AN A.S. PRATT PUBLICATION
MAY 2026
VOL. 12 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 4** **May 2026**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

California Consumer Privacy Act Enforcement in Review: Ensuring Privacy Programs Work in Practice

By Ashleigh Bickford and Gregory J. Leighton

In this article, the authors explain that California has gotten more aggressive on privacy and that regulators now expect privacy tools to work in practice — not just on paper. The authors add that California regulators are testing opt-outs, vendor contracts and employee notices for real-world performance.

Enforcement of the California Consumer Privacy Act (CCPA) entered a new and more assertive phase in 2025, with regulators focusing on how privacy practices actually function to protect consumers. Both the California Privacy Protection Agency (CalPrivacy) and the California Attorney General (AG) played active roles in this shift. CalPrivacy issued investigations, and its first enforcement orders centered on the technical performance of opt-out mechanisms, consent tools and data subject rights portals. The AG also brought its own enforcement action, also reinforcing that CCPA compliance depends on whether business' privacy controls operate effectively, not just whether they exist on paper. For businesses subject to the CCPA, 2025 enforcement made clear that compliance turns on how privacy practices work in reality — not just how they appear online or on paper.

This article looks at a series of 2025 CCPA enforcement actions to show what regulators' "proof-of-performance" focus means for privacy compliance obligations. CalPrivacy's settlement with Tractor Supply Co. highlights increased scrutiny of privacy notices for consumers, employees and job applicants. Settlements with American Honda Motor Co. and Todd Snyder Inc. highlight expectations around CCPA-compliant vendor and adtech contracts, functioning cookie management platforms (CMPs) and opt-out tools, and right-sized identity verification. The AG's settlement with Healthline Media, LLC illustrates the CCPA's purpose-limitation principle in the context of sensitive health data, and CalPrivacy's recent Delete Act actions against multiple data brokers reinforce registration obligations.

Taken together, these developments show that regulators are increasingly focused on whether privacy programs actually work in practice to protect consumers and that they are willing to test those programs for compliance.

---

* The authors, attorneys with Polsinelli, may be contacted at abickford@polsinelli.com and gleighton@polsinelli.com, respectively.

CURRENT, ACCURATE PRIVACY NOTICES

The CCPA requires businesses to maintain privacy notices that accurately disclose the categories of personal information collected and shared; the rights available to consumers to exercise over their personal information; and clear instructions on how those rights may be exercised. These notices must reflect current practices and be updated at least annually. The CCPA is unique among state privacy laws in extending the notice requirement to job applicants and employees, meaning that businesses must prepare and maintain notices tailored to employment.

The Tractor Supply enforcement action illustrates CalPrivacy's heightened scrutiny of privacy notice compliance. CalPrivacy imposed a $1.35 million penalty — its largest CCPA fine to date — after finding that Tractor Supply's consumer-facing privacy notice failed to disclose key categories of personal information collected or shared, did not adequately describe consumer rights and did not provide instructions on how to exercise those rights. CalPrivacy also emphasized that Tractor Supply had not updated its privacy notice in four years, despite the requirement for annual review. In addition, even though the Tractor Supply Co. had job applicants and employee notices in place, the notices were found to be non-compliant because they failed to describe CCPA rights or explain how those rights could be exercised.

From a practical standpoint, the Tractor Supply action demonstrates that businesses must ensure they have current, accurate privacy notices in place, conduct annual notice reviews and treat employee and applicant notices as meaningful compliance documents — not afterthoughts.

CCPA PROVISIONS IN VENDOR AND ADTECH CONTRACTS

Businesses under the CCPA must also maintain contracts that contain certain CCPA-required data protection terms with service providers, contractors and other third parties that they disclose personal information to and be able to provide those contracts to regulators upon request. Regulators have made clear that businesses cannot rely on assumptions, generic industry frameworks or vendor assurances to satisfy these obligations. Instead, companies must be able to demonstrate, often on short notice during an audit, that each vendor relationship includes executed agreements containing the required provisions. Increasingly, the concern is not simply that the right contractual

---

[1] Commonwealth v. Kurtz, Nos. 98, 99, 100 MAP 2023 (Pa. Dec. 16, 2025), available at https://www.pacourts.us/assets/opinions/Supreme/out/J-36A-2024oajc%20-%20106611829340009817.pdf?cb=1.

