Insights, News & Events

MULTI-COURT SPLIT ON WEBSITE TRACKING FEDERAL WIRETAPPING CLAIMS CREATES COMPLIANCE CONFUSION: 6 STRATEGIES TO AVOID RISK

Insights
Apr 7, 2026

Multi-Court Split on Website Tracking Federal Wiretapping Claims Creates Compliance Confusion: 6 Strategies to Avoid Risk

A significant and rapidly developing split has emerged among federal district courts regarding whether claims under the Electronic Communications Privacy Act (ECPA) can advance based on the use of common website tracking technologies such as cookies, pixels, and analytics tools. Plaintiffs usually allege that these tools collect personal information about users' activity on a website and may share that data with third parties. The lawsuits further contend that this kind of data sharing happens without proper opt-in consent and falls within what's known as the "crime-tort exception," and thereby constitutes unlawful "interceptions" under the ECPA. District courts across the country have issued differing decisions on whether these claims can proceed, reflecting fundamentally different interpretations of the statute. The law is still evolving, and businesses may face increasing exposure to potential lawsuits as courts continue to grapple with these issues. This Insight will cover everything you need to know about these recent decisions and how they could impact your business.

Overview of the Applicable Law

The ECPA prohibits the intentional interception of electronic communications and provides a private right of action for violations. To bring a claim, a plaintiff must allege that:

Related People

Usama Kahf, CIPP/US
Partner

949.798.2118

Chelsea Viola
Associate

213.403.9626

- The defendant intentionally intercepted a communication;
- What was intercepted was the actual content of the communication; and
- The interception must have been done using some kind of tool or technology.

The statute has a "one-party consent rule," which means that an interception may be permitted if at least one party to the communication has given prior consent.

However, that protection is **not absolute.** The provision includes an important carve-out: the crime-tort exception, which eliminates that protection where a communication is "intercepted for the purpose of committing any criminal or tortious act" in violation of any law. Courts are divided on how to interpret this exception – specifically, whether the interception requires a criminal or tortious purpose, or whether it is enough that the interception merely results in some form of criminal or tortious act. The latter is a critical distinction because it would mean that plaintiffs can invoke the crime-tort exception and allege an ECPA claim as long as they can separately allege sufficient facts to state a tort claim (such as invasion of privacy) based on the same conduct. With such interpretation, it wouldn't matter at the pleading stage that the website technology was not installed for a criminal or tortious purpose.

Expanding ECPA Exposure

Courts are divided on how to interpret the crime-tort exception under the ECPA, resulting in inconsistent outcomes and increasing uncertainty. And a growing number of courts have adopted a more plaintiff-friendly approach, a posture that exposes businesses to more potential liability and nationwide class actions. Recent cases have allowed ECPA claims to survive motions to dismiss based on allegations of unlawful data collection and disclosure.

Why it matters: These decisions significantly lower the pleading burden for plaintiffs and broaden potential exposure for businesses using standard website tracking technologies. It effectively allows ECPA claims to proceed even where the alleged data-sharing was for routine purposes such as marketing or analytics.

Xuan Zhou, CIPP/US, CIPM, CIPP/E

Associate

858.597.9632

Service Focus

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Here's a rundown of what the courts have said when upholding these types of ECPA claims:

***1. Stein v. Edward-Elmhurst Health* (N.D. Ill. Mar. 3, 2026)**

Plaintiffs don't have to argue that the defendant acted with unlawful intent to bring a successful ECPA claim under the crime-tort exception. Allegations that data sharing itself violates laws such as HIPAA may be enough to invoke the exception.

- The court determined that the ECPA focuses on a criminal or tortious **act**, not a criminal or tortious **purpose**.
- The Northern District of Illinois also explicitly acknowledged that courts are **"all over the map"** on this issue and certified the question for interlocutory appeal, signaling that appeals courts may step in and provide some guidance on the question.

***2. Semien v. PubMatic Inc*. (N.D. Cal. Jan. 27, 2026)**

Adequately alleged invasion of privacy claims, particularly involving data profiling, could establish a "tortious purpose" under the crime-tort exception.

