Gallagher

# The Website Tracking Risk
# **Hiding in Plain Sight**

Tracking pixels, session replay, and cookie-consent tools are driving a wave of litigation. Most companies don't fully understand the risk — and few know whether their cyber insurance would respond.

# Wrongful collection is a growing exposure companies underestimate

Most companies understand the data they collect directly. Far less visible is the data transmitted in the background every time someone visits their website, through tracking pixels, session-replay tools, and third-party analytics scripts.

These tools are used across nearly every marketing and product team to measure performance and improve digital experiences. Increasing litigation activity and regulatory scrutiny have made website tracking a growing area of privacy risk for organizations.

Two gaps drive the exposure: most organizations assume a privacy-policy disclosure is enough, and few can say whether their cyber insurance would cover a claim.

# How tracking pixels create legal exposure

A tracking pixel is a small piece of code embedded in a web page or email. When the page loads or a user takes an action, it sends data such as IP addresses, pages viewed, search activity, device identifiers, and form-field interactions, to a third party such as an analytics provider or advertising platform. In some cases, data may be transmitted in real time and before a user has provided consent. The evolving legal environment is what makes this risk significant.

In California and other states, real-time data sharing with third parties is increasingly treated under decades-old wiretapping and interception laws, statutes written for phone calls, now applied to digital tracking. Statutory damages per violation add up quickly in a class-action setting. Litigation involving website tracking technologies has increased significantly in recent years and a plaintiff need not even be a customer: a single website visit can be enough to trigger a claim.

# Disclosure is no longer enough

Many companies assume their privacy policy covers them. Courts and regulators are increasingly focusing on consent rather than disclosure alone.

Telling users that tracking occurs may not protect an organization if data is collected before users take a clear, affirmative action to allow it. The same gap appears in cookie banners that offer a "reject" option while scripts keep firing underneath. That difference, between what users are shown and what actually happens, is where these cases are built.

# Examples of website tracking claims

| Type of Claim | What Is Alleged |
|---|---|
| 1 **Tracking Pixel Claim** | A website visitor alleges that information about pages visited and actions taken on the website was transmitted to a third-party advertising platform without proper consent. |
| 2 **Session Replay Claim** | A plaintiff alleges that website interactions — clicks, keystrokes, or form activity — were intercepted and shared with a third-party analytics provider. |
| 3 **Cookie Consent Banner Claim** | A company represents that users can reject non-essential tracking technologies, but technical testing allegedly reveals that certain tracking scripts continue to activate regardless of user preference. |
| 4 **AI Chatbot Privacy Claim** | Customer inquiries submitted through an AI-powered chatbot are allegedly transmitted to third-party providers without clear disclosure or consent. |

## The question few companies can answer: would your cyber insurance respond?

If a tracking-related class action arrived tomorrow, would your policy cover it? The answer is rarely automatic. Many cyber policies contain wrongful-collection, invasion-of-privacy, or wiretapping-related exclusions; others sublimit these claims or treat them very differently from a traditional data breach. Because these matters often don't involve a traditional data breach, coverage may depend on how policy terms, exclusions and definitions apply to the specific allegations.

Two companies with similar-looking coverage can end up with very different outcomes, which is why this analysis is worth doing before a demand letter arrives, not after.

## What legal, marketing, and risk teams should prioritize

- Audit every tracking technology on your site. Marketing stacks grow without central oversight, and agencies or legacy projects often add scripts no one is tracking.
- Map the data flow — what is collected, how it is transmitted, and which third parties receive it.
- Test consent; don't assume it. Confirm non-essential tracking is blocked until a user affirmatively opts in, across all pages and devices.
- Review disclosures for specificity — general language creates gaps between what is stated and what occurs.
- Pressure-test your insurance. Confirm how your cyber program treats tracking, wrongful-collection, and privacy claims before you need it.
- Document consent practices, audits, and remediation — these records can be critical in a dispute.

Website tracking has evolved from a compliance consideration into a broader governance and risk-management issue.

The key question is simple: would your current practices, and your insurance, withstand scrutiny? Gallagher's Technology practice helps software companies, IT services providers, and technology-enabled businesses evaluate website tracking exposures, strengthen privacy governance, and better understand how their cyber insurance may respond to website tracking and privacy-related claims.

ajg.com/industries/technology-insurance