JANUARY 13, 2025

Year in Review: What You Need to Know about 2024 Web Tracking Litigation

by Meghan K. Farmer , Tatum Andres

This article was also contributed to by Mitch Seymour of Honeypot Technologies.

Overview

In 2024, lawsuits targeting companies for their use of commonly deployed digital tracking technologies, such as pixels, and session replay tools proliferated. Frequently used on apps and websites, tracking technologies enable businesses to collect data about user interactions to refine marketing strategies and improve engagement. Plaintiffs now allege that the tracking technologies "record" or "intercept" user interactions without appropriate consent in violation of state and federal laws. As these cases make their way through the courts, we can glean important insights into emerging trends and legal developments in tracking technology litigation.

Here are Three Things You Can Do to Reduce Your Risk

1. Stay Informed About Applicable Laws - They May Not Be the Ones You Expect.

Plaintiffs' attorneys are leveraging old statutes like the California Invasion of Privacy Act of 1967 (CIPA),[1] the Video Privacy Protection Act of 1988 (VPPA),[2] the Song-Beverly Credit Card Act of 1970,[3] and Arizona's Telephone, Utility, and Communication Service Records Act of 2006 (TUSCRA) [4] to challenge practices involving the recording or interception and sharing of user information using modern-day online tracking tools. Courts must determine if these statutes—originally designed to apply to telephones, brick and mortar video rental stores, and paper receipts—apply to communications collected by technologies like pixels and similar technologies. Many claims are dismissed because the recorded data does not meet the statutory definitions, underscoring the difficulty of applying outdated laws to modern contexts, but in 2024 there were cases that proceeded on the basis that users did not properly consent to the data collection practices because businesses had insufficient cookie policies and privacy policies, and a reasonable user reading them would not believe they were consenting to the collection of certain personal data.[5]

2. Adapt to Change - Be Aware of Evolving Court Interpretations of Key Terms.

Inconsistent judicial rulings have encouraged plaintiffs to broaden the scope of wiretap litigation. At the heart of these claims is the assertion that companies are allowing third parties to "eavesdrop" on users'

online activities without obtaining proper consent. Plaintiffs frame the use of tracking technologies like pixels and session replay software as invasive practices akin to wiretapping. The legal landscape for such claims varies by jurisdiction. For example, under federal law, only one party needs to consent to recording conversations (including chatbot interactions). Most states follow this "one-party consent" rule, but states with "all-party consent" laws, like California, have seen significant legal activity. These states generally require prior consent from all parties if the recorded content involves individuals with a reasonable expectation of privacy.

Recent lawsuits now target the unauthorized collection of consumer information, including email addresses, IP addresses, and consumer data obtained from AI-driven chatbots and advanced analytics tools, citing violations of wiretapping laws. Courts are split on whether technology providers act as third-party eavesdroppers or are integral to the defendant's business operations. Additionally, courts are split on if these laws apply to tracking technology. In *Vita v. New England Baptist Hospital,*[6] Massachusetts' highest court ruled that website interactions do not constitute "communications" under the state's wiretap law. The court emphasized that the statute, enacted in 1968, was designed to protect person-to-person conversations, not interactions with pre-generated web content. This conservative interpretation contrasts with broader readings in California and Pennsylvania, illustrating the jurisdictional variability in tracking technology litigation. This lack of uniformity creates an opening for plaintiffs to test novel legal theories.

3. Be Proactive - Understand and Configure Your Tracking Tools with Notice and Consent in Mind to Ensure Compliance.

To combat the above claims, businesses must prioritize understanding the tracking tools they deploy and the personal data these tools collect from consumers. While successful defenses against this type of litigation are emerging, such claims can often be avoided altogether if businesses take proactive measures to their tracking practices with legal standards before challenges arise.

Emerging Defenses in Privacy Litigation

The following are effective defenses that businesses are increasingly leveraging to navigate privacy litigation successfully:

- **Lack of Standing:** Plaintiffs must prove a concrete injury, such as unauthorized capture of personally identifiable information (PII), to establish standing. Courts have dismissed cases where no such injury is demonstrated. For example, in cases involving anonymized session replay data, courts have dismissed claims for failing to meet this standard. The rationale is that session replay data, when stripped of identifying details, does not constitute a harm sufficient to meet standing requirements. These decisions emphasize the need for plaintiffs to show actual, tangible harm rather than speculative or abstract injuries.