[2] Carpenter v. United States, No. 16–402 (U.S. June 22, 2018), available at https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

terms are missing, but that businesses are unable to locate and produce the agreements when regulators ask.

Several 2025 enforcement actions illustrate this trend. In CalPrivacy's investigation into Honda's privacy practices, CalPrivacy found that Honda had disclosed personal information to advertising technology partners and then could not prove that they had entered into contracts that contained the required CCPA provisions. Similarly, in the AG's settlement with Healthline, the AG concluded that Healthline assumed its advertising partners had adopted industry-standard contracts but had failed to verify that the agreements included the specific terms required by the CCPA. The Tractor Supply action discussed above also involved insufficient contractual provisions with vendors handling personal information. These actions show that businesses must inventory their vendor relationships, ensure that they have these agreements on hand, identify contractual gaps and confirm that updated CCPA-compliant terms are executed and maintained across all data-sharing partnerships.

FUNCTIONING CMPS AND OPT-OUT MECHANISMS

Another focus of 2025 CCPA enforcement was that consumer-facing opt-out tools actually function and are easy for consumers to use. CalPrivacy repeatedly stressed that having a cookie banner, consent-management platform (CMP) or "Do Not Sell or Share My Personal Information" link is not enough if the underlying system does not actually honor consumer choices by stopping tracking technologies or triggering a stop on the sale or sharing of information. Regulators also focused on the "symmetry of choice" principle, which requires businesses to make it just as easy to opt-out of data collection and sharing as it is to opt-in. Applied to CMPs, designs that require users to take extra steps, contain less conspicuous opt-out options or otherwise steer consumers toward "accept all" selections may be treated as dark patterns. Even one additional click required to opt out is enough to create a more burdensome choice. In addition, the option to opt out must be just as apparent to consumers and cannot be displayed in a less conspicuous color or font than the option to opt in.

Several CalPrivacy enforcement actions last year focused on the functionality of opt-out mechanisms. In the Honda action, Honda's website cookie banner allowed consumers to "Accept All" cookies with one click, but users had to individually toggle off categories of cookies they wanted to opt out of. This extra step was deemed a "dark pattern" and non-compliant with symmetry of choice requirements. The Todd Snyder settlement similarly involved a CMP that was misconfigured for approximately 40 days, during which the banner disappeared before users could interact with it — preventing consumers from submitting opt-out requests altogether.

Healthline's enforcement action reinforced this theme: although Healthline implemented multiple opt-out mechanisms, including a "Do Not Sell or Share My Personal Information" link, CMP and Global Privacy Control signal detection, none of

the tools functioned correctly, and Healthline continued to disclose personal information to advertisers even after consumers attempted to opt out.

Collectively, these actions signal that businesses must regularly test their CMPs, cookie banners and opt-out tools; review user experience designs for symmetry-of-choice compliance; and monitor vendor-provided tools to ensure they perform as intended.

PURPOSE LIMITATION PRINCIPLE

Regulators also emphasized the CCPA's purpose-limitation principle, which requires that personal information only be used or disclosed for purposes that were disclosed at the time of collection or that consumers can reasonably anticipate. Sensitive personal information, such as data-revealing health conditions, requires special scrutiny because of the heightened risks involved.

The purpose-limitation principle is illustrated by the AG's $1.55 million settlement with Healthline. Healthline allegedly disclosed to advertisers the titles of health-related articles visited by consumers, including content suggesting specific medical diagnoses such as multiple sclerosis or HIV. Although Healthline's privacy policy referenced targeted advertising generally, it did not disclose that sensitive, health condition-revealing browsing data would be shared with third parties for targeted advertising purposes. The AG argued that consumers could not reasonably expect such sensitive information to be used for targeted advertising, and therefore, Healthline violated the purpose-limitation rule. This action underscores the need for businesses to map their data flows, identify whether any sensitive personal information is being used for advertising or analytics and ensure that their privacy notice disclosures clearly and specifically reflect these practices.