- The Northern District of California rejected PubMatic's arguments that the ECPA claim should be dismissed because the website owners consented to the installation of the PubMatic pixel, and data collection was **motivated by profit and routine commercial activity**, not by any intent to injure plaintiffs.
- But, the court held that establishing a consent or a profit motive won't defeat the claim if the crime-tort exception applies. The court explained that seeking financial gain and committing a tort are not mutually exclusive; profit can be the reason for the tortious conduct.

***3. Krzyzek v. OpenX Techs., Inc*. (N.D. Cal. Jan. 27, 2026)**

Plaintiffs' invasion-of-privacy allegations were enough to invoke the crime-tort exception.

- The Northern District of California rejected arguments that website operator consent barred the claim and that a profit motive automatically defeats the crime-tort exception.

- The court explained that the exception could be triggered by alleging an individual's website interactions are tracked and used to create a "profile" of that user.

4. *Garcia v. Truist Financial Corp.* (C.D. Cal. March 25, 2026)

The key issue is the purpose of the interception, not whether the interception itself was unlawful.

- The Central District of California said that the criminal or tortious purpose used to invoke the exception must be **independent** of the act of interception and **exist at the time it occurs**.
- The court held that plaintiff plausibly alleged that the defendant intentionally embedded a third-party tracking tool on its website to monitor users and share their data, and defendant used that tool to collect and disclose sensitive consumer information, constituting an invasion of privacy.

A handful of other decisions in Illinois, Minnesota, and California district courts similarly allowed claims to proceed where plaintiffs alleged that intercepted data was disclosed to third parties in violation of HIPAA or other privacy laws. These courts often treated disclosure to third parties **as an independent unlawful act** that triggers the crime-tort exception.

Narrowing the ECPA Path for Plaintiffs

Other courts have taken a more restrictive approach, emphasizing the limits of the statute and the need for concrete factual allegations. This line of cases reflects a broader trend of courts narrowing plaintiffs' path by requiring concrete allegations of unlawful purpose and rejecting claims based solely on routine data collection or profit-driven conduct.

Why it matters: This approach raises the bar for plaintiffs and provides defendants with a viable path to early dismissal, particularly where complaints rely on generalized allegations about tracking technologies without specific facts showing unlawful conduct.

Here's a rundown of what the courts have said when tossing out ECPA claims:

***1. Nichols v. PeaceHealth* (W.D. Wash. Mar. 4, 2026)**

The crime-tort exception requires well-pleaded facts showing a separate criminal or tortious purpose, not merely conclusory allegations.

- A website operator is generally a party to the communication, triggering the one-party consent rule.
- Allegations that data was used for targeted advertising purposes were insufficient to establish unlawful intent.
- The court held that plaintiffs must allege (1) a distinct unlawful objective beyond the act of data collection itself, and (2) concrete facts showing misuse of protected information, not just disclosure. Since the complaint lacked these allegations, the court dismissed the claim.

***2. Lakes v. Ubisoft, Inc*. (N.D. Cal. April 2, 2025)**

The use of pixels and cookies to share user data with third parties wasn't unlawful interception under the ECPA, because the company sought consent and didn't intercept the data for a criminal or tortious purpose.

- **Consent**: Ubisoft's privacy policy adequately disclosed the use of cookies and third-party data sharing. The court rejected plaintiffs' argument that more specific disclosures were required, concluding that a reasonable user would understand the disclosed practices to cover the alleged conduct.
- **Crime-tort exception**: Plaintiffs failed to plausibly allege that the interception was undertaken for a criminal or tortious purpose, thus triggering the exception and violating the ECPA. Allegations that the tracking tools were used to improve advertising and generate revenue were insufficient; profit-seeking alone does not satisfy the exception.

***3. Zocco v. Nelnet, Inc.* (N.D. Cal. Jan. 29, 2026)**

The defendant, as the website operator, was determined to be a party to the allegedly intercepted communications, because plaintiffs knowingly interacted with its online platform. As a result, the one-party consent rule applied.

