Shumaker

NOVEMBER 12, 2026 | PUBLICATION

Client Alert: Beyond the Pixel: Fifth Circuit Decision Signals Expanding Privacy Litigation Risks for Businesses Using Website Tracking Technologies

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Businesses have increasingly relied on website tracking technologies to understand consumer behavior, measure advertising performance, and personalize digital experiences. But a recent federal appellate decision underscores a growing legal concern: information that appears to be ordinary website activity may expose businesses to significant privacy litigation when transmitted to third-party advertising platforms.

On October 23, 2026, the U.S. Court of Appeals for the Fifth Circuit issued its decision in *Rand v. Eyemart Express, L.L.C.*, No. 25-10784 (5th Cir. Oct. 23, 2026)[1], reversing the dismissal of a proposed class action alleging that an optical retailer improperly disclosed consumers' health-related information to Meta Platforms, Inc. (Meta) through the Meta Pixel.

The court concluded that the plaintiffs sufficiently alleged an injury to establish Article III standing and plausibly alleged that their website interactions constituted individually identifiable health information (IIHI) transmitted to Meta without their knowledge or consent.

Although the ruling does not establish liability, it has important implications for businesses using advertising pixels, analytics tools, session-replay software, and other website tracking technologies.

The central lesson is that privacy litigation exposure increasingly depends not merely on what information a business intentionally collects, but also on what its digital technologies disclose to third parties and what

those third parties can infer from the information received.

The Dispute: When Website Activity Becomes Health Information

Eyemart Express (Eyemart) operates retail locations and a website that allows consumers to browse eyewear, purchase prescription glasses, and schedule eye examinations.

According to the complaint, Eyemart implemented the Meta Pixel, a tracking technology designed to collect information about website interactions and transmit that information to Meta for advertising and analytics purposes.

The plaintiffs, all Facebook users, alleged that the technology transmitted information concerning their searches, product selections, prescription eyewear purchases, and appointment-scheduling activity.

They further alleged that Meta could associate these interactions with identifiable Facebook users, allowing the company to connect individuals with specific health-related products and services.

The plaintiffs asserted claims under several legal theories, including:

- The federal Wiretap Act, part of the Electronic Communications Privacy Act
- The Missouri Wiretap Act
- The Illinois Eavesdropping Act
- Common-law intrusion upon seclusion
- Breach of contract

Notably, the plaintiffs did not assert a direct claim under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Rather, they relied on HIPAA's definition of IIHI to characterize the information allegedly disclosed.

The district court dismissed the action, concluding that the plaintiffs had not adequately alleged the disclosure of qualifying health information to Meta.

The Fifth Circuit disagreed, reversing the dismissal and returning the case to the district court for further proceedings.

A Significant Development in Article III Standing

One of the most consequential aspects of *Rand* is the Fifth Circuit's treatment of standing in privacy litigation.

Following the U.S. Supreme Court's decision in *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), defendants have frequently challenged whether plaintiffs alleging statutory privacy violations suffered a sufficiently concrete injury to pursue claims in federal court.

In *Rand*, the Fifth Circuit concluded that the alleged unauthorized disclosure of identifiable health information constituted a concrete and particularized injury.

The court explained that the alleged harm was closely analogous to injuries historically recognized under common-law privacy torts, including intrusion upon seclusion and public disclosure of private facts.

Importantly, the plaintiffs were not required to demonstrate that they had experienced identity theft, financial

loss, or another conventional economic injury.

Instead, the alleged unauthorized disclosure of their private health-related information was sufficient to establish injury in fact.