DATA SUBJECT REQUESTS AND VERIFICATION

The CCPA differentiates between consumer rights requests that require identity verification and those that do not. Requests to opt-out of the sale or sharing of personal information and requests to limit the use of sensitive personal information do not require verification. For requests to access, delete and correct personal information, the verification process must allow the business to confirm the consumer's identity to a reasonable degree of certainty — typically by matching at least two data points provided by the consumer. Regulators have emphasized that businesses must avoid collecting unnecessary additional personal information for verification purposes when consumers attempt to exercise their data subject rights.

CalPrivacy investigations have found CCPA violations where businesses required consumers to provide more information than necessary to verify their identity, or where they required verification for rights that do not. For example, in the Honda action, a violation was found when they required consumers to submit eight separate data points to verify their identity for access, deletion and even opt-out requests, exceeding what

was necessary for identify verification. Similarly, in the Todd Snyder action, CalPrivacy found a violation because the company required consumers to upload a government-issued ID to submit data subject rights requests, even for rights requests that do not require verification.

Together, these actions demonstrate that businesses must calibrate identity-verification procedures to the specific type of request and ensure that their systems for handling data subject requests are not collecting excessive or unnecessary personal information.

DATA BROKER ENFORCEMENT UNDER THE DELETE ACT

Along with consumer-facing tools, CalPrivacy also kept busy in 2025 enforcing the data broker regulations under the California Delete Act, which applies to any business that collects and sells the personal information of consumers with whom they do not have a direct relationship. The Delete Act requires data brokers to register annually with CalPrivacy and disclose certain information about the information they are collecting and selling, as well as include those same disclosures in their privacy policy. Starting in 2026, data brokers must process statewide deletion requests through CalPrivacy's centralized Delete Request and Opt-Out Platform (DROP).

In early 2025, CalPrivacy announced multiple enforcement resolutions under the Delete Act, including orders and settlements with Key Marketing Advantage, LLC, National Public Data, Inc., Background Alert, Inc. and other data brokers that failed to register timely. Penalties ranged from $46,000 to $58,500 and included daily fines for late registration, payment of attorneys' fees and costs, and in one case, a requirement that the data broker shut down its operations through 2028 or face a $50,000 penalty.

These actions signal that data broker compliance is an active enforcement priority. For data brokers the message is straightforward: confirm whether you qualify as a data broker, register on time and prepare now for the operational demands of DROP, including the need to honor large volumes of deletion and opt-out requests on a recurring basis.

CONCLUSION

Together, these enforcement actions and trends demonstrate that California is moving from a check-the-box model of privacy compliance to a proof-of-performance model. Regulators are increasingly concerned with whether tools are accessible and effective from the consumer's perspective and whether technical implementations match the promises made in privacy notices and user interfaces. To comply, businesses should:

- Regularly test consent tools to confirm that CMPs, cookie banners, GPC recognition and other opt-out mechanisms function technically — not just visually — and that these signals are honored by third-party partners.

- Ensure data-sharing contracts with vendors include all CCPA-required provisions and that downstream partners are bound to appropriate restrictions on processing and secondary use.
- Maintain symmetry of choice by ensuring that opting out is no more burdensome than opting in and by avoiding dark patterns that make opting in easier than opting out.
- Implement right-size identity verification for data subject requests to avoid over-verification while still protecting against fraud and unauthorized access.
- Maintain accurate and compliant privacy notices for consumers, job applicants and employees, and update these notices at least annually to reflect current data practices and statutory requirements.
- Monitor Delete Act obligations for any business that may qualify as a data broker, confirm registration where required, and ensure deletion workflows and request-handling processes meet statutory requirements.