Shumaker

MAY 11, 2026 | PUBLICATION

How the Federal Wiretap Act Became a Weapon Against Privacy Policy Missteps — And What Companies Should Do About It

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The Stakes at a Glance

A landmark federal court ruling in August 2025 established a new pathway for class action plaintiffs to leverage alleged misstatements and inaccuracies in corporate privacy policies as the foundation for federal wiretapping claims under the Electronic Communications Privacy Act (ECPA), also known as the Wiretap Act. This development marks a significant escalation in the tracking technology litigation wave. Unlike state-law wiretapping claims brought under statutes such as the California Invasion of Privacy Act (CIPA), ECPA claims can be asserted in any federal court nationwide. The statute provides for statutory damages of the greater of $100 per day of violation or $10,000, creating enormous potential aggregate exposure in class action proceedings. Plaintiffs' firms are increasingly relying on ECPA theories in both pre-suit demand letters and class action complaints, and the pace of filings is accelerating rapidly.

Any company that maintains a website, publishes a privacy policy, and deploys commonly used tracking technologies, such as pixels, cookies, software development kits, or third-party analytics tools, should understand this risk.

The Backdrop: How State-Law Tracking Technology Claims Set the Stage

The Surge in CIPA Litigation

The rise of ECPA-based privacy policy claims did not happen in a vacuum. Beginning around 2022 and accelerating through 2025, plaintiffs' attorneys filed thousands of lawsuits under state all-party consent wiretapping statutes, with the vast majority brought under CIPA in California state and federal courts.

The core theory in these cases is straightforward: when a website deploys a third-party tracking pixel or similar technology—such as the Meta Pixel, TikTok Pixel, or Google Analytics tag—the tool allegedly intercepts the "contents" of a website visitor's communications while in transit. Because California is an all-party consent jurisdiction, plaintiffs argued this interception violated CIPA unless every party to the communication, including the website visitor, consented.

Over time, plaintiffs expanded their theories to target CIPA's pen register and trap-and-trace device provisions under Section 638.51. Under this theory, the collection and transmission of website-related metadata to third parties via tracking technologies is functionally equivalent to operating a pen register capturing dialing, routing, addressing, and signaling information. Courts have largely accepted that website-based trackers can plausibly constitute pen registers under the statute's broad language, especially where they capture information such as IP addresses, HTTP request headers, and granular browsing behavior data.

The potential exposure under CIPA is significant, with statutory damages of $5,000 per violation multiplied across a class of website visitors. Many of these cases have progressed past motions to dismiss, and one high-profile case—*Frasco v. Flo Health*—went to a jury trial in 2025 in which Meta was found to have violated CIPA Section 632 by intentionally eavesdropping on plaintiffs' confidential communications without consent. The ongoing litigation pressure led many companies to settle pre-suit demand letters at nuisance value, funding further filings from the plaintiffs' bar.

Defense Victories and Shifting Strategies

The litigation landscape was not entirely one-sided. Defendants secured meaningful victories on several fronts. In the Ninth Circuit, courts held that a party to a communication cannot eavesdrop on itself, creating a significant obstacle for certain plaintiffs' theories. Some courts also ruled that CIPA Section 631(a)'s first clause applies only to "telephone wire, line, cable, or instruments" and not to internet-based communications. Federal courts in California dismissed CIPA claims on Article III standing grounds, finding that plaintiffs failed to demonstrate concrete, particularized harm from routine data collection. The Third Circuit held that a third-party tracking company was not a third-party eavesdropper where it received information directly from users' browsers rather than through an interception.

On the legislative front, California lawmakers introduced Senate Bill 690, proposing to clarify that tracking technologies used for "commercial business purposes" fall outside CIPA's scope. That bill stalled in 2025, however, and was placed on a two-year track, leaving the business community without near-term legislative relief.

These defense-side developments, while significant, did not extinguish tracking technology litigation. Instead, they appeared to encourage plaintiffs' counsel to search for alternative legal frameworks, leading

them to the ECPA and its crime-tort exception.

The ECPA's Crime-Tort Exception: A Nationwide Theory of Liability

The One-Party Consent Statute and Its Critical Carveout

The ECPA, enacted in 1986, prohibits the intentional interception, disclosure, or use of electronic communications. Unlike CIPA and other all-party consent state statutes, the ECPA is a one-party consent law. Under this framework, a website operator that is a party to the communication and that consents to the tracking tools it has installed on its own website would appear to have a complete defense.

However, two additional features of the statute warrant attention. First, the ECPA contains an ordinary business use exception, sometimes referred to as the "provider exception," under 18 U.S.C. § 2511(2)(a)(i). This provision permits an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service whose facilities are used in the transmission of a communication, to intercept, disclose, or use that communication "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." In theory, this exception could shield website operators who argue that their use of tracking technologies is a routine, necessary component of delivering their online services, such as maintaining website functionality, performing analytics to improve performance, or protecting against fraud. In practice, however, courts have not broadly extended this exception to commercial tracking technology deployments aimed at advertising and behavioral targeting, and plaintiffs routinely argue that data collection for advertising purposes exceeds the scope of what is "necessary" to the rendition of service.

Second, there is a critical carveout to the one-party consent defense itself. Under 18 U.S.C. § 2511(2)(d), the one-party consent defense does not apply where 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 the so-called "crime-tort exception," and it has become the linchpin of a new wave of class action litigation.

To invoke the crime-tort exception, a plaintiff must establish two things: (1) that a third-party tracking tool intercepted electronic communications, which is often uncontested at the pleading stage; and (2) that the interception was carried out "for the purpose of" committing some independent crime or tort beyond the act of interception itself. Courts have held that the exception contains both a temporal requirement—the interceptor must have the independent criminal or tortious purpose at the time of the interception—and a separateness requirement—the crime or tort must be "beyond the act of intercepting itself."

A Brief Comparison: ECPA vs. CIPA Exception Frameworks

The structure of available defenses under the ECPA differs from those under CIPA in important ways. CIPA is an all-party consent statute, meaning that the consent of every party to a communication is required. Under CIPA Section 631(b), the statute carves out an exception for the use of equipment "furnished and used pursuant to the tariffs" of a public utility engaged in providing communication services, a narrow provision rooted in the traditional telephonic context. For pen register claims under CIPA Section 638.51, the statute provides a separate set of exceptions permitting providers of electronic or wire communication services to use pen registers to operate, maintain, and test their services; to protect the rights or property of the provider; to protect users from abuse of service; or where user consent has been obtained.

By contrast, the ECPA's ordinary business use exception and its one-party consent defense are structurally broader, but the crime-tort exception claws back much of that breathing room. Under CIPA, the core defense

question is typically whether the website visitor consented to the interception. Under the ECPA, the question shifts to whether the interception was carried out for the purpose of committing an independent crime or tort, a question that, as described below, plaintiffs have learned to answer by pointing to a company's own privacy disclosures. Courts analyzing both statutes have noted that they "perform the same analysis" with respect to the party exemption. But the practical litigation dynamic under the ECPA is distinct: the ordinary business use exception has not proven to be a reliable shield where the challenged tracking serves advertising or commercial profiling purposes rather than core service delivery.

Early Applications: Health Care and Health Insurance Portability and Accountability Act (HIPAA)

For several years, the crime-tort exception was most frequently invoked in the health care context. Plaintiffs alleged that hospitals and health systems deploying tracking pixels on their websites transferred protected health information (PHI) to third parties in violation of HIPAA. These claims focused on scenarios where users interacted with search bars, intake forms, or URLs that could reveal health-related data. The alleged HIPAA violation supplied the "criminal or tortious act" that triggered the crime-tort exception. Federal district courts in multiple jurisdictions allowed ECPA claims premised on HIPAA violations to survive motions to dismiss.

This health care-focused application of the crime-tort exception seemed to cabin the ECPA's reach. Then came the pivotal August 2025 ruling that expanded the theory well beyond the health care industry.

The Ruling That Changed the Game: *Smith v. Rack Room Shoes*

The Case

The case that opened the floodgates was a class action filed against Rack Room Shoes, Inc.—a footwear retailer, not a HIPAA-regulated health care entity. The complaint alleged that Rack Room embedded tracking technologies from multiple third-party companies, including Meta and Attentive, into its website. These tools allegedly intercepted visitors' browsing activity, purchase history, and other personally identifiable information, and transmitted that data to third parties for commercial use.

To overcome the one-party consent defense, the plaintiffs invoked the crime-tort exception and argued that the interception was carried out for the purpose of committing the tort of intrusion upon seclusion. Crucially, the plaintiffs anchored their claim in the retailer's own privacy disclosures, pointing to alleged misrepresentations including statements that the company collected information through cookies and beacons but that "none of the information collected through cookies or beacons is personally identifiable," that the usage of cookies was "in no way linked to any Personal Information while on our site," and that consent banner language stated that necessary cookies "do not store any personally identifiable information."

The plaintiffs argued these representations created a reasonable expectation of privacy for website visitors and that the representations were false, thus undermining that expectation and supplying the independent tort.

Judge Lin's August 4, 2025 Ruling

On August 4, 2025, Judge Rita F. Lin of the Northern District of California issued a ruling on the defendant's second motion to dismiss, allowing the Wiretap Act claim to survive. The key passage of the ruling stated that plaintiffs adequately alleged Rack Room "intended to disclose its customers' personally identifiable communications, which it had promised not to collect or use, to third parties so that it could deliver targeted

ads to its customers," and that this alleged conduct, "in contradiction [of] the commitments it made in its privacy policy, can plausibly constitute a further invasion of privacy beyond the act of intercepting the information alone."

