WHAT REAL ESTATE BUSINESSES NEED TO KNOW ABOUT USING WEBSITE TRACKING TECHNOLOGIES

DIANE KREBS is a principal in Jackson Lewis P.C.'s Long Island office and a member of the firm's Real Estate group. Her practice covers housing law, civil rights, and labor and employment discrimination. Diane provides strategic counsel to corporate owners and real estate employers, designing tailored compliance training programs on workplace investigations, implicit bias, and diversity, equity, and inclusion initiatives. She also advises clients regarding human resources documentation crucial for employer compliance, including employment applications, disciplinary procedures, and employee handbooks. Diane conducts in-house sensitivity and handbook training sessions to cultivate respectful organizational cultures and preempt harassment litigation. Her proactive approach addresses post-COVID-19 employment law challenges, offering specialized guidance to brokerage, property management, and investment firms on ADA compliance, workforce restructuring, and transactional support. Diane is a trusted legal advisor skilled in navigating the complex regulatory landscape for real estate employers, ensuring compliance and resilience in today's evolving environment.

DAMON SILVER is a principal in the New York City office of Jackson Lewis P.C. He is a Certified Information Privacy Professional (CIPP/US) and strategically advises clients across various industries on privacy, data, and cybersecurity matters, including compliance with data privacy and security frameworks like the CCPA, HIPAA, and FERPA; responding to data breaches; and vetting new technologies (e.g., generative AI, digital marketing, and electronic monitoring tools) and vendors.

JOHN SNYDER is a principal in the New York City office of Jackson Lewis P.C. and co-leader of the firm's Real Estate industry group. He has extensive experience litigating state and federal discrimination, retaliation, commission and wage and hour, contract, restrictive covenant, executive compensation, and whistleblower claims. John handles litigation related to federal, state, and local fair housing issues, as well as employment contracts, executive compensation, and non-competition matters nationwide. He also advises clients on employee hiring and departures and drafts restrictive covenants, employment, and executive compensation agreements.

MELISSA PASCUALINI is an associate in the Long Island office of Jackson Lewis P.C. Her practice focuses on representing employers in workplace law matters, including preventive advice and counseling. As a member of the firm's Privacy, Data, and Cybersecurity group, she advises national and regional companies on emerging privacy and cybersecurity issues, including data breaches, mandates, and preventative safeguards. She also regularly advises clients on compliance with the myriad of federal, state, and local employment laws, including the FMLA, FLSA, state/local wage and hour, sick leave laws, and related requirements, and assists with the development and implementation of effective employment policies, handbooks, procedures, and contracts.

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

Website tracking technologies provide many valuable insights to real estate businesses. However, the carefree use of such tools has passed. Although the United States does not have a specific federal law regulating the use of data tracking, hundreds of

lawsuits were filed over the past few years alleging that the use of various website tracking technologies violates wiretap and video privacy laws and constitutes a tortious invasion of privacy. Website tracking technologies also have garnered regulatory attention, in particular, from the Federal Trade Commission (FTC) and the Department of Health and Human Services, each of which has issued guidance on the privacy concerns presented by these technologies. By managing these technologies in careful compliance with fast-evolving law, real estate businesses can lower the risk of lawsuits and regulatory attention associated with their use of website tracking technologies.

KEY LEGAL CLAIMS

Most websites today use a variety of technologies to monitor, analyze, and respond to users' on-site activities. For instance, they can track how long users spend on each page, what they click on, which videos they view, and what they say in communications with chatbots. Website tracking provides benefits to users, such as showing them content of potential interest or remembering what they put in their shopping carts. On the other hand, the use of these technologies makes some people uncomfortable, for instance when the apartment they viewed on one website starts appearing in ads on unrelated sites all over the web.

Two types of tracking activities have driven much of the litigation and enforcement activity so far: (i) allowing third parties to collect or access information about visitors' website activity for use in sending targeted ads; and (ii) allowing third parties to access visitors' communications with chatbots. On the basis of these activities, among others, plaintiffs have asserted a number of privacy-related claims, including:

Wiretap Violations

The Electronic Communications Privacy Act was passed in 1986 and updated the Wiretap Act to protect the interception, use, or disclosure of oral, wire, and electronic communications.[1] Wiretap laws may be triggered if communications with chatbots or other features of a website (e.g., web forms and search bars) are "intercepted" by third parties without consent. Under the federal Wiretap Act, damages can be up to the greater of $100 a day or $10,000 per violation. Comparable state laws also exist, which can add to the damages. For example, violations of California's wiretap law, the California Invasion of Privacy Act,[2] can result in damages of up to $5,000 per violation.

Invasion of Privacy

Those interceptions, along with the tracking of other website activity, can also form the basis for invasion of privacy claims—particularly if the visitors' interactions with the site reveal arguably sensitive information (e.g., about the visitors' medical condition, sexual orientation, or religious or political affiliations).

Breach of Contract or Violation of the FTC Act

If the tracking activity on a site is inconsistent with the disclosures in the site's privacy policy or terms of use, that inconsistency can result in breach of contract claims or violations of the FTC Act's prohibition on "unfair or deceptive acts or practices."[3]

Video Privacy Protection Act violations

Disclosing visitors' interactions with video content, without valid consent, may violate the Video Privacy Protection Act (VPPA).[4] The VPPA was passed in 1988 to protect consumer data from being shared by video rental companies. In recent years, plaintiffs have alleged that the VPPA also covers website tracking technologies. The VPPA provides for statutory damages, as well as attorneys' fees. The per-violation cap is $2,500 under the VPPA.

KEY LITIGATION ISSUES

Though claims based on the use of website tracking technologies are still novel, the emerging body of caselaw is beginning to illuminate the key issues on which these cases turn. One key issue is whether the site owner can establish that the site visitor provided informed consent to the collection of the

visitor's personal information by the site's tracking technologies. Whether that consent was timely and informed are frequent sources of dispute.

With respect to timing, a federal appellate court in 2022 held that site owners must collect consent *before* tracking visitors' activities.[5] Accordingly, a consent defense might not be viable to site owners that rely on disclosures in the privacy policy they link to at 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, and analysis of the current caselaw suggests that courts may undertake a fact-intensive inquiry. For instance, courts may look at whether the site owner's privacy policy or terms of use describe the tracking technologies used on the site in sufficient detail and using sufficiently straightforward language to enable a visitor to understand what information of theirs will be collected when they visit the site and whether that information will be disclosed to outside parties. Courts may also assess the degree to which the tracking technologies used on a site align with the reasonable expectations of a site visitor. The use of tracking technologies to facilitate the site owner's internal assessment of how its site is functioning, and in what content visitors seem most interested, would likely be viewed as aligning with the reasonable expectations of a site visitor. By contrast, if the site owner is permitting third parties to track activity on its site, which the third party then uses for its own commercial purposes, that tracking activity is likely to be viewed as unaligned with a site visitor's reasonable expectations, thereby increasing the risk to the site owner if it does not clearly disclose that activity to site visitors and collect their advance consent. Erring on the side of detailed disclosure (e.g., with respect to the categories of tracking technologies used, personal information collected, and third parties with access to that information) is the safer approach.

Another key issue is whether there was an "interception" sufficient to establish a wiretap violation. Courts have grappled with questions related to what constitutes an "interception," including whether a third party's non-simultaneous access to a site visitor's communication suffices, as well as what level of detail site visitors must allege in their complaints to adequately plead that the site owner permitted the interception of their personal information. In a 2024 California case, for example, the court held the plaintiff needed to plead facts sufficient to show the communication was, in fact, *in transit* when it was allegedly accessed by the third-party, rather than being accessed by that party *after* it arrived at its destination.[6]

A significant issue that has arisen with respect to VPPA claims is whether the site owner is a "video tape service provider" and therefore subject to the VPPA's restrictions. Site owners have disputed their status as video tape service providers" on the grounds that they are not engaged in the business of delivering video content. What it means to be engaged in that business has grown murky as organizations increasingly integrate video content into their product and service offerings or use such content to bolster their brands. In another 2024 California case, the court found that for the VPPA to apply, the delivery of video content must be central to the defendant's business or product.[7] Use of video content solely for marketing purposes, the court held, rather than "as part of a particular field of endeavor," is an indication the site owner is not "centered, tailored or focused around providing and delivering audiovisual content."[8] Granting the site owner's motion to dismiss, the court was swayed by the fact the video at issue featured a human-interest story, with footage of the site owner's employees, rather than featuring goods or products offered by the site owner.

Courts also have entertained arguments that site visitors' VPPA claims fail because the goods or services they purchased, rented, or subscribed to from the site owner were not audiovisual goods or services and, accordingly, the site visitors were not VPPA "consumers." In a recent New York case, for example, the court granted the site owner's motion to dismiss on the grounds that the site visitor, a subscriber to the defendant's newsletter, did not, through that

subscription, gain access to audiovisual content that was inaccessible to non-subscribers.[9]

MITIGATION STRATEGIES

Zooming Out

Real estate businesses may benefit from zooming out and looking at website risk broadly. Currently, over 15 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), for 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;
- 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); and
- Maintain programs to ensure their use and retention of personal information is narrowly tailored to the purposes for which they collected that information.[10]

The CCPA also requires covered organizations to scrutinize how they use and how long they retain personal information and imposes cybersecurity audit obligations.

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 a mitigation plan will vary depending on the business's operations and activities. Some key elements include:

- Mitigating class action litigation risk by eliminating unnecessary use of trackers, determining whether trackers grant third parties real-time access to site activity, 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, developing processes to timely and properly respond to requests from data subjects, and complying with data minimization mandates.
- Reviewing data security risk assessments, policies, and procedures to ensure data collected by website tracking technologies is adequately addressed and protected.

CONCLUSION

Website tracking technologies provide many valuable insights to real estate businesses. However, the days of carefree use of such tools has passed. Although US law was slower than that of the European Union and other jurisdictions to regulate the use of trackers, and this area was not, for a long time, a focus of the plaintiffs' bar, that has changed rapidly the past few years, with litigation and regulatory enforcement likely to further ramp up in years to come. Real estate businesses need to prepare accordingly.

Notes

1 18 U.S.C. § 2510 et seq.

2 Cal. Pen. Code § 630 et seq.

3 15 U.S.C. §§ 41-58.

4 18 U.S.C. § 2710.

5 Popa v. Harriet Carter Gifts, Inc., 45 F.4th 687 (3d Cir. 2022).

6 Esparza v. Kohl's, Inc., 23-cv-01988-AJB-KSC (S.D. Cal. Mar. 18, 2024).

7 Hernandez v. The Container Store, Inc., 2:23-cv-05067, 2024 WL 72657 (C.D. Cal. Jan. 3, 2024).

8 Id. at *2.

9 Lamb v. Forbes Media LLC, 2023 WL 6318033, *13 (S.D.N.Y. Sept. 28, 2023).

10 Cal. Civ. Code §§ 1798.100.