wiley

NEWSLETTER

# Mitigating Risk as Website Technology Litigation Surges

June 2026

Companies are facing a growing trend of claims that businesses' website technologies – including cookies for website optimization, analytics, and marketing – violate pre-internet state wiretap laws, such as the California Invasion of Privacy Act (CIPA), Cal. Penal Code §§ 630-638. This is an increasing risk area for government contractors – regardless of size or sector – that have an online presence and that use these technologies. Cases against contractors seem to be increasing along with the prominence of their presence in the news cycle. Another factor may be consolidation in the industry – a contractor may find itself subject to CIPA suits arising from acquiring another contractor that may not have implemented as robust data collection prevention.

In light of this, government contractors should review their use of website technologies to identify and address potential risks under these laws and understand how to best deal with any demand letters or lawsuits arising from this trend.

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 thousands of open data privacy cases, per Westlaw Litigation Analytics: Data Privacy Analytics (last visited Feb. 11, 2026). Website technology litigation has become a key component of this privacy litigation.

## Authors


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

Scott A. Felder
Partner
202.719.7029
sfelder@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@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

Government Contracts
Litigation
Privacy, Cyber & Data Governance
State Privacy Laws

Plaintiffs are advancing novel theories as to how 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. 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 pen register or a trap and trace device without first obtaining a court order," recently, plaintiffs and plaintiffs' law firms have used CIPA Section 638.51 to sue companies across all sectors over their use of various website technologies. These plaintiffs are using California laws to pursue claims against companies outside of California merely because the defendants' websites are accessible in the state.

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. *See W.W. v. Orlando Health, Inc.*, No. 6:24-cv-1068-JSS-RMN (M.D. Fla. March 6, 2025). The court determined that the plaintiff sufficiently alleged that the defendant intercepted the contents of her electronic communications.

***What Government Contractors Can Do to Mitigate Risk***

Government contractors can proactively take steps to mitigate these risks around use of website technologies.

Before receiving a demand letter, government contractors can:

- Review website data collection practices to assess compliance obligations, including all digital properties in their review, such as legacy websites or websites of any subsidiaries as well as newly acquired entities.
- Update privacy policies, cookie banners, and cookie consent management features to ensure compliance with privacy laws.
- Audit cookie banner and consent management features regularly.

After receiving a demand letter or a lawsuit, government contractors 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; and
- Assessing forum selection clauses in applicable agreements to determine where litigation may be brought.

Ideally, to avoid added expense and risk, government contractors should not wait until they receive a demand letter or lawsuit to assess their website data collection practices, cookie banners, and consent management features.