AN A.S. PRATT PUBLICATION
SEPTEMBER 2025
VOL. 11 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 7** **September 2025**

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

(2025–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 Privacy Protection Agency Intensifies Enforcement: Recent Enforcement Actions and Trends

By Arsen Kourinian, Lei Shen, Amber C. Thomson and Megan P. Von Borstel*

The authors of this article explain two recent California Privacy Protection Agency enforcement actions, which reflect a strong commitment to holding businesses accountable for violations of the California Consumer Privacy Act and the California Delete Act and highlight the Agency's priorities in protecting consumer rights and ensuring data broker accountability.

The California Privacy Protection Agency (CPPA) has intensified its enforcement activities in 2025, bringing enforcement actions under both the California Consumer Privacy Act (CCPA) and the California Delete Act in the last few months. The recent enforcement actions against Todd Snyder, Inc. and Jerico Pictures, Inc. – and other actions by the agency – reflect a strong commitment to holding businesses accountable for violations of these laws, and highlight the CPPA's priorities in protecting consumer rights and ensuring data broker accountability.

ENFORCEMENT TRENDS AND PRIORITIES

The CPPA's recent enforcement actions highlight several emerging regulatory priorities:

- *Focus on Honoring Opt-Out Requests*: The CPPA has penalized businesses for failing to properly process and honor consumer opt-out of sale/sharing requests, including those submitted via cookie banners and opt-out preference signals such as Global Privacy Control (GPC).

- *Crackdown on Dark Patterns*: In September 2024, the CPPA issued an enforcement advisory targeting "dark patterns,"[1] user-interface designs that impair or subvert consumer autonomy.

- *Emphasis on Data Minimization*: An April 2024 enforcement advisory[2] emphasized data minimization as a foundational principle of the CCPA. The agency noted that some businesses collect excessive personal

* The authors, attorneys at Mayer Brown, may be contacted at akourinian@mayerbrown.com, lshen@mayerbrown.com, athomson@mayerbrown.com and mvonborstel@mayerbrown.com, respectively.

[1] https://cppa.ca.gov/pdf/enfadvisory202402.pdf.

[2] https://cppa.ca.gov/pdf/enfadvisory202401.pdf.

information when processing consumer requests, which may lead to enforcement actions.

- *Scrutiny of Data Broker Compliance Under the Delete Act*: After launching investigative sweeps to ensure data brokers comply with registration requirements under the Delete Act, the agency penalized a company for failing to register and pay an annual fee as required by the Delete Act. Noncompliance can result in administrative fines, including penalties of $200 per day.

CASE ANALYSES

Todd Snyder, Inc.

In May 2025, the CPPA ordered a national clothing retailer,[4] Todd Snyder, Inc., to change its business practices and imposed a $345,178 fine for multiple CCPA violations, including:

- Failing to properly configure its privacy portal and cookie banner, resulting in a 40-day delay in processing consumer opt-out requests.
- Requiring consumers to submit more personal information than necessary to process their privacy requests.
- Requiring consumers to verify their identity before they could opt-out of the sale/sharing of their personal information.

The CPPA found that Todd Snyder lacked adequate oversight of the third-party cookie tools on its website. For 40 days in late 2023, the site's opt-out mechanisms were not properly configured to process consumer requests to opt-out of the sale or sharing of their personal information. Specifically, when consumers clicked a link to manage their preferences, a cookie consent banner appeared but then disappeared instantaneously or failed to work properly, resulting in consumers being unable to exercise their right to opt out. The site also ignored opt-out preference signals, such as GPC.

The CPPA also highlighted failures with Todd Snyder's data privacy request procedures. Todd Snyder directed consumers to submit a "Data Request Form" for all data privacy requests, requiring consumers to provide their name, country of residence, and a photograph of the consumer holding their "identity document." This information was requested regardless of the request type, including for requests to opt out of sale/sharing. This violated the CCPA in two ways: (i) applying a verification standard to opt-out of sale/sharing requests (which do not require verification under the statute) and (ii) requiring more personal information than necessary – including sensitive information, like a driver's license, state identification card, or passport number – to verify a consumer's identity.

[4] https://cppa.ca.gov/pdf/20250501_snyder_order.pdf.

Under the order, Todd Snyder must implement and maintain specific methods for submitting requests to opt out of sale/sharing – including refraining from requiring consumers making a request to opt out of sale/sharing to provide more information than necessary to process the request, ensuring that the company's methods for submitting requests to opt-out of sale/sharing comply with the CCPA – and ensuring that it honors opt-out preference signals for known consumers.

Jerico Pictures, Inc.

In February 2025, the CPPA brought an enforcement action[5] against Jerico Pictures, Inc., d/b/a National Public Data, a Florida-based data broker. The CPPA alleged that the company failed to register and pay an annual fee as required under the Delete Act. Instead, the company registered 230 days late, and only after being contacted by the CPPA's Enforcement Division. The CPPA sought a $46,000 fine against the company for its violations. This enforcement action comes after the CPPA previously filed a claim against the company in October 2024 in the U.S. Bankruptcy Court for the Southern District of Florida alleging that the company owed the agency an administrative fine related to its failure to register as a data broker in California.

Since October 2024, the CPPA has also taken action against five additional data brokers, resulting in settlements.

KEY TAKEAWAYS

- *Proactive Compliance is Crucial*: Staying ahead of regulatory requirements is essential to avoid costly fines and reputational damage.
- *User Interface Design Should Support Consumer Choice*: The use of dark patterns – designs that mislead or manipulate users – can trigger enforcement actions. User interfaces should clearly and easily enable consumers to exercise their privacy rights.
- *Don't Outsource Compliance*: Businesses should regularly monitor and validate their third-party privacy management tools to ensure they are working as expected. A business cannot simply defer to their third-party tools without understanding their limitations or validating their operation.
- *Data Minimization is a Core Expectation*: Businesses should collect only the minimum personal information necessary to fulfill a specific purpose, particularly when processing consumer data privacy requests.
- *Timely Data Broker Registration is Mandatory*: Data brokers must comply with registration deadlines under the Delete Act to avoid daily penalties and enforcement scrutiny.

[5] https://cppa.ca.gov/announcements/2025/20250220.html.

The CPPA's recent enforcement actions underscore its ongoing commitment enforcing California's data privacy laws. Businesses should regularly evaluate and update their compliance strategies, focusing on user-centric design, data minimization, and transparent data practices to align with evolving regulatory expectations.