SpencerFane®

Navigating the Rising Risk of Website Tracking Litigation: What Business Leaders Need to Know

In today's digital-first economy, website tracking technologies – such as cookies, pixels, and session replay tools – are essential for understanding user behavior, optimizing marketing, and driving business growth. However, a surge in lawsuits and regulatory scrutiny has made the use of these tools a significant legal risk for organizations across industries. Business leaders must understand the evolving landscape of website tracking litigation, recognize which activities can trigger claims, and implement robust compliance strategies to protect their companies. If your organization receives a legal demand or lawsuit related to website tracking, experienced legal counsel can make all the difference.

The Legal Risks of Website Tracking

Over the past several years, a multitude of lawsuits have been filed against businesses for their use of tracking pixels and similar technologies. Plaintiffs allege that these tools collect and share user data with third parties without adequate disclosure or consent in violation of privacy laws such as the California Invasion of Privacy Act (CIPA), the Video Privacy Protection Act (VPPA), HIPAA, and various state wiretapping statutes. The statutory damages they assert are intimidating, with CIPA, for example, imposing $5,000 per violation, and class actions multiplying potential exposure into the millions.

The risk is not limited to consumer-facing companies. Any business that collects, shares, or analyzes user data through website tracking tools can be targeted, especially if sensitive information is involved or if disclosures and consent mechanisms are lacking.

California's Legislative Response – and Its Delay

Recognizing the explosion of litigation and the uncertainty it created for businesses, California lawmakers introduced Senate Bill 690 (SB 690) earlier this year. This bill was designed to clarify and limit the application of CIPA to common website tracking technologies, such as cookies, pixels, and session replay tools, when used for legitimate commercial business purposes. SB 690 would provide a safe harbor for businesses, exempting standard tracking practices from CIPA's wiretapping prohibitions and significantly reduce litigation risk for companies using these tools in the ordinary course of business.

However, despite strong support from the business community, SB 690 has recently been delayed and is now not expected to be considered until 2026, at the earliest. This postponement has left businesses in a continued state of legal uncertainty. Importantly, the delay has created a "window of opportunity" for plaintiffs and their attorneys, who are now filing claims at an accelerated pace in anticipation of the law's eventual passage.

What Business Activities Trigger Claims?

Several common business activities have been at the center of recent litigation:

- **Embedding Pixels on Sensitive Webpages:** Health care providers and other organizations have faced lawsuits for placing tracking pixels on appointment scheduling pages, patient portals, or pages discussing health conditions. These pixels can transmit protected health information (PHI) to third parties, potentially violating HIPAA and state privacy laws.
- **Tracking User Interactions for Marketing:** Retailers and e-commerce businesses often use pixels to monitor product views, cart additions, and purchases. Sharing this data with ad networks without clear user consent can trigger claims under state wiretapping laws and consumer privacy statutes.
- **Streaming Video Content with Tracking:** Companies that stream video content and use pixels to monitor engagement have been sued under the VPPA for sharing viewing data with third parties.
- **Session Replay and Keystroke Monitoring:** Tools that record user sessions or keystrokes can capture sensitive information and have led to lawsuits under

wiretapping statutes.
- **Failure to Disclose or Obtain Consent:** Many lawsuits allege that users were unaware of data collection and sharing, highlighting the importance of clear, conspicuous disclosures and valid consent.

How Companies Can Protect Themselves

To mitigate the risk of website tracking litigation, business leaders should prioritize the following best practices:

1. **Audit Your Tracking Technologies:** Conduct a comprehensive inventory of all tracking tools on your website, including what data is collected, how it is used, and where it is sent.
2. **Enhance Transparency and Consent:** Update privacy policies to clearly disclose tracking activities and implement robust cookie consent mechanisms that comply with applicable laws.
3. **Limit Data Collection:** Only collect data necessary for your business purposes and avoid gathering sensitive information unless absolutely required and legally justified.
4. **Review Vendor Agreements:** Ensure contracts with third-party tracking providers include appropriate data protection provisions and clarify roles and responsibilities.
5. **Regularly Assess Risks:** Periodically review your tracking practices and stay informed about evolving legal requirements and regulatory guidance.
6. **Train Your Team:** Educate employees involved in website management and marketing about privacy obligations and compliance best practices.

Responding to Website Tracking Claims: Practical Guidance

When a business receives a demand letter or lawsuit related to website tracking, it's important to respond promptly and with a clear strategy. Legal and technical professionals can provide valuable support in addressing these issues. Common areas of assistance include:

- Coordinating technical audits and forensic reviews of website tracking tools
- Evaluating the legal basis of claims and assessing potential exposure

- Preparing responses to demand letters and formal complaints
- Managing litigation, including motions and class action defense
- Facilitating settlement discussions and regulatory communications
- Advising on compliance improvements to reduce future risk

By working with professionals who understand both the legal and technical dimensions of website tracking, organizations can better manage risk, maintain compliance, and protect their reputation. Whether addressing an active claim or proactively reviewing practices, taking informed steps can help safeguard business operations in a rapidly evolving regulatory environment.

This blog was drafted by Shawn Tuma, an *attorney in the Spencer Fane Plano, Texas office and the leader of the firm's Cyber | Data | Artificial Intelligence | Emerging Technology team. For more information, visit www.spencerfane.com.*

Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.