The Fifth Circuit's analysis follows decisions from other federal appellate courts recognizing standing in cases involving the alleged unauthorized disclosure of digital activity, including:

- *Salazar v. Paramount Global*, 133 F.4th 642 (6th Cir. 2025)
- *Pileggi v. Washington Newspaper Publishing Co.*, 146 F.4th 1219 (D.C. Cir. 2025)
- *Salazar v. National Basketball Ass'n*, 118 F.4th 533 (2d Cir. 2024)
- *In re BPS Direct, LLC; Cabela's LLC Wiretapping Litigation*, 175 F.4th 423 (3d Cir. 2026)

Collectively, these decisions reflect increasing appellate recognition that the unauthorized disclosure of certain identifiable digital activities can constitute a legally cognizable privacy injury.

For defendants, this development may complicate early efforts to dispose of tracking-related litigation solely on standing grounds.

Nevertheless, establishing Article III standing is not equivalent to establishing a statutory violation. Plaintiffs must still satisfy the substantive requirements of their asserted causes of action, including any applicable interception, consent, party-exception, contractual, and other elements or defenses.

The distinction remains critical for businesses defending website-tracking claims.

Health Information Is Not Limited to Medical Records

Perhaps the most significant aspect of *Rand* is the court's treatment of information generated through ordinary website interactions.

The plaintiffs fell into two categories: consumers who searched for prescription eyewear or scheduled eye examinations, and consumers who purchased prescription eyewear and provided prescription-related information.

The district court had determined that merely browsing prescription eyewear did not constitute the disclosure of health information.

The Fifth Circuit rejected that narrow interpretation.

Applying HIPAA's statutory definition of IIHI for purposes of analyzing the plaintiffs' allegations, the court explained that information need not reveal a particular diagnosis or medical condition to relate to an individual's health or the provision of healthcare.

The court emphasized the relationship between the information collected, the services offered, and the ability to associate the information with an identifiable individual.

This reasoning has implications beyond traditional healthcare providers.

Businesses operating in industries such as vision care, pharmacies, fertility services, behavioral health, medical devices, wellness services, and other health-adjacent markets may collect information through digital interactions that reveal something about a consumer's healthcare interests or activities.

A website visitor might never provide a medical history, enter a diagnosis, or submit a patient intake form. Nevertheless, interactions with particular products, services, or appointment-scheduling features may generate information that plaintiffs contend is sensitive and individually identifiable.

That does not mean every visit to a health-related website constitutes IIHI. The nature of the information, its relationship to healthcare, the identity of the recipient, and the surrounding circumstances remain important.

But *Rand* demonstrates why businesses should avoid assuming that information is legally insignificant merely because it originates from a public-facing webpage.

The HIPAA Distinction: Regulatory Compliance Is Not the Entire Analysis

The Fifth Circuit's reliance on HIPAA's definition of IIHI warrants careful consideration.

HIPAA generally applies to covered entities and their business associates, subject to the statute's and regulations' applicable requirements. Not every business selling health-related products or services is necessarily subject to HIPAA.

Further, HIPAA does not provide individuals with a private right of action for damages.

Neither principle, however, necessarily insulates a business from privacy litigation involving information associated with health-related activities.

In *Rand*, HIPAA's definition of IIHI informed the court's analysis of the nature of the information allegedly disclosed. The plaintiffs pursued their claims through other federal and state laws and common-law theories.

The court did not determine that Eyemart violated HIPAA, nor did it resolve whether the alleged conduct ultimately violated the wiretap statutes or other laws asserted.

This distinction is particularly important for organizations that have historically evaluated website tracking primarily through a HIPAA compliance lens.

A business may conclude that it is not a HIPAA-covered entity and still face allegations involving unauthorized interception, disclosure of private information, deceptive privacy representations, or other statutory and common-law claims.

The absence of a HIPAA obligation does not necessarily mean the absence of privacy litigation risk.

Conversely, the use of HIPAA terminology in a complaint does not automatically establish that the information is legally protected under every statute invoked or that a disclosure was unlawful.

Each cause of action requires a separate legal analysis.

Why the Decision Matters Beyond California

For several years, California has been a focal point for website-tracking litigation, including claims under the California Invasion of Privacy Act (CIPA).