- **Party Exemption:** Courts remain divided on whether technology providers should be treated as independent third-party eavesdroppers or as tools of the defendant's business. Two lines of

reasoning have emerged:

- *Javier* Line: Courts following the *Javier v. Assurance IQ, LLC*[7] interpretation have ruled that technology providers qualify as independent third-party eavesdroppers if they can exploit intercepted data for their own purposes. For example, marketing companies that use collected data to build their own databases are treated as separate entities from the defendant. This line of reasoning imposes greater risks for businesses using third-party tools that retain or monetize user data.
- *Graham* Line: Conversely, courts following the approach in *Graham v. Noom*,[8] have held that providers acting solely to support the defendant's operations are not independent eavesdroppers. These providers are likened to tape recorders—tools that passively collect data without any independent intent to use or profit from it. This reasoning protects companies whose technology partners serve as mere extensions of their business processes.

Companies should carefully assess whether their providers may be considered independent eavesdroppers, as in Javier, or mere extensions of their operations, as in Graham. To mitigate risks, businesses should prioritize partnering with vendors whose data collection practices are strictly limited to supporting business operations, avoiding relationships with providers that monetize or independently retain user data.

- **Consent:** Demonstrating user consent remains a critical defense in these cases, with courts scrutinizing whether companies effectively informed users and obtained proper authorization for data collection. Key distinctions have emerged between effective and flawed consent mechanisms:

- Effective Consent: Courts have endorsed practices where companies ensure robust and informed consent, including offering equally prominent "accept" and "decline" options on consent banners and clearly informing users about the nature of tracking technologies to enable informed decision-making.
- Flawed Consent: Courts have invalidated consent mechanisms when notices are inconspicuous, poorly designed, or difficult to read. For example, small text, inconspicuous color schemes, or notices that fail to appear in a timely manner may result in a finding that users could not reasonably know or agree to the company's privacy practices. As one court noted, [9] users must be able to meaningfully understand their options and the implications of their choices for consent to be valid.

Businesses should implement clear, user-friendly cookie banners and privacy policies that transparently inform users about the nature and purpose of data collection. Consent banners must offer equally prominent "accept" and "decline" options to meet statutory requirements and validate user consent. Additionally, businesses should clearly communicate how user data will be used and shared, aligning their privacy practices with users' reasonable expectations. Ambiguous or inconspicuous consent mechanisms can undermine trust and fail to meet legal standards, increasing the risk of litigation.

Regularly reviewing and updating privacy policies to reflect evolving legal standards ensures that consent mechanisms remain effective and defensible.

Looking Ahead

To stay ahead of evolving privacy challenges and minimize litigation risks in 2025 and beyond, businesses must embrace clear, comprehensive disclosures, implement robust consent frameworks, and maintain unwavering compliance with privacy laws. By taking these proactive steps, you won't just protect your organization—you'll also strengthen user trust and demonstrate your commitment to transparency and accountability. Our expert legal services are ready to partner with you, helping evaluate your data collection and sharing practices, uncover potential risks in third-party partnerships, and craft consent mechanisms that align seamlessly with statutory and regulatory standards.

Footnotes

---

[1]California Penal Code § 638.51 (2023).

[2]Video Privacy Protection Act of 1988 (18 USC § 2710).

[3]California Song-Beverly Credit Card Act, Cal. Civ. Code § 1747.08.

[4]Arizona Telephone, Utility, and Communication Service Records Act A.R.S. § 44-1376 et seq.

[5]*See for example, Calhoun v. Google, LLC,* No. 22-16992, 2024 U.S. App. LEXIS 20978 (9th Cir. Aug. 20, 2024).

[6]*Vita v. New England Baptist Hospital*, SJC-13542, 2024 WL 4558621 (Mass. Oct. 24, 2024).

[7]*Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022).

[8]*Graham v. Noom,* 533 F. Supp. 3d 823 (N.D. Cal. 2021).

[9]*Price v. Carnival Corporation,* 2024 WL 221437 (S.D. Cal., January 19, 2024).