ALM | LAW.COM

The Legal Intelligencer

Website AdTech Litigation: The Latest Trend in Privacy Class Actions

By Jenn Hatcher, Al Saikali and Avery Epstein
August 23, 2023

Hundreds of class actions have been filed in the last six months against companies using certain advertising technology (adtech) in their websites. In-house counsel for companies in all industries need to understand website adtech, the legal risks, and how to mitigate those risks.

What Is Website Adtech?

Website adtech comes in various forms, such as session replay technology, chat bots, and the focus of this article—pixels, tags, and web beacons. Companies use these technologies to understand how users interact with their websites and to target/re-target those consumers (and others like them) on third-party platforms like social media. In fact, an estimated 22.5 million companies (and over 60% of websites) use website adtech. The most widely used of these are Google Analytics and Meta Pixel (formerly the Facebook Pixel).

What Is a Marketing Pixel? And a Cookie?

A marketing pixel is code embedded into a website that identifies third-party cookies in a visitor's browser to capture and share information about the visitor's website interactions. The pixel is used to collectively track website traffic, website conversions, and website visitor behavior.

Marketing pixels work with third-party cookies (small pieces of text code stored on a user's browser). Cookies store user information that can be read later by a website to perform a specific function; they allow you to save your login information, see items you previously left in your shopping cart, etc. Once a cookie is stored on your browser, it works with a pixel to read the data in the cookie and add more information to it. Pixels can identify the existence of certain cookies in a visitor's browser, resulting in the browser sharing information about the user's visit with third-party platforms such as social media sites. The visitors can then be targeted with advertisements when they visit those third-party platforms.

Class Actions Based on Website AdTech

A recent tidal wave of class actions target companies utilizing website adtech. The lawsuits seek to contort old laws to create a necessary, but missing, element of their common-law claims—damages.

- **Wiretap Lawsuits**

The largest category of these lawsuits is alleged violations of state and federal wiretap laws. (Plaintiffs also include garden-variety common-law claims such as invasion of privacy, breach of contract, negligence, and unjust enrichment—all of which are fatally missing any allegation of cognizable harm.) Plaintiffs argue that the undisclosed sharing of their website interactions with third-party social media platforms is a surreptitious recording of their online activity. Setting aside the lack of any real harm, the plaintiffs attempt to creatively skirt around two important facts. First, their browsers are responsible for sharing their website history with third parties. Second, the way this technology works is typically disclosed by the third party that installed the cookie in the plaintiff's browser, so there is nothing "surreptitious" about what is happening.

Courtesy photos

L-R: Jenn O. Hatcher, Avery Epstein, and Alfred J. Saikali of Shook, Hardy & Bacon.

A subset of wiretap lawsuits against health care providers came about as a result of a flurry of activity in 2022. In January 2022, Mass General Brigham settled a pixel class action for $18.4 million. That June, consumer watchdog organization The Markup published a series of articles investigating the health care industry's use of adtech on their websites. The investigation found that 33 of Newsweek's top 100 hospitals used Meta Pixel on their public-facing websites. Just one month later, plaintiffs filed two class actions against Meta in the N.D. of California: one involving the University of California-San Francisco, and one involving the MedStar Health System. Lawsuits continued to be filed, and then, in December 2022, the U.S. Department of Health and Human

Services' Office of Civil Rights published guidance on the "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," adding fuel to the fire and bolstering plaintiffs' confidence in their claims.

The majority of recently filed pixel litigation against health care providers is in the early pleading stages. However, one recent decision, *Kurowski v. Rush System for Health*, Case No. 22-cv-5380 (N.D. Ill. March 2, 2023), granted a motion to dismiss the majority of claims, and importantly noted that "the HHS guidance … is not controlling and only applies prospectively," and stated that if any interception occurred at all, it was carried out by third parties. Additionally, a Baltimore County, Maryland, court recently denied class certification in *Doe v. Medstar Health,* Case No. 24-C-20-000591 (Md. Cir. Ct. Mar. 10, 2023), finding the class overly broad where the proposed class included plaintiffs who accessed MedStar's Patient Portal profile and separately plaintiffs who accessed MedStar's publicly accessible website. While it is unclear whether the Rush decision is signaling the direction the courts will take more broadly, plaintiffs and defendants both eagerly await substantive rulings that are anticipated in the fourth quarter. Hundreds of website adtech wiretap lawsuits have been filed nationwide, and hundreds more have been threatened but not (yet) filed.

