MAY 2023

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Website Adtech: What Every In-House Lawyer Must Know (Now!)

The biggest data privacy litigation risk companies currently face is class action litigation based on the use of certain website advertising technology (adtech). Are you wondering what this means for your company? This alert explains the underlying technology, the tsunami of litigation sweeping the country, and provides steps to mitigate these risk.

The Technology

Online advertising is an essential way for most companies target and grow their customer base. Website adtech helps to do this by helping companies understand how users interact with their website and connecting with them on other platforms. Examples of commonly-used adtech include:

- *Session replay technology* — code on a website that allows companies to understand how a visitor interacts with the website – the most popular areas on a site, information on conversion, and whether website errors are impacting performance.

- *Chat bots* — the "Talk to an Agent" feature we typically encounter, often in the bottom corner of a website. It allows visitors to "chat" with a live agent or receive automated responses to common questions.

- *Pixels, tags, or web beacons* — website code that identifies the existence of certain third-party cookies in a visitor's browser that results in the browser sharing information about the visit with third party platforms like social media. The visitors (and others like them) can then be targeted with advertisements

SUBSCRIBE

ARCHIVE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

when they visit those third party platforms.

What Are The Legal Risks?

A tidal wave of lawsuits are now targeting companies that use this website adtech. The lawsuits seek to contort the intent of old laws (like wiretap statutes) and apply them to modern technology in an attempt to create a necessary, but missing, element of their common-law claims — damages.

Wiretap Claims

The plaintiffs in these class actions contend that the use of website adtech violates wiretap laws, which prohibit the surreptitious interception of the content of communications. These lawsuits are often filed in jurisdictions with two-party consent laws. The laws create private rights of action and often offer statutory damages, which the plaintiffs believe entitle them to thousands of dollars per website visit per person per instance. In other words, the lawsuits are potentially crippling.

In 2021, a wave of approximately 50 such lawsuits targeted companies in Florida that used session replay technology. The plaintiffs used a shotgun approach to file throughout the state in an attempt to create favorable precedent that could be leveraged into a much larger wave of lawsuits. That attempt backfired. Instead, thanks in large part to Shook's Privacy Litigation Team, courts dismissed the lawsuits, reasoning: (1) the information being intercepted was not "content"; (2) the interception was not always surreptitious; (3) commercial website visitors had no reasonable expectation of privacy while on the website; and (4) a Florida-specific business exception to the wiretap law prevented the claims from proceeding. Plaintiffs attempted to pivot to allegations that chat-bot technology, not session replay, was the real problem—but the courts rejected that strategy too. Shortly thereafter, the plaintiffs voluntary dismissed most of the remaining lawsuits.

After two unfortunate decisions in 2022, however, the fury of lawsuits has begun again. In *Javier v. Assurance IQ, LLC* (9th Cir. May 2022) and *Popa v. Harriet Carter Gifts* (3d Cir. Aug 2022), the Courts allowed wiretap allegations to proceed against companies that used undisclosed session replay technology. It is now typical for two or three of these lawsuits to be filed *every day* in states with two-party consent requirements.

Pixel Litigation

Meanwhile, a second wave of lawsuits was developing against companies that use pixel technology on their websites. The

Jenn Hatcher
Associate
816.559.0306
jhatcher@shb.com

Anna Gadberry
Associate
816.474.6550
agadberry@shb.com

lawsuits came about as a result of a series of articles published by a consumer watch dog organization in the summer of 2022.

One category of these novel lawsuits relies primarily on the same wiretap laws used in the session replay litigation. The plaintiffs argue that the undisclosed sharing of their 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 the fact that *their browsers* are responsible for sharing their website history with third parties, and the way this technology works is typically disclosed by the third-party who installed the cookie in the plaintiff's browser.

A second category of pixel lawsuits relies on the Video Privacy Protection Act (VPPA), a federal law enacted in the era of brick-and-mortar video rental stores to prohibit video tape service providers from disclosing an individual's video-watching history with third parties. VPPA lawsuits target companies that embed pixels in videos on their websites. The plaintiffs allege the pixels result in the illegal sharing of identifiable consumers' video viewing history with third-party social media platforms. The lawsuits typically fail to recognize that the information shared with third parties typically does not identify any actual viewing activity. Nevertheless, the plaintiffs seek to impose potentially catastrophic statutory damages of $2,500 per violation (which they interpret as "per website visit").

The risk has increased as a result of mixed court decisions, some of which have allowed these lawsuits to proceed. *See, e.g., Lebakken v. WebMD* (N.D. Ga. Nov. 2022); *Ambrose v. Boston Globe Media Partners* (D. Mass. Sep. 2022); *but see Kurowski v. Rush Sys. for Health*, 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023); *Doe v. Medstar*, Case No. 24-C-20-000591 (Mar. 10, 2023) (Cir. Ct. Baltimore). Adding further fuel to the fire are an $18 million settlement in one of these lawsuits and an HHS Office for Civil Rights Guidance that warned covered entities on the use of certain website adtech. As a result, over 200 such class action lawsuits have been filed nationwide, hundreds more have been threatened but not (yet) filed, and the trend does not appear to be slowing down.

The Next Wave

As if this wave of litigation is not enough, a new one is on the horizon. It will target companies whose website adtech does not behave consistently with the visitor's privacy choices. For example, a company's cookie banner may appear to give the visitor an opportunity to decline the installation of any cookies, but (often unbeknownst to the website owner) the website

nevertheless uploads cookies to the visitor's browser. Consumers are increasingly incorporating privacy controls into their browsers, and the signals websites receive from visits by these can be incredibly challenging to identify and comply with. The plaintiffs' bar will be opportunistically quick to allege that this challenge is a violation of consumer protection laws that prohibit deceptive and unfair conduct.

Mitigation Techniques

Fortunately, there are steps companies can take to mitigate the website adtech litigation risk.

1. **Understand what adtech is being used** on their website(s) and what information it shared with third parties. One of the best ways to do this is through the (privileged) engagement of third-party website assessment firms who will identify existing technology, explain what information is being shared with third parties, and help you implement appropriate privacy settings.

2. **Disclose the use of website adtech** at the direction of experienced privacy counsel. It is important that you work with counsel because a "cut-and-paste" approach is dangerous. You will want to tailor the disclosure language, which may be different depending on pixel placement. You may need to consider a pop-up banner (similar to, or within, a traditional cookie banner). You may need to link to a more fulsome online privacy notice and terms of use, which counsel will also need to draft. 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 earlier.

3. **Review agreements** with third parties. These may be agreements with companies responsible for maintaining your website adtech. Do they contain sufficient protection if your company is sued because of your website developer's work? Covered entities using pixel technology may also need to explore the need for a business associate agreement in light of recent OCR guidance.

4. **Explore privacy settings** in the website adtech. You may be able to limit or mask information shared with third-party platforms.

These forward-looking solutions may not eliminate the risk of claims based on earlier uses of the website adtech but they will help you avoid being the "slowest gazelle."

One final piece of advice: **schedule a standing quarterly meeting** between your company's Legal, Marketing, IT/Website

Development, and Compliance functions. Ideally, the meeting should be moderated by privacy counsel (under privilege) who can talk about these trends/risks and how to mitigate them.

If you have questions, are facing a potential lawsuit, or need someone to help ensure your company is in compliance with the most current recommendations and regulations, Shook's Privacy & Data Security team stands ready to assist.