



Privacy & Cybersecurity Update

April 2026

Website Cookie Management Tools and Privacy and ECPA/Wiretapping Claims

A cookie management tool (CMT), also known as a consent management platform, is a type of software solution designed to enable website end users to control how a website deploys nonessential cookies and pixels (e.g., targeted advertising and social media pixels). Organizations commonly implement CMTs to comply with legal requirements or as a best practice.

But what happens when a website CMT is not functioning properly? Organizations need to be aware that consumer protection attorneys are scanning publicly available websites, including those used solely in the business-to-business context, and that there has been a significant increase in legal claims based on improperly configured CMTs.

CMT Legal Requirements

There are over 20 state consumer privacy laws that regulate how covered organizations can deploy third-party cookies and pixels for targeted advertising purposes. For example, many of these laws require an organization to provide website users with the ability to opt out from having their personal data (e.g., IP addresses) used for targeted advertising purposes. In some circumstances, state consumer privacy laws require a covered business to obtain affirmative consent before using cookies and pixels to collect sensitive personal data (e.g., geolocation data) or personal data on a minor or child.

In addition, state surveillance laws, such as the California Invasion of Privacy Act (CIPA), may impose stricter requirements on the use of third-party cookies, pixels, beacons and tags, although there is conflicting case law on

the issue. (See our website for more details on [CIPA and related legal claims](#).)

It is common for an organization to deploy a CMT to comply with its legal requirements. A CMT should, at a minimum, be able to:

- Scan websites for cookies and create a cookie declaration table
- Assist in the development of privacy and cookie notices that describe to end users how a website collects and processes personal information and other data
- Maintain a record of when a website end user consents to or declines the use of nonessential cookies
- Provide a website end user the ability to change their cookie/pixel preferences at any time

However, implementing and maintaining a properly functioning CMT can be difficult, especially when there are multiple essential and nonessential cookies within a website.

When a CMT is not properly configured, an organization may be in violation of data privacy laws and exposing itself to litigation under Title III of the Electronic Communications Privacy Act, as amended (ECPA).

Website ECPA/Wiretapping Claims

ECPA provides for liability against any person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.”

It is generally considered a one-party consent law (i.e., only one party, such as the website owner, needs to consent to

the interception of a communication transmitted over the website). However, the one-party exception does not apply if the “communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” This is commonly known as ECPA’s “crime-tort” exception, and it essentially revokes a defendant’s ability to rely on the law’s one-party consent framework.

Accordingly, consumer privacy plaintiffs’ attorneys are scanning publicly available websites, including those used in the business-to-business context, to determine whether websites’ CMTs align with the privacy disclosures and commitments made to website end users. For example, privacy policies often include verbiage informing end users that they have the right to consent to or opt-out of the use of nonessential cookies, and they direct these end users to the CMT to exercise this right.

Attorneys who identify that certain nonessential cookies are being deployed due to a malfunctioning CMT and in violation of the commitments set forth in a privacy policy are claiming that a communication has been unlawfully intercepted and ECPA’s crime-tort exception nullifies the consent-based defenses that would otherwise be available to the website owner. *See Smith v. Rack Room Shoes, Inc.*, No. 24-cv-06709-RFL, (N.D. Cal. Jan. 23, 2026); *Riganian v. LiveRamp Holdings, Inc.*, 791 F. Supp. 3d 1075 (N.D. Cal. 2025); and *B.N. v. Oregon Reproductive Medicine, LLC*, No. 3:25-cv-00202-IM (D. Or. Nov. 12, 2025). And these consumer privacy lawyers are prepared to file lawsuits and arbitration demands seeking damages, including punitive damages, and attorneys’ fees, although they seem to often prefer quick out-of-court settlements.

Conclusion

Organizations often use CMTs to comply with various legal requirements governing the use of certain nonessential cookies and pixels, such as those used for marketing and online behavioral advertising purposes. However, implementing and maintaining a properly functioning CMT can be complex and time-consuming, especially for organizations deploying dozens of cookies and pixels. And consumer privacy attorneys are frequently scanning

websites for improperly functioning CMTs to generate legal complaints and demand letters targeting unsuspecting businesses. To help avoid these claims, an organization should routinely assess its CMT configuration for compliance and consider retaining a third-party expert to help optimize CMT functionality.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Kim Sim Sandell

310.382.1309

Kim.Sandell@ThompsonHine.com

Jenna Schneider

513.352.6633

Jenna.Schneider@ThompsonHine.com

Certified Information Privacy Professional/United States (CIPP/US)

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2026 THOMPSON HINE LLP. ALL RIGHTS RESERVED.