PUBLICATION

California AG Secures Landmark Privacy Settlement Over Tracking: What It Means for Your Website

Authors: Matthew George White, Alisa L. Chestler
July 07, 2025

In a record-setting enforcement action under the California Consumer Privacy Act (CCPA), the California Attorney General (AG) announced a $1.55 million settlement with Healthline Media, a popular online publisher of health and wellness content. The settlement – the largest to date under the CCPA – includes not only monetary penalties but also stringent injunctive relief targeting the company's online tracking and advertising practices. While ad tech enforcement has been building for years, this is the first time California has drawn a clear line in the sand around how website tracking must function in practice. The implications for publishers and other businesses are immediate and far-reaching, particularly where there is the potential for personal information, such as health concerns or financial data, to be impacted.

The Allegations: Sharing Diagnoses Through Pixels

According to the AG's complaint, Healthline failed to honor consumer opt-outs of data sharing, including Global Privacy Control (GPC) signals, and shared personal information with advertisers in ways that allowed them to infer a user's specific medical condition based on the titles of articles they read – such as "Newly Diagnosed with HIV?" or "The Ultimate Guide to MS for the Newly Diagnosed." The site's consent banner purportedly allowed users to disable tracking, but the backend told a different story. Even after users opted out, Healthline allegedly continued to transmit identifiers and article titles to third parties for cross-context behavioral advertising.

These disclosures, the AG argued, violated several core CCPA provisions, including:

- failure to process valid opt-out requests (Civ. Code §§ 1798.120, 1798.135);
- sharing personal information without contracts that meet CCPA standards (Civ. Code § 1798.100(d));
- violating the "purpose limitation" principle by using data in ways consumers would not reasonably expect (Civ. Code § 1798.100(c)); and
- misleading consumers through a non-functional cookie banner (Bus. & Prof. Code § 17200).

The Settlement: Beyond the Financial Penalty

The settlement does more than impose a $1.55 million fine – it redefines the boundaries of compliant ad tech use in California. This is the largest monetary penalty ever obtained by the California AG under the CCPA, signaling that privacy violations tied to health-related inferences are not just technical foot faults – they're high-stakes regulatory risks. But the true weight of the settlement lies in the scope of its injunctive provisions, which will require Healthline to reengineer fundamental aspects of its website architecture, advertising practices, and third-party relationships.

- ***Mandatory GPC Compliance***: Healthline must process opt-out preference signals like the GPC and test mechanisms to ensure they function as intended.

- ***Contractual Scrutiny***: The company must audit contracts with advertising and analytics partners and confirm that all CCPA-required terms are in place.

- ***Sensitive PI Disclosures***: If Healthline uses or shares sensitive personal information for advertising purposes, it must provide clear notice and allow consumers to limit that use.

- ***Ban on Disclosing Diagnosis-Based Article Titles***: Healthline is prohibited from sharing personal information in a way that reveals the titles of "Diagnosed Medical Condition Articles," which include dozens of specifically named health-related articles.

- ***Ongoing Oversight***: For three years, Healthline must file annual reports with the AG detailing contract compliance, opt-out testing, and data practices.

Context: A Converging Front of Regulatory and Litigation Pressure

California's AG has now brought four CCPA enforcement actions and more should be expected. In parallel, private plaintiffs have brought hundreds of wiretap and privacy lawsuits under statutes like the California Invasion of Privacy Act (CIPA), many based on similar tracking technologies.

This action also signals an evolution in California's regulatory approach: moving beyond mechanical violations to target disclosures that regulators deem "unexpected," "intimate," or "offensive" – even when buried in a privacy policy. It's a warning shot to businesses that handle consumer health or similarly sensitive data, regardless of regulatory schemes such as HIPAA, FCRA, and GLBA, to name a few.

Why This Matters – and What You Should Do

This isn't just another settlement – it's a blueprint. Regulators are no longer satisfied with boilerplate privacy policies and symbolic opt-out links. They're following the data, testing the tech, and demanding verifiable compliance. If your website uses tracking technologies – especially in health, finance, or other sensitive industries – this action puts you on notice.

Regulators are watching, and plaintiffs' attorneys are following closely behind.

Five Action Items to Prioritize Now:

1. Audit Tracking Technologies

Use a tool (or engage experienced outside counsel) to identify all third-party pixels, cookies, and trackers deployed on your site – especially those that transmit URL paths, page titles, or other personal or sensitive information.

2. Validate Consent Mechanisms

Ensure your cookie banner is operational, legally accurate, and aligns with actual back-end behavior. Simulate opt-out flows, including GPC signals, and validate that tracking ceases when and how it should.

3. Review Ad Tech Contracts

Confirm that you have contracts in place with all third parties receiving personal information via tracking technologies. In California, these must include CCPA-required terms, including limits on use and obligations to honor opt-outs (increasingly required in other states and industries as well).

4. Limit Disclosures of Sensitive Inferences
Avoid disclosing page titles or URLs that could be used to infer sensitive information (e.g., medical, financial, sexual orientation). Consider filtering or hashing such data before transmission.

5. Update Privacy Disclosures
Review and revise your privacy policy to clearly explain what data is collected, who it's shared with, and how consumers can exercise their data rights.

Final Thoughts

This action is a cautionary tale that every company should be paying attention to. A $1.55 million price tag, sweeping operational mandates, and three years of regulatory oversight – all because pixels were quietly doing more than they should have. If your site uses tracking technologies, especially around sensitive content like health or finance, you're not flying under the radar. Regulators are inspecting your backend, not just your banner. Compliance isn't about what you say in your privacy policy – it's about what your tech stack actually does. In the words of the complaint: "***trust – but verify"*** that your privacy program does what your website says it does.

If you're unsure whether your website's tracking practices could survive regulatory scrutiny – or if you're looking to proactively reduce litigation risk – now is the time to act. Our team has deep experience guiding clients through ad tech investigations, updating consent flows and privacy notices, and defending against wiretap and CCPA class actions. Whether you need a rapid risk assessment, a remediation plan, or representation in an enforcement or litigation matter, we're ready to help you protect your brand, your bottom line, and your users' trust.

Don't wait for a demand letter or regulator's subpoena – contact the authors, Matt White, AIGP, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, Alisa Chestler, CIPP/US, QTE, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team today, and make sure you're prepared before regulators – or plaintiffs – come knocking.