wiley

ALERT

Key Areas to Watch as Website Technology Litigation Continues to Surge

March 3, 2026

Companies are facing a growing trend of plaintiffs asserting claims that businesses' common website technologies – including the use of cookies for website optimization, analytics, and marketing – violate pre-internet state wiretap laws, such as the California Invasion of Privacy Act (CIPA). Online businesses across all sectors have received demand letters and have been sued in individual and class actions under a number of novel theories.

In light of this, companies should review their use of website technologies to address potential risks under these laws and understand how to best deal with such claims in settlement negotiations, litigation, and/or arbitration.

Below we outline some recent trends and strategies for dealing with threatened and actual litigation.

Website Technology Litigation Is Skyrocketing

In 2025 alone, federal courts dealt with nearly 3,000 open data privacy dockets.[1] Website technology litigation has become a key component of this privacy litigation.

Plaintiffs are advancing novel theories as to how common website technologies – like third-party analytics involving user information such as locations or identifying and/or behavioral metadata, social media pixels, web beacons, and chat features – violate laws like CIPA.[2] Enacted in the late 1960s, CIPA prohibits wiretapping and eavesdropping via telephone, although some courts have applied the statute to modern technologies, including routine online business practices. While CIPA Section 638.51 prohibits installing or using "a

Authors

Attison L. Barnes, III
Partner
202.719.7385
abarnes@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

David E. Weslow
Partner
202.719.7525
dweslow@wiley.law

Stephanie Rigizadeh
Associate
202.719.4736
srigizadeh@wiley.law

Practice Areas

Emerging Technologies
Litigation
Privacy, Cyber & Data Governance
State Privacy Laws
Trump Administration Resource Center

pen register or a trap and trace device without first obtaining a court order,"[3] recently, plaintiffs and plaintiffs' firms have used CIPA Section 638.51 to sue companies across all sectors over their use of various website technologies.

Beyond California, there is risk under other state wiretapping laws as well, including the Florida Security of Communications Act (FSCA). In a March 2025 case, a court denied in part a health care organization's motion to dismiss in a lawsuit brought by a plaintiff claiming the defendant used tracking technologies to intercept patient communications for advertising purposes, in violation of the FSCA.[4] The court determined that the plaintiff sufficiently alleged that the defendant intercepted the contents of her electronic communications.[5]

What Companies Can Do to Mitigate Risk

Companies can proactively take steps to mitigate these risks around use of website technologies.[6]

Before receiving a demand letter, companies can:

- Review their website data collection practices to assess compliance obligations.
- Update their privacy policies, cookie banners, and cookie consent management features to ensure compliance with privacy laws.
- Audit their cookie banner and consent management features regularly.

After receiving a demand letter, companies should also assess potential factual and legal defenses. These defenses could include:

- Lack of standing based on failing to suffer an actual injury.
- Claims that conflict with applicable regulatory frameworks and are therefore unsupportable.
- Consent to use of online technologies.

Additionally, companies should assess any forum selection clauses in privacy or membership agreements to determine where litigation may be brought. In one recent case involving a global hospitality company that is contesting a plaintiff's claims, the Northern District of California granted a motion to transfer the case to the Eastern District of Virginia, based on a forum selection clause in an agreement that the plaintiffs made by choosing to become members of a rewards program.[7]

***

Wiley's Privacy, Cyber & Data Governance practice has a deep bench of attorneys guiding companies through a broad range of risk management and policy compliance under state and federal privacy frameworks, and develops legal strategies to help companies navigate litigation risks. Wiley's Litigation practice, bolstered by strong capabilities in cases involving website technologies and deep substantive data privacy experience, helps companies succeed in complex, high-stakes litigation, including class action lawsuits. For more information, please contact one of the authors of this alert.

[1] Westlaw Litigation Analytics: Data Privacy Analytics (last visited Feb. 11, 2026).

[2] Cal. Penal Code §§ 630-638.

[3] *Id.* § 638.51

[4] *W.W. v. Orlando Health, Inc.*, No. 6:24-cv-1068-JSS-RMN (M.D. Fla. March 6, 2025).

[5] *Id.* at 11-12.

[6] This document is intended to provide general information about legal developments and should not be construed as providing legal advice or legal opinions. You should consult an attorney for any specific legal questions.

[7] Order Granting Mot. to Transfer, *Shah v. Hilton Worldwide Holdings*, No. 25-cv-01018-EKL, at 1, 2-4 (N.D. Cal. Jan. 7, 2026).