Plaintiffs have increasingly challenged the deployment of advertising pixels, session-replay technologies, chat tools, and other third-party website integrations, often alleging that those technologies intercept communications without appropriate consent.

The *Rand* decision reinforces that these disputes are not confined to California.

The Fifth Circuit has jurisdiction over federal appeals from Texas, Louisiana, and Mississippi. Its decision provides additional appellate authority for plaintiffs pursuing claims arising from website tracking in those jurisdictions.

The underlying lawsuit also illustrates how a single website's technology can become the subject of claims invoking multiple states' privacy and communications statutes.

This creates an important challenge for businesses operating nationally.

A company may deploy a single website, advertising platform, and consent management solution across the United States while interacting with consumers whose claims may implicate different state laws.

Those laws may vary materially in their definitions of interception, requirements for consent, available statutory damages, and defenses.

Accordingly, a website tracking program designed solely around one state's privacy requirements may not adequately address the full range of potential litigation exposure.

The Hidden Risk: What Third Parties Can Learn from Website Data

The practical significance of Rand extends beyond the Meta Pixel itself.

Modern websites often rely on interconnected technologies, including Google Analytics, Google Tag Manager, advertising conversion tools, customer relationship management integrations, session-replay platforms, and marketing automation software.

These technologies may collect or transmit information such as page addresses, search terms, product identifiers, event names, transaction details, device identifiers, and other data associated with user activity.

Individually, certain data elements may appear innocuous.

When combined with other information available to a third-party platform, however, those elements may reveal substantially more about an identifiable individual.

For example, a business might configure an advertising tool to record when a consumer selects a particular product or initiates an appointment request.

Even without transmitting a diagnosis, the event may disclose a meaningful connection between an identifiable consumer and a health-related product or service.

The Fifth Circuit's analysis illustrates why the recipient's ability to connect website activity with an existing user profile matters.

For businesses, this means evaluating website tracking requires more than identifying whether a particular form collects names, email addresses, or medical information.

It requires understanding the actual transmission of information between the website and third parties, including how transmitted data may be associated with individuals.

The analysis should also account for server-side tracking, conversion APIs, customer-list uploads, and other

integrations that may not be apparent from a conventional browser-based review.

Consent Management Platforms Are Not a Substitute for Technical Compliance

Many organizations have responded to the increase in website-tracking litigation by implementing consent management platforms (CMP) and cookie banners.

These technologies can be valuable components of a privacy compliance program, but their effectiveness depends on proper configuration and implementation.

A website may display a consent banner while certain tracking technologies continue to transmit information before the user makes a selection.

Similarly, a CMP may block some categories of cookies without necessarily preventing every network request, server-side event, or third-party disclosure.

Businesses should therefore distinguish between the existence of a consent mechanism and its actual technical operation.

Relevant considerations include whether:

- Nonessential tracking technologies activate before consent where consent is legally required
- A user's rejection or withdrawal of consent prevents the relevant subsequent transmissions
- Consent preferences are consistently implemented across pages, devices, and integrated technologies
- Sensitive product, scheduling, account, and transaction pages are subject to appropriate restrictions
- Third-party scripts or server-side integrations bypass the intended consent controls
- Privacy notices accurately describe the organization's actual collection and disclosure practices

Consent requirements vary depending on the applicable law, the nature of the technology, and the information involved. A universal opt-in requirement does not necessarily apply to every website or tracking activity.

Nevertheless, businesses should ensure that their consent practices align with the legal requirements governing their operations and with the technologies actually deployed.

A privacy notice or cookie banner that does not reflect the underlying data flows may provide considerably less protection than an organization anticipates.

Practical Steps for Businesses to Reduce Website-Tracking Exposure

In light of *Rand* and the continuing development of website-tracking litigation, organizations should consider a coordinated legal and technical assessment of their digital environments.