The court expressly analogized the privacy policy misrepresentation theory to the HIPAA-based crime-tort cases, stating that "the allegations are analogous to the purpose of engaging in a HIPAA violation, which courts consistently find constitutes an independent prohibited purpose" under the ECPA's crime-tort exception. The court also rejected the defense argument that a primary financial motivation should shield the defendant from liability, joining what it described as the majority of courts holding that "a monetary purpose does not insulate a party from liability under the Wiretap Act, at least at the motion to dismiss stage."

The Replicable Formula and Its Implications

A Template for Plaintiffs Nationwide

What the *Smith v. Rack Room Shoes* decision effectively established is a replicable formula for stating an ECPA cause of action against virtually any company that operates a website and makes certain privacy disclosures. The formula has three core elements: (1) the company deployed third-party tracking technologies on its website; (2) those technologies intercepted visitors' electronic communications; and (3) the company's own privacy policy, cookie banner, or other disclosures contained statements that were allegedly inaccurate or misleading regarding the collection, use, or sharing of personally identifiable information, thereby establishing an independent tortious purpose under the crime-tort exception.

This formula is particularly potent because it turns the company's own privacy disclosures into the plaintiffs' primary exhibits. Rather than needing to prove a violation of a sector-specific federal statute like HIPAA, the plaintiffs need only identify discrepancies between what a privacy policy promises and what the company's tracking technologies actually do.

Why ECPA Claims Are More Dangerous Than CIPA Claims

The shift from state-law to federal ECPA claims carries several important strategic advantages for plaintiffs. First, the ECPA is a federal statute, meaning claims can be filed in any federal court nationwide, not just in all-party consent jurisdictions like California. Second, unlike CIPA claims, which require courts to wrestle with questions about whether tracking pixels intercept the "contents" of communications or merely capture "record information," the ECPA crime-tort formula focuses on the purpose of the interception rather than the nature of the intercepted data, sidestepping some of the defense-friendly rulings in the CIPA context. Third, approximately 70 percent of lawsuits alleging ECPA violations have been filed as class actions, amplifying exposure. And fourth, the Wiretap Act creates criminal liability that carries over into its civil remedies, providing an additional layer of severity for defendants to contend with.

What Companies Should Do Now

The good news is that companies can take proactive steps to reduce their litigation exposure. The central lesson of the *Smith v. Rack Room Shoes* decision is that privacy disclosures themselves have become both a sword and a shield: inaccurate disclosures create vulnerability, but accurate, carefully drafted disclosures can help neutralize the crime-tort theory. Businesses should consider the following measures:

Audit and update privacy policies. Companies should ensure that their privacy policies accurately reflect the actual data collection, sharing, and use practices associated with every tracking technology deployed on

their websites. Statements claiming that cookies do not collect personally identifiable information, for example, should be verified against the actual functionality of the technologies in question.

Review cookie banners and consent mechanisms. Cookie consent banners and associated disclosures should be reviewed for accuracy. Any claims about what categories of cookies do or do not collect should be confirmed through technical audits. Courts have scrutinized the adequacy of browsewrap-style consent mechanisms, and some have found that hyperlinks buried in website footers are insufficient to put users on notice. Businesses should consider implementing affirmative consent mechanisms, such as pop-up banners that require users to click to accept or reject cookies.

Conduct regular technical audits. Organizations should regularly engage independent third parties to test website cookie consent mechanisms and verify that opt-in and opt-out choices function as intended. This includes confirming that third-party scripts are not firing before users have provided consent and that the data transmitted to third parties matches what disclosures describe.

Manage third-party vendor relationships. Businesses should pass down compliance obligations to analytics and advertising technology vendors by contract, ensuring that data sharing practices are clearly defined and limited. The *Rack Room Shoes* court noted that it was relevant that the complaint did not allege the third parties were aware of the retailer's privacy policy commitments, suggesting that contractual protections and vendor communication may be relevant to future defenses.

Monitor the litigation and legislative landscape. The tracking technology litigation space continues to evolve rapidly, with new theories, rulings, and legislative proposals emerging on a regular basis. Companies should stay current on developments in California and other states with active privacy litigation, as well as federal court decisions interpreting the ECPA's crime-tort exception.

Conclusion

The *Smith v. Rack Room Shoes* ruling represents a significant and practical shift in the landscape of tracking technology litigation. By establishing that a company's own privacy policy misrepresentations can supply the predicate tort for a federal Wiretap Act claim, the decision created a formula that is simple to replicate, applicable across industries, and available to plaintiffs in every state. Companies that rely on common tracking technologies should treat the accuracy and completeness of their privacy disclosures as a first-order litigation risk management priority. The disclosures that once seemed like routine compliance documents are now the primary targets of a rapidly growing body of federal class action litigation.

For more information, please contact Jade Davis.

Shumaker