- To trigger the exception, plaintiffs must show that committing a crime or tort was a primary or determining purpose of the interception, not merely that the conduct could be unlawful.
- Allegations that defendant used tracking technologies for financial gain by itself were insufficient to meet this standard.

Similarly, federal district courts in Illinois, Massachusetts, Texas, and California have dismissed claims where plaintiffs failed to show that data collection was undertaken with the specific purpose of committing a crime or tort, rather than for routine commercial objectives.

What This Means For Your Business: Expanding Risk and Uncertainty

Taken together, these decisions signal increasing and uneven litigation risk for businesses that reply on common website tracking technologies, including:

- **Broader exposure to federal claims.** Plaintiffs are no longer relying solely on state laws (such as CIPA) and are instead bringing nationwide class actions under the ECPA.
- **Inconsistent risks across states and districts.** Plaintiffs' firms that have historically focused on California wiretapping statutes are now leveraging ECPA to pursue broader, multi-jurisdictional claims. The same tracking practices may be dismissed by one court and allowed to proceed by another, increasing the likelihood of litigation and the cost of defending these claims.
- **Challenges to routine data practices.** Even standard uses of cookies, pixels, and analytics tools may be scrutinized, particularly where plaintiffs allege data sharing with third parties.
- **Heightened risk from third-party vendors.** Cases involving registered data brokers rather than the website operators themselves (like *Semien v. PubMatic* and *Krzyzek v. OpenX*) suggest that not only website owners, but also third-party ad tech and analytics providers, may face direct liability.
- **Uncertainty around consent and purpose.** Courts are split on whether user consent and routine, profit-driven

data use are sufficient defenses, making outcomes difficult to predict at the motion to dismiss stage.

6 Strategies Employers and Website Operators Can Use Now

Given the evolving and uncertain legal landscape, businesses should take proactive steps to mitigate potential exposure under the ECPA. Consider these best practices:

1. Map Your Data Flow. Inventory all data collected across websites, applications, and embedded tools. Map how data is transmitted (e.g., URLs, headers, form fields, event tracking) and where it is sent, including third parties. Classify data by sensitivity, especially health, financial, or other protected information.

2. Evaluate Your Tracking Technologies and Configuration. Audit analytics tools, pixels, SDKs, and session replay technologies to determine what data is captured and transmitted. Assess whether configurations (e.g., URL parameter capture, IP logging, user identifiers) result in disclosure of sensitive or user-identifiable information. Implement technical controls such as data minimization, redaction, filtering, or disabling certain tracking features where appropriate.

3. Strengthen Your Disclosures and Consent Mechanisms. Ensure privacy notices accurately and comprehensively describe data collection, use, and sharing practices, including tracking technologies. Deploy and calibrate cookie consent and preference management tools to obtain legally sufficient consent where required. Consider jurisdiction-specific requirements (e.g., opt-in vs. opt-out regimes).

4. Review Your Vendor Agreements. Audit agreements with analytics providers, ad tech vendors, data brokers, and other third parties to confirm restrictions on data use, retention, and onward disclosure. Evaluate whether vendors qualify as "service providers," "processors," or independent third parties under applicable laws. Incorporate contractual safeguards into your vendor agreements, including data processing addenda, audit rights, and clear limitations on use for secondary purposes.

5. Limit Sensitive Data Exposure. Scrutinize whether any tracked data could be construed as health or other

protected information. Implement safeguards to prevent transmission of such data to third parties.

6. Prepare For Potential Changes: Work with legal counsel to keep tabs on ongoing court decisions and appellate activity, particularly the anticipated 7th Circuit review in *Stein*. Be prepared to adjust practices as courts continue to refine the scope of ECPA liability.

Conclusion

To stay informed, subscribe to Fisher Phillips' Insights System for timely updates on ECPA and other privacy-related trends. For personalized guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Digital Wiretapping Litigation Team. You can also explore additional resources on our U.S. Privacy Hub at any time.