- **VPPA Lawsuits**

Another category of website adtech lawsuits relies on the Video Privacy Protection Act (VPPA), 18 U.S.C. Section 2710, et seq., a federal law enacted in the era of brick-and-mortar video-rental stores to prohibit videotape service providers from disclosing an individual's video-watching history with third parties. Although the VPPA was passed in 1998, hundreds of companies with websites embedded with videos have been hit with lawsuits in the last year. VPPA lawsuits target companies that embed pixels in videos on their websites, thereby allegedly resulting in the sharing of video-watching behavior on those sites with third parties. Under the VPPA, "video tape service providers" are prohibited from knowingly providing a "consumer's" personally identifiable information to a third party without consent. The plaintiffs seek to impose potentially catastrophic statutory damages of $2,500 per violation (which they interpret as "per website visit").

While some VPPA lawsuits have survived the pleading stage, recent decisions signal a change. For instance, in *Martin v. Meredith,* No. 1:22-cv-04776-DLC (S.D.N.Y. Feb. 17, 2023), the court dismissed a VPPA claim, noting that the only disclosures were of a website visitor's Facebook ID and the name of the webpage the user visited—not the name of the video watched as required under the VPPA. Even more recently, on May 24, 2023, the Northern District of California dismissed a VPPA claim against Healthline, finding that the plaintiff was not a "consumer" within the VPPA because she was not a "renter" or "purchaser" of Healthline's goods or services, even where she alleged she subscribed to Healthline's email list. *Jefferson v. Healthline Media,* No. 3:22-cv-05059 (N.D. Cal. May 24, 2023). These recent decisions may establish the foundation for early dismissal of VPPA claims where plaintiffs do nothing more than access a website and watch a video.

What's Next?

As if this wave is not enough, a new one is on the horizon. The plaintiffs' bar is starting to focus its efforts on cookie compliance—where a website visitor declines third-party cookies when visiting a website but the website nevertheless sends them to the individual's browser. The claims seek statutory damages based on alleged violations of state consumer-protection laws that prohibit deceptive and unfair trade practices.

How to Continue Using Adtech While Mitigating the Legal Risks

Fortunately, companies can mitigate most website adtech litigation risks by considering these steps:

- *Understand what adtech is being used on your website(s) and what information you share with third parties.* One way to do this is through the (privileged) engagement of third-party website assessment firms that are in the business of doing exactly that. They also help implement privacy controls and can be an important player in the conversation between legal, information technology and marketing departments.
- *Disclose the use of website adtech.* Express, prior consent is key. It is important that you work with experienced privacy counsel because a "cut-and-paste" approach is dangerous with respect to website adtech that is customized to your environment and marketing needs. You may need to consider a pop-up banner (similar to, or within, a traditional cookie banner) as some courts have rejected the use of privacy policies linked at the bottom of a website as sufficient to meet notice/consent requirements. If your company uses a chat functionality, it may need to consider linking to the more fulsome disclosures in the "chat box" that pops open to begin the conversation. It will also be a good time to test whether your cookie disclosure avoids the "next wave" risk identified above.
- *Review agreements with third parties responsible for maintaining your website adtech.* Do they contain sufficient protection if your company is sued because of your website developer's work? HIPAA-covered entities using website adtech should also consider exploring the need for a business-associate agreement depending on where and how the adtech is used.
- *Establish a quarterly conversation between legal, marketing, IT, and other stakeholders, at the direction of counsel, to ensure your organization is apprised on the latest privacy risks associated with new technologies.* This has the added benefit of ensuring that your privacy counsel understands your business goals, technology, industry, and risk tolerance.

These forward-looking solutions may not eliminate the risk of a claim, but they should ensure your organization is not the "slowest gazelle."

Al Saikali *is chair of the Shook, Hardy & Bacon's privacy and data security practice group.* **Jenn Hatcher** *is an associate practicing in privacy and data security and class action litigation.* **Avery Epstein** *is a summer associate and student at the University of Iowa College of Law.*