Cybersecurity and Data Privacy Update

State Privacy Enforcement Accelerates, With California Targeting Substantive Compliance and Connecticut Bringing Its First Action

As federal privacy enforcement shows signs of slowing, states are aggressively stepping in to fill the void.

On July 1, 2025, the California attorney general (AG) announced a $1.55 million settlement with Healthline Media, a prominent health information publisher. The settlement imposes novel restrictions on Healthline's data practices, extending beyond the requirements of the California Consumer Privacy Act (CCPA), and signals a new emphasis on substantive compliance and not just procedural missteps. The settlement also offers a window into the California AG's enforcement approach, including a broad interpretation of what constitutes sensitive data and a reliance on technical forensic analysis.

California is not alone in this uptick in state enforcement: On July 8, 2025, the Connecticut AG announced its first enforcement action under the Connecticut Data Privacy Act (CTDPA), targeting a business whose procedures the prosecutors had been testing.

Both settlements highlight a sharpened focus among state regulators on enforcing their privacy regimes, a trend we have previously noted. See our May 5, 2025, client alert "Key Themes From the 2025 IAPP Global Privacy Summit" and our May 2, 2025, client alert "Eight-State Consortium of Privacy Regulators Marks Shift Toward Coordinated Enforcement."

Beyond Checklists: Healthline Settlement Focuses on Substantive Data Practices

California AG Takes Expansive View of What Could Constitute 'Inferred' Health Information

The California AG's action against Healthline centered on the use of cookies and similar technologies for targeted advertising — what the CCPA terms "cross-context behavioral advertising." The AG's allegations included:

- **Failure to honor opt-outs.** Despite users opting out via the website's cookie banner, the "Do Not Sell or Share My Personal Information" link, and the Global Privacy Control (GPC) signal, Healthline's website continued to place cookies and pixels from third-party advertisers due to a misconfiguration of Healthline's opt-out mechanism. Not only was this a violation of the CCPA, but the AG alleged that Healthline misled consumers by offering this non-functional cookie consent banner, violating the state's consumer protection statute.

State Privacy Enforcement Accelerates, With California Targeting Substantive Compliance and Connecticut Bringing Its First Action

- **Violation of "purpose limitation principle" for inferred health-related information.** Healthline was accused of violating the CCPA's "purpose limitation principle" when it shared with advertisers the titles of articles consumers viewed that reference illness diagnoses (*e.g.*, "The Ultimate Guide to MS for the Newly Diagnosed," and "Newly Diagnosed with HIV? Important Things to Know.") According to the California AG, such article titles could reveal health-related information about the reader to third parties in a manner inconsistent with consumer expectations, as that practice was not disclosed to consumers.

- **Inadequate vendor contracts.** The California AG alleged that Healthline's agreements with advertising partners lacked CCPA-mandated terms for the selling or sharing of personal information for targeted advertising, such as specifying the limited purposes for which personal information could be used and obliging vendors to honor opt-out preferences expressed through the "U.S. Privacy String."

The complaint was also notable for relying on technical evidence, referencing the number of cookies and pixels placed, transmitting data to third parties, and investigating downstream vendors. This suggests a growing reliance on forensic audits in regulatory investigations.

California AG Extends Settlement Obligations Beyond Correcting Past Violations

In a departure from previous CCPA settlements, the Healthline agreement imposes obligations that exceed the CCPA's minimum requirements, including:

- **Prohibition against selling or sharing article titles.** Alongside general CCPA compliance requirements, the settlement categorically prohibits Healthline from selling or sharing data that reveals a consumer is viewing a "Diagnosed Medical Condition Article," which is defined as an article with a title or URL that indicates the consumer visiting the article has already been diagnosed with a medical condition. While the CCPA permits such sharing provided consumers are notified and given the right to opt out, the settlement goes further by barring the practice outright. In addition, should Healthline choose to disclose "sensitive personal information" for advertising purposes, it now must provide a Notice of Right to Limit Use and Disclosure of Sensitive Personal Information. Although the settlement stops short of explicitly classifying the viewing of a "Diagnosed Medical Condition Article" as "sensitive personal information," the settlement's context suggests that the California AG views article metadata as such.

- **Prohibition against the sale or sharing of titles, which would otherwise be permitted.** This provision represents a shift from prior CCPA settlements, which primarily imposed requirements to ensure future compliance with the law. For example, the California Attorney General's $1.2 million settlement with Sephora requires the company to clarify in its online disclosures to consumers that it sells personal information, and the company must also honor consumer's rights to opt out of sales and sharing, including requests made through the GPC — all explicit CCPA requirements. Similarly, the California Privacy Protection Agency's $632,500 settlement with Honda requires the company to request the minimum information necessary to process consumer rights requests, honor opt-outs expressing through a GPC signal, and provide symmetry in choice related to cookie preference, among other requirements — all ties to specific compliance with the CCPA. The Healthline settlement, by contrast, requires the company to refrain from conduct otherwise permitted by law, foreshadowing a new direction for California privacy enforcement.

First Enforcement Action Under the Connecticut Data Privacy Act

The Connecticut AG also signaled a turn to enforcement, announcing a settlement with TicketNetwork, Inc. over allegations that the ticket seller failed to provide a CTDPA-compliant privacy notice and did not address deficiencies after receiving multiple cure notices.

The state AG's office conducted "privacy notice sweeps," issuing over two dozen cure notices to different companies. TicketNetwork was singled out for repeatedly claiming to have resolved deficiencies when it had not, and for failing to respond promptly to follow-up correspondence. The episode underscores the importance of timely and substantive engagement with regulatory inquiries. See our May 5, 2025, client alert "Key Themes From the 2025 IAPP Global Privacy Summit."

Key Points for Businesses

In the absence of federal action, state regulators are likely to continue filling the gap. To mitigate risks, companies should consider the following:

- **Develop and publish compliant privacy notices.** Businesses must provide accurate descriptions about personal information practices in privacy notices that reflect personal information use and sharing practices. Reviewing these privacy notices regularly can ensure they accurately describe data practices and include all terms required by the law.

State Privacy Enforcement Accelerates, With California Targeting Substantive Compliance and Connecticut Bringing Its First Action

- **Mandate end-to-end testing of opt-outs.** Businesses should not rely on a vendor's assurances of compliance. A program for documenting continuous, automated testing of all consumer opt-out mechanisms, including the GPC, cookie banners, and "Do Not Sell/Share" links can address this vulnerability. This "trust, but verify" approach should include detailed logs of any failures and remediation steps taken.

- **Verify downstream signal compliance.** Passing on a consumer's opt-out request is insufficient. To ensure that requests are honored, a business can map data flows with third parties and contractually obligate third parties with whom it sells or shares personal information to process and document compliance with technical opt-out signals that it receives from consumers and the business.

- **Audit all vendor contracts.** Agreements with service providers and third parties may not include all terms required by the CCPA, including language designating the specific, limited purpose for processing. Businesses should designate specific roles or individuals responsible for ongoing contract review and compliance.

- **Classify and control data.** Business operations that generate data from user activity (*e.g.*, browsing history, purchase patterns) can be assessed for their capacity to reveal sensitive information about the individual, such as health diagnoses. This data may need to be subject to heightened controls, stricter sharing limitations, and a risk assessment to ensure its use aligns with reasonable consumer expectations and company disclosures.

Contacts

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Dana E. Holmstrand
Associate / Washington, D.C.
202.371.7014
dana.holmstrand@skadden.com

Lisa V. Zivkovic
Associate / New York
212.735.2887
lisa.zivkovic@skadden.com