POLSINELLI

Publications

February 24, 2025 • Updates

Developments in Online Tracking Litigation: Risks Hiding in Plain Sight on Your Site

Litigation involving online tracking experienced a substantial year-over-year increase from 2023 to 2024, with a particularly significant increase in cases asserting claims under the California Invasion of Privacy Act (CIPA). Other web tracking-based claims also saw significant increases in 2024, including claims alleging violations of the Federal Wiretap Act (FWA) and claims asserting violations of other states' multiparty consent wiretapping statutes. While Video Privacy Protection Act (VPPA) claims experienced a slight decline during the first part of the year, filings started to creep up again after the Second Circuit's decision in Salazar v. NBA, No. 23-1147 (2d Cir. Oct. 15, 2024), held that a broad scope of individuals who may not have purchased video services could still be considered "consumers" under the VPPA. The plaintiffs' bar also advanced new claims against several e-commerce companies alleging online tracking-based violations of the Song-Beverly Credit Card Act of 1971. All of the foregoing causes of action have strict liability statutory penalties ranging from $250 to $10,000 per violation, which can become a significantly expensive problem even with relatively little website traffic.

The increase in online tracking lawsuits reflects a rapidly evolving legal landscape, with web tracking class actions becoming a persistent challenge for businesses across industries.

Tracking Technologies That Create Litigation Risk

There are numerous names for online tracking technologies: pixels, beacons, tags, cookies, scripts, etc. The functionalities can vary, but, at bottom, the tracking technologies that create litigation exposure are bits of code that collect and then share data about user interactions on a website. Third-party social media platforms like Meta, TikTok, LinkedIn, etc. often develop these code components so that businesses can leverage marketing opportunities on their platforms. Trackers can be configured to capture information such as operating system, browser type, IP address, time and device details, and more specific information, including how long a person spends on a web page, which buttons a person clicks, which pages a person viewed and which search terms a person entered. The code for these technologies can be viewed by anyone who visits the website on which they are deployed with a few mouse clicks, and some social media platforms permit users to find information about which organizations have leveraged these trackers to share that user's

Related People

- Starr Turner Drum
- Xeris E. Gregory

Related Capabilities

- Privacy & Cybersecurity
- Privacy Litigation

information with that social media platform.

Online Tracking Litigation Background

This surge in online tracking litigation has not come from legislatures passing new laws. Instead, the plaintiffs' bar has been testing the bounds of the application of old laws passed in the 1960s through the 1980s on new technology.

For example, CIPA was passed in 1967 and prohibits "wiretapping" and the use of a "pen register" or "trap and trace device" without the consent of the parties to a communication. The FWA was passed in 1968 and updated in relevant part in 1986. It prohibits intercepting a communication by a nonparty to the communication without consent of one party to the communication, and even if one party does consent to the interception, the interception may not be conducted for a criminal or tortious purpose. The VPPA was passed in 1988 and prohibits "video tape service providers" from disclosing video rental information without a consumer's consent.

The unifying theory when alleging that new technologies are violating these old laws is that tracking technologies allegedly disclose private information to third parties without consent. Outside of a recent ruling by the Massachusetts Supreme Court in Vita v. New England Baptist Hospital, SJC-13542 (Mass. Oct. 24, 2024), holding that its wiretapping law did not extend to online tracking technology, courts largely have not rejected these theories outright. In some cases, claims have been brought against websites that use cookie banners that ostensibly present users with an option to opt out but allegedly either transmit information before the user can opt out or continue to transmit information to third parties despite the user's selection to opt out. Defending these claims requires an analysis of the underlying technology on the website, the relevant disclosures made to users and any terms to which users are bound.

A Special Note for Health Care Defendants

Although no industry is safe from these claims, health care providers have been consistent targets in web tracking litigation during the past few years. The uptick correlated with a U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) bulletin issued in December 2022. The HHS OCR Bulletin asserted that information collected on a covered entity's website could constitute protected health information (PHI), even if an individual did not have an existing relationship with the covered entity and even if the information collected did not include specific treatment or billing information. Multiple lawsuits have been filed by website visitor plaintiffs against health care providers that had website analytics technologies installed on sections of their websites, particularly in the context of alleging that tracking on covered-entity websites violates the "criminal or tortious" provision of the FWA by allegedly constituting a HIPAA violation.

In November 2023, the American Hospital Association, the Texas Hospital Association and two health care providers filed a lawsuit to enjoin enforcement of the HHS OCR Bulletin. On June 20, 2024, the court vacated a portion of the HHS OCR Bulletin in a win for HIPAA-covered entities.[1] The court found the HHS OCR Bulletin required "covered entities to perform the impossible" and concluded that an individual's IP address combined with a visit to a web page addressing specific conditions or health care providers is not individually identifiable health information under HIPAA. While this may have lessened the threat of regulatory enforcement tied to this particular type of tracking, the plaintiffs' bar has thus far not retreated from asserting covered entities' website tracking activities constitute an FWA violation.

Avoiding Website Tracking Litigation Risk

The simplest way for companies to avoid website tracking litigation risk is to not deploy any third-party tracking tools on their web properties. This blunt approach could have negative business impacts, though, and a more nuanced approach can simultaneously preserve marketing benefits and reduce litigation risk. To take a more tailored approach to mitigating risk, companies can:

- Use internal resources or outside counsel to assess which third-party tracking technologies are used on the company's web properties.
- Work with web development and marketing teams to pressure test the utility of third-party trackers for the business and determine if any should be removed or should be isolated to specific pages or sections of the company's website.
- Consider the implementation of a consent management platform and implement geofencing and use case-specific opt-in configurations on those platforms.
- Assess and update website privacy policies to ensure they accurately disclose the use of tracking technologies.
- Assess and update terms of use to ensure the company is satisfied with its choice of forum and dispute resolution process.
- Consider opportunities to bind users to the company's terms of use through clickwrap or similar mechanisms and implement same.
- Monitor and regularly audit all of the foregoing.

[1] American Hospital Assn. v. Becerra, No. 4:23-cv-01110-P, (N.D. Tex. June 20, 2024)