1. Conduct a comprehensive tracking technology inventory.

Identify advertising pixels, analytics tools, session-replay technologies, chat applications, conversion APIs, and other integrations operating across websites and mobile applications.

The inventory should include technologies implemented through tag management systems, third-party plugins, and server-side configurations.

2. Examine actual data transmissions.

Evaluate the information transmitted to third parties during relevant user interactions, including browsing, searches, account creation, purchases, and appointment scheduling.

Technical testing should assess both the content of transmissions and the circumstances under which they occur.

3. Identify sensitive pages and user journeys.

Pay particular attention to pages involving healthcare services, prescription products, financial information, or other potentially sensitive activities.

Organizations should consider whether advertising or analytics functionality is necessary on those pages and whether less intrusive configurations are available.

4. Validate consent management configurations.

Test whether tracking technologies operate consistently with applicable consent requirements and the organization's stated privacy practices.

Testing should include scenarios in which users accept, reject, or withdraw consent.

5. Review third-party agreements and platform configurations.

Evaluate the contractual terms governing advertising, analytics, and other technology providers, including provisions addressing permitted data uses, restrictions on sensitive information, and the parties' respective compliance responsibilities.

6. Align privacy disclosures with actual practices.

Review privacy policies, cookie notices, and other consumer-facing disclosures to ensure they accurately describe the organization's collection, use, and disclosure of website information.

7. Establish ongoing governance and change management.

Website tracking configurations change frequently as marketing teams introduce new campaigns, vendors, and technologies.

Organizations should establish procedures for reviewing new integrations, documenting compliance decisions, and periodically validating existing controls.

Importantly, these reviews should involve collaboration among legal, information technology, cybersecurity, marketing, and privacy personnel.

A legal assessment without technical validation may overlook how information is actually transmitted. Conversely, a technical assessment without consideration of applicable privacy laws may fail to identify material legal exposure.

What Businesses Should Watch Next

The Fifth Circuit's decision does not resolve whether Eyemart ultimately violated the federal Wiretap Act, the Missouri Wiretap Act, the Illinois Eavesdropping Act, or any other law asserted by the plaintiffs.

Those substantive issues remain for further proceedings.

The court also did not establish that every advertising pixel is unlawful or that every interaction with a health-related website constitutes protected health information.

Nevertheless, *Rand* represents another important development in the evolving judicial treatment of digital privacy injuries and website tracking.

It also highlights the increasing significance of the relationship between website activity, third-party data collection, and consumer identifiability.

For businesses, the implications are broader than the particular technology or industry involved.

The relevant question is no longer simply whether a website collects sensitive information directly from consumers. Businesses must also understand whether their digital tools allow third parties to receive, associate, or infer sensitive information from ordinary website interactions.

As privacy litigation continues to develop across federal circuits and under different state statutory frameworks, businesses should approach website tracking as an enterprise privacy governance issue rather than solely a marketing or website functionality decision.

Organizations that proactively assess their tracking technologies, validate their consent mechanisms, and align their data practices with applicable legal requirements will be better positioned to identify potential exposure and defend their practices if challenged.

Shumaker's Technology, Data Privacy, Cybersecurity & Artificial Intelligence service line advises businesses on the legal, regulatory, and operational challenges associated with emerging technologies and the collection, use, and protection of information.

Our attorneys assist organizations with privacy compliance programs, website-tracking and consent management assessments, technology agreements, cybersecurity governance, incident response, and the defense of privacy-related claims.

For additional information about the implications of *Rand v. Eyemart Express* or assistance evaluating website tracking technologies and related litigation risks, contact Shumaker's Technology, Data Privacy, Cybersecurity & Artificial Intelligence team.

This article is provided for informational purposes only and does not constitute legal advice.

If you have any questions or to learn more, please contact a member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line.

https://www.ca5.uscourts.gov/opinions/pub/25/25-10784-CV0.pdf

[1] https://www.ca5.uscourts.gov/opinions/pub/25/25-10784-CV0.pdf

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker