ Personal Data. Review and comply with the CCPA’s additional requirements aimed at protecting children.

5. Train Managers and Employees on Compliance. Ensure relevant staff receive CCPA training covering consumer rights, forms and notices, and other obligations.

6. Seek Legal Guidance. It is critical for businesses to actively partner with legal counsel to manage risk and stay ahead of emerging trends.

Key Takeaways for Businesses

This lawsuit and settlement represent the latest development in a wave of enforcement activity in California and beyond. For example:

- Officials from California, Colorado, and Connecticut announced in September a coordinated investigative sweep targeting companies whose websites may be ignoring automatic opt-out preference signals that users can configure in their browsers.
- The California Privacy Protection Agency (CPPA) is promoting awareness to consumers on how to use opt-out preference signals (OOPS), following a compliance campaign aimed at businesses subject to the CCPA.
- Earlier this year, AG Bonta announced an investigative sweep into whether location data businesses (such as advertising networks, mobile app providers, and data brokers) subject to the CCPA offer and implement consumers' right to stop the sale and sharing of personal information, particularly when it is geolocation data.

Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. You can also visit FP's US Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group or Consumer Privacy Team.

Our team is ready to help you respond to any inquiry you may receive. The Fisher Phillips Consumer Privacy Team can help you assess your current state of CCPA compliance and respond to any inquiry in a manner that best protects your business.