Legal Update Article

What Real Estate Businesses Need to Know About Using Website Tracking Technologies

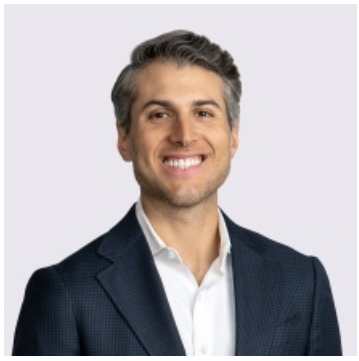
By Joanne Braddock Lambert, Damon W. Silver & John A. Snyder

January 25, 2024

Meet the Authors

Joanne Braddock Lambert

(She/Her)
Principal
407-246-8447
Joanne.Lambert@jacksonlewis.com



Damon W. Silver

Principal
(212) 545-4063
Damon.Silver@jacksonlewis.com

Real estate businesses frequently operate multiple websites. These may include corporate websites, websites for each of their properties, and websites for their apps and ancillary service offerings. To maximize the convenience and insights from their websites, real estate businesses often use a variety of website tracking technologies to better understand how visitors interact with their sites, to improve those sites, and to develop and execute advertising and marketing campaigns.

By managing these technologies in careful compliance with fast-evolving and ever-changing laws, real estate businesses can lower the risk of lawsuits and regulatory attention. Hundreds of lawsuits were filed in 2022 and 2023 alleging the use of various website tracking technologies violates wiretap and video privacy laws and constitutes a tortious invasion of privacy. Website tracking technologies have garnered regulatory attention particularly from the Federal Trade Commission (FTC) and the Department of Health and Human Services (HHS). Each of these federal governmental agencies has issued guidance on the privacy concerns presented by these technologies.

Real estate businesses can maintain safeguards to mitigate the risks of using website tracking technology. This article is intended to help real estate businesses better understand this new area and start honing their mitigation strategies.

Key Legal Claims

Most of today's websites use a variety of technologies to monitor, analyze, and respond to users' on-site activities. For instance, they track how long users spend on each page, what they click on, which videos they view, and what they say in communications with chatbots.

These technologies serve functions that most people consider legitimate, like showing them similar content of potential interest or remembering the contents of their shopping carts. On the other hand, the technologies are also responsible for making some people feel uncomfortable, for instance, by appearing to follow the viewer over the web, wherever they go, with ads of the apartment the user looked at on one website.

Two types of tracking activities have driven much of the litigation and enforcement activity so far: (1) allowing third parties to collect or access information about visitors' website activity for serving targeted ads; and (2) allowing third parties to access visitors' communications with chatbots.

Common claims include wiretap violations, invasion of privacy, breach of contract or violation of the Federal Trade Commission Act, and Video Privacy Protection Act (VPPA) violations.

Wiretap laws and the VPPA provide for statutory damages, as well as attorneys' fees. The per-violation cap is $2,500 under the VPPA. Damages for violating the federal

John A. Snyder
(He/Him)
Principal
(212) 545-4054
John.Snyder@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity
Real Estate
Website and Digital Tracking Compliance Assessment

Wiretap Act can be up to the greater of $100 a day or $10,000 per violation. Further, violations of California's wiretap law, the California Invasion of Privacy Act, can result in damages of up to $5,000 per violation.

Key Legal Defenses

A body of caselaw is starting to emerge. One key defense is establishing that the site visitor provided informed consent to the collection of their personal information by the site's tracking technologies. The key elements of this defense are (1) proper timing and (2) informed consent.

On the timing element, in a 2022 decision, a federal appellate court held that site owners must collect consent *before* tracking visitors' activities. Accordingly, a consent defense might not be viable to site owners that rely on disclosures in their privacy policy linked to the bottom of the site's home page or on consent collected as the visitor completes a transaction.

The standard for whether consent was adequately "informed" is unclear. Analysis of the current caselaw suggests that courts may undertake a fact-intensive inquiry, accounting for issues like the specific types of technologies used and the specific claims asserted. Erring on the side of detailed disclosure (*e.g.,* on the categories of tracking technologies used, personal information collected, and third parties with access to that information), for now, is the safer approach.

Other key defenses include:

- As to wiretap claims, arguing there was no "interception" where the third party did not gain *simultaneous* access to the site visitor's communications, but gained access at some subsequent point.

- For VPPA claims, arguing the site owner is not a "video tape service provider" because it is not "engaged in the business" of delivering video content (increasingly difficult to establish, at least at the motion-to-dismiss stage, as organizations increasingly incorporate video content into their product and service offerings or use it to bolster their brands).

- Procedural defenses like lack of personal jurisdiction, lack of standing because of insufficiently concrete harm, and expiration of the applicable statutes of limitations.

Mitigation Strategies

Zooming Out: Real estate businesses may benefit from zooming out and looking at website risk broadly. Currently, 14 states (led by California) have passed comprehensive privacy laws. These laws have broad definitions of "personal information" (or "personal data") that cover certain information collected by website tracking technologies and impose an array of obligations related to the collection and use of that information.

Using the California Consumer Privacy Act (CCPA) as an example, organizations that collect personal information from California residents must:

- Provide privacy notices at or before the time they begin collecting covered personal information;

- Post detailed privacy policies on their websites;
- Include specific provisions in contracts with vendors; and
- Extend certain rights to data subjects (*e.g.,* the right to access, correct, delete, or opt out of the sale or sharing of their information).

The CCPA also requires covered organizations to scrutinize how they are using and how long they are retaining personal information and imposes cybersecurity audit obligations.

Homework: Real estate businesses need to determine what website tracking technologies are in use on their sites, what information those technologies collect, and whether and to whom that information is disclosed. Acquisitions, turnover in marketing and web development teams, and other factors can make it difficult for real estate businesses to determine where they may have tracking technologies running on their sites without their knowledge and, in some cases, without delivering much, if any, return on investment.

Develop a Mitigation Plan

The specifics of this plan will vary depending on the business's operations and activities, but some of the key elements include:

- Mitigating class action litigation risk by eliminating unnecessary use of trackers and ensuring visitors receive clear, detailed, and timely notices regarding the tracking of their online activities and give consent to that tracking.
- Complying with state comprehensive privacy laws; for instance, by updating privacy policies and notices, ensuring service agreements with vendors include requisite terms, and developing processes to timely and properly respond to requests from data subjects.
- Reviewing data security risk assessments, policies, and procedures to ensure data collected by website tracking technologies is adequately addressed.

Please contact a Jackson Lewis attorney with any questions.