Insights, News & Events

CCPA CRACKDOWN CONTINUES: MOBILE APP MAKER FINED $1.4 MILLION FOR OPT-OUT NONCOMPLIANCE

Insights
Dec 1, 2025

A mobile gaming company just agreed to pay $1.4 million and implement corrective measures to resolve allegations that it violated the California Consumer Privacy Act (CCPA), another reminder that mobile apps and digital platforms are in the crosshairs of the state's Attorney General. Announced on November 21, the settlement with Jam City, Inc., is yet another cautionary reminder that any business offering app-based tools must provide clear and accessible privacy rights to users. According to AG Rob Bonta, Jam City failed to offer users a method to opt-out of the sale or sharing of their personal information across more than 20 gaming apps. The gaming company also allegedly sold or shared the data of minors ages 13 to 16 without the required opt-in consent. Here's what your company can learn from the Jam City settlement.

The Alleged CCPA Violations

Jam City develops and operates mobile games tied to major entertainment brands such as *Frozen*, *Harry Potter*, and *Family Guy*. The AG alleged the company collected personal information from users within its apps and disclosed it to third-party advertising partners to deliver personalized ads. The state's investigation found three core CCPA violations:

1. Failure to Provide a Valid Opt-Out Method

None of Jam City's 21 apps offered an in-app mechanism allowing users to direct the company to stop selling or sharing their personal information. For mobile-first businesses, the AG emphasized that opt-out tools must be

Related People

Darcey M. Groden, CIPP/US

Partner

858.597.9627

Chelsea Viola

Associate

213.403.9626

accessible directly within the app, not just an external website.

2. Selling or Sharing Minors' Data Without Consent

The AG found that some of Jam City's apps sold or shared the personal information of minors aged 13 to 16 without first obtaining affirmative opt-in consent from those users, violating the CCPA's heightened protections for minors.

3. Opt-Out Options Weren't Easy to Find or Access

Jam City's apps did not provide a clear or easy-to-navigate way for users to exercise their privacy rights, according to the AG. The CCPA requires that opt-out mechanisms be simple, transparent, and accessible.

The Settlement

To resolve the allegations, Jam City agreed to a $1.4 million payment and to correct the issues identified by the AG above, in addition to enhancing disclosures to help users understand how their personal information is collected, shared, and used for advertising.

A Growing Trend: CCPA Enforcement Targets Mobile Apps Digital Platforms

The Jam City settlement is part of a broader enforcement t aimed at businesses that operate through mobile apps or re heavily on digital tracking and advertising technologies. Se recent actions reflect regulators' increasing scrutiny of app ecosystems, children's privacy, and ad-supported platform

- Sling TV (October 2025): $530,000 settlement for failing provide an easy-to-use opt-out and insufficient protectio children.
- Healthline (July 2025): $1.55 million settlement for impro targeted advertising involving sensitive health-related da
- Tilting Point Media (June 2024): $500,000 settlement fo collecting and sharing children's data without parental co a mobile game.

Attorney General Bonta has also conducted investigative sv targeting mobile apps, ad-tech practices, location data pro

Service Focus

- California Litigation and Appellate
- Consumer Privacy Team
- Litigation and Trials
- Privacy and Cyber

Related Offices

- Irvine
- Los Angeles
- Sacramento
- San Diego
- San Francisco
- Silicon Valley
- Woodland Hills

streaming services, and businesses that may be ignoring o
preference signals.

What Should Businesses Do Now?

To stay ahead of enforcement trends and reduce the risk of similar allegations, businesses should consider taking the following steps now:

1. Audit All Opt-Out Mechanisms.

Review your websites, mobile apps, and connected devices to ensure consumers can easily find and use a valid CCPA opt-out. For app-based businesses, confirm opt-outs function directly within the app itself. Even in apps, businesses are required to provide an opt-out link which states "Do Not Sell or Share My Personal Information" or to provide the alternative opt-out link.

2. Implement or Strengthen Guardrails for Minors.

If any portion of your product or service is accessible to consumers under age 16, ensure you have compliant opt-in options and clear disclosures. (For consumers under the age of 13, consent for the sale of personal information must be obtained from a parent or legal guardian rather than from the minor consumer.) Review age-screening processes and parental tools, if applicable.

3. Review Contracts With Ad-Tech and Analytics Partners.

Ensure all agreements include CCPA-required terms, limit downstream use of data, and contain appropriate representations and audit rights. Verify that partners' practices align with what you disclose to consumers.

4. Evaluate User Experience for Potential Hiccups.

Examine whether your design choices unintentionally create friction, confusion, or misleading pathways for consumers attempting to exercise privacy rights.

5. Provide CCPA Training for Key Teams.

Marketing, product, engineering, and customer support teams play hands-on roles in implementing privacy controls. Ensure they understand opt-out requirements, minors' protections, and how data is handled across systems.

Conclusion

We will continue monitoring developments in this area as CCPA enforcement efforts expand. If you have questions about this settlement or would like assistance evaluating your data privacy practices, 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. To stay informed, subscribe to Fisher Phillips' Insight System and visit FP's U.S. Consumer Privacy Hub for additional compliance resources.