AN A.S. PRATT PUBLICATION
JANUARY 2026
VOL. 12 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 1** **January 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.

Website Tracking Lawsuit Against Retailer Dismissed for Lack of Standing: What California Ruling Means for Your Business

By Catherine M. Contino, Usama Kahf and Xuan Zhou*

The authors of this article discuss a recent California federal court decision, which represents another data privacy win for businesses defending against the surge of lawsuits filed under the California Invasion of Privacy Act (CIPA) based on routine marketing and analytics tools.

A California federal court recently handed businesses another major victory in the ongoing wave of privacy lawsuits targeting website analytics and tracking tools. Judge Fernando Aenlle-Rocha of the Central District of California dismissed a proposed class action against a national retailer for lack of Article III standing. The court found that the plaintiff failed to allege any specific, concrete harm stemming from the company's use of standard website data collection software – a decision that adds to a growing body of rulings limiting these suits.

The *Price v. Converse, Inc.*, case represents another data privacy win for businesses defending against the surge of lawsuits filed under the California Invasion of Privacy Act (CIPA) based on routine marketing and analytics tools – a trend led by a small number of plaintiff firms bringing near-identical complaints across industries.

THE CASE

This is not the first time Converse has successfully defended against such claims. Earlier in 2025, the U.S. Court of Appeals for the Ninth Circuit affirmed the company's victory in a similar CIPA website chat "wiretap" case, rejecting attempts to stretch the law beyond traditional surveillance contexts.

In the most recent case, a plaintiff claimed that Converse violated the California Trap and Trace Law (part of CIPA) by sharing data with a social media company's pixel through a software development kit. Plaintiff alleged that this "SDK" collects data that may be used as an electronic fingerprint to assist the social media company in profiling the user based on their activity on Converse's website. The plaintiff argued this "tracking tool" acted as an illegal "trap and trace device" by collecting browser, device, and location data to identify users without prior opt-in consent.

---

* Catherine M. Contino, Usama Kahf, CIPP/US, and Xuan Zhou, CIPP/US, CIPM, CIPP/E, attorneys at Fisher & Phillips LLP, may be reached at ccontino@fisherphillips.com, ukahf@fisherphillips.com and xzhou@fisherphillips.com, respectively.

WEAPONIZING DATA PRIVACY CLAIMS

This also is not the first time that the plaintiff's law firm has filed such a lawsuit. In fact, the Los Angeles-based plaintiffs' firm has filed over 550 such CIPA website pixel claims – the second-most prolific law firm in the country. It has likely sent thousands of demand letters that never resulted in litigation but have led companies to collectively pay out millions of dollars in settlements.

Given the dollars at stake, it is not surprising that many of these litigation factories are springing up to take advantage of these novel legal theories, with more plaintiffs' firms jumping on the bandwagon. They often file cookie-cutter complaints repeating the same allegations in the hopes of leveraging a quick settlement.

THE COURT'S DECISION

In this most recent case, Converse scored a win and the court dismissed the case for lack of standing. The judge found that:

- The plaintiff failed to allege a concrete, particularized injury as required by Article III of the U.S. Constitution.
- Merely claiming a statutory violation of CIPA is not enough. There must be a harm closely related to traditional privacy torts like intrusion upon seclusion or disclosure of private facts.
- The alleged data collection through "device fingerprinting," while potentially undesirable, did not constitute the kind of "highly offensive" invasion of privacy recognized by courts.

The court found that plaintiff's allegations were insufficient to show any "concrete injury" comparable to traditional privacy harms. As Judge Aenlle-Rocha explained, the plaintiff failed to allege that the tracking software "caused her to experience any harm remotely similar to the highly offensive interferences or disclosures actionable at common law."

In reaching its conclusion, the court relied heavily on the Ninth Circuit's recent decision in *Popa v. Microsoft*, emphasizing that an "injury in law is not an injury in fact."

5 KEY TAKEAWAYS FOR BUSINESSES

This case underscores a growing judicial recognition that many CIPA "pixel" lawsuits are overreaching – targeting ordinary marketing activity rather than genuine invasions of privacy. Here are some key lessons your business can apply to your data practices given this victory.

1. STANDING REMAINS A HIGH BAR FOR WEB TRACKING CLAIMS

Courts are increasingly dismissing suits that allege technical privacy violations without real-world harm. Businesses that use tracking tools, analytics pixels, or similar code may face lawsuits, but plaintiffs need to show more than mere data collection and sharing in order to advance the ball.

2. AUDIT YOUR WEBSITE TOOLS, BUT KEEP PERSPECTIVE

Even though standing defenses can be successful, prevention is still the best defense:

- Audit your site for tracking tools and third-party integrations.
- Regularly monitor cookie consent process. You should regularly have an independent third party (whether a law firm or other vendor) test your website cookie consent mechanism to verify that the opt-in and opt-out choices continue to function as intended.
- Disclose data collection practices clearly in your privacy policy.
- Obtain user consent where required, particularly for behavioral tracking. Consider obtaining opt-in consent prior to firing up third-party cookies on your website. Even though no California law currently requires such prior opt-in consent for website cookies, plaintiffs in CIPA litigation are claiming that it is a violation of CIPA to allow cookies to share date with third parties in real time without first obtaining opt-in consent. There is no controlling authority yet on whether plaintiff's theory of liability is correct, but the best way to avoid this litigation altogether is to do what plaintiffs' attorneys are saying you should be doing. Again, we are not saying they are right; rather, we are saying you do not need to be a target.

3. STAY AHEAD OF STATE PRIVACY LAWS

CIPA-based suits are on the rise in California, and similar litigation is spreading across 29 other states under similar wiretapping laws (for example, in Illinois, New York, Colorado, Texas, and even Florida). Businesses and retailers should ensure compliance with all applicable state privacy and wiretapping laws.

4. KEEP COMPLIANCE DOCUMENTATION READY

Maintain records of:

- User consent mechanisms;
- Vendor contracts governing data sharing; and
- Regular audits of cookies, analytics, and embedded code.

5. EXPECT ONGOING DIVERGENCE BETWEEN COURTS

While this decision limits certain consumer claims in federal court, plaintiffs may refile in state court under broader standing doctrines or pursue other privacy statutes. Federal courts are split on whether website analytics data – like IP addresses or device identifiers – are private enough to support a claim. While this case falls on the business-friendly side, others have reached the opposite conclusion, so proactive compliance remains essential.