Insights, News & Events

CALIFORNIA PRIVACY AGENCY HITS STUDENT TICKETING COMPANY WITH $1.1M FINE: 3 LESSONS ABOUT TRACKING CONSUMERS

Insights
Mar 5, 2026

California Privacy Agency Hits Student Ticketing Company With $1.1M Fine: 3 Lessons About Tracking Consumers

In what state officials call their first decision to address privacy violations involving students and California schools, the California Privacy Protection Agency just announced a $1.1 million fine against PlayOn Sports for its consumer tracking practices. The February 27 statement from CalPrivacy alleges that PlayOn's digital platform, which allows students to purchase tickets to high school functions like sporting events, dances, and arts performances, required users to agree to tracking technologies without offering a sufficient way to opt out. What happened and what are the three key lessons you can learn from this fine about tracking?

What Happened?

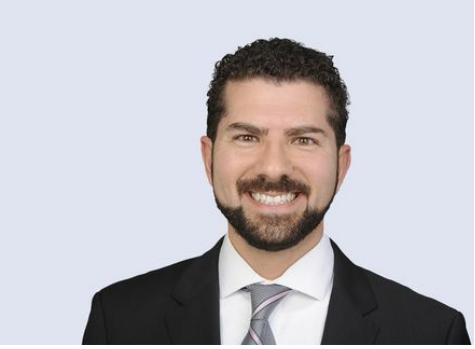
PlayOn Sports operates GoFan, a digital platform that sells tickets to high school sporting events, dances, and arts performances across California and other states. When students and parents used the platform, they were required to agree to terms allowing PlayOn to track their online activity through cookies and similar technologies for advertising purposes.

CalPrivacy's investigation found three violations:

Related People

Logan S. Booth, CIPP/US
Of Counsel

720.644.2889



Usama Kahf, CIPP/US
Partner

949.798.2118

- **Inadequate Opt-Out Mechanism:** PlayOn directed users to third-party websites (the Network Advertising Initiative and Digital Advertising Alliance) to opt out of tracking, rather than providing a direct way to opt out on the GoFan platform itself. CalPrivacy found this violated the California Consumer Privacy Act (CCPA) requirement that businesses provide consumers a "clear and conspicuous link" to opt out.
- **Failure to Honor Opt-Out Preference Signals:** The platform didn't recognize or respond to Global Privacy Control (GPC) signals – automated browser settings that tell websites not to sell or share personal information. Under the CCPA, businesses must honor these signals.
- **Deficient Privacy Notices:** PlayOn's privacy notices failed to adequately inform users about what personal information was being collected and how it would be used.

Under the settlement, PlayOn agreed to pay $1.1 million and implement corrective measures, including building native opt-out mechanisms and honoring opt-out preference signals.

3 Key Takeaways

School-aged children are one of the most digitally integrated generations in the United States, making it likely that companies will continue to develop platforms to cater to their needs, interests, and lifestyles. This means that businesses targeting this market would be wise to heed the guidance offered in CalPrivacy's decision to mitigate risk:

1. Children are afforded enhanced protection: CalPrivacy specifically noted that "students are a uniquely vulnerable population whose data should be used to enhance their own learning, not to fuel advertising and commercial surveillance." As such, your organization should understand that children-oriented platforms will receive enhanced scrutiny, and be ready to articulate a clear nexus between the data you're collecting on students and the educational rationale for its collection.

2. Offloading opt-out processes is insufficient: If a digital platform is going to collect personal information covered by the CCPA, it must offer users a native means to opt out. Directing users to third-party providers is not a valid alternative. California officials have made it clear that if your

Service Focus

Privacy and Cyber

Industry Focus

Education

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

organization is sophisticated enough to gather the information, it is sophisticated enough to develop its own means by which users can disenroll.

3. An investigation into one infraction can lead to penalties for others: Beyond citing PlayOn for its inadequate opt-out methods, CalPrivacy also sanctioned the company for two other violations: failing to recognize and honor opt-out preference signals, and falling short of privacy notice requirements. This shows that once California privacy regulators initiate an investigation, they're empowered to assess the organization's CCPA compliance beyond the scope of the initial allegation. If officials uncover multiple abuses, punitive measures will correspondingly increase.

Next Steps

The best way to insulate your organization from CCPA violations is to implement a robust data protection compliance program. Engaging data privacy attorneys is a great first step. They can assist you by:

- Auditing what personal information your business gathers;
- Determining which laws and regulations apply;
- Identifying gaps in existing practices; and
- Designing, developing, and deploying enterprise-wide compliance programs.

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.