Articles + Publications | December 7, 2023

Beware Common Website Technology Tools That Can Lead to Wiretap Claims

Privacy & Cybersecurity Newsletter

WRITTEN BY

Tara L. Trifon | Thomas J. Cunningham

RELATED OFFICES

Hartford | West Palm Beach

Knowing how consumers behave while on a website can provide businesses with valuable information. Frequently businesses employ “session replay” tools to analyze what users do on their website. “Session replay” is software embedded in a website that allows companies to improve the effectiveness of a website. Use of this technology has been challenged in a number of class action lawsuits filed over the past few years. Another group of lawsuits allege that some companies are unlawfully embedding code in their chat features that allows a third-party service provider to create and retain a real time transcript of chats with consumers.

Plaintiffs claim these technologies violate state privacy laws, including wiretap statutes. The lawsuits are typically filed in states that prohibit the recording of a communication without the consent of all parties, so-called two party consent states such as California, Florida, and Pennsylvania. The plaintiffs allege that monitoring or recording website users’ activity or chats on a website without notice to and consent from the consumer violates wiretap statutes.

Generally, plaintiffs claim that the session replay and/or chatbot tools collect and send information about a user’s interaction with a web page, such as keystrokes and mouse movements. However, they also claim that these tools give third parties access to certain information outside of the browser, like IP addresses, geolocation, other websites the user may have visited, the time of use, and the type of computer. This may include information that the user voluntarily inputs, including terms input into a search engine or chatbot conversation. Plaintiffs have likened session replay and chatbots to permitting the third-party service provider to look over the website user’s shoulder.

Because use of these tools is widespread, litigation challenging their use has been significant. While plaintiffs typically target larger businesses, a material portion of the litigation challenging these tools has been directed at smaller and medium-sized businesses.

Defendants have asserted several defenses to these claims, with varying degrees of success. First, courts disagree as to whether the collected information actually constitutes the content of a communication, which is a necessary element of wiretap claim. Some courts hold that such information is non-communicative, comparing the keystrokes and clicks to in-person movements in a store that is recorded by video camera. *See Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318 (S.D. Fla. 2021). But other courts have held that these recordings

could be “content of a communication” because it reveals what the user intended, such as personal interest, browsing history, and habits. *See Alhadeff v. Experian Info. Sols., Inc.*, 541 F. Supp. 3d 1041 (C.D. Cal. 2021). If a court determines that the collected information does not constitute a communication, there is no viable wiretap claim.

Second, consent is an important defense for the defendants in these cases. A wiretap claim can be defeated if the plaintiff knew that the defendant was monitoring or recording activity on a website and agreed to that monitoring or recording. Website users’ consent to the terms and conditions of websites can take several different forms, generally referred to as “wrap” agreements. Courts focus on the type of wrap agreement a website utilizes to determine its effectiveness, commonly finding that scroll wrap or clickwrap agreements offer the most notice and best evidence of assent by the user. These type of wrap agreements are generally enforced (provided that the scope of the agreement encompasses the relevant software technologies and third parties). Conversely, browse wrap agreements are typically only upheld when there is evidence that the website user had actual knowledge of the terms. Sign-in-wraps could fall in either the clickwrap or browse wrap category, depending on whether the website user actually signed up or looked at the relevant policy/terms, and is therefore subject to a case-by-case analysis. Ultimately, though, a wiretap claim may be defeated if the defendant can establish that the plaintiff continued using the website after receiving adequate notice of the session replay and/or chatbot tools.

Third, a company may be able to obtain dismissal of a wiretap claim by demonstrating that the embedded code only gave the company the ability to analyze their own data and no third-party service provider could intercept and use the data itself. Courts have considered this to be a tool utilized by the company. *See Licea v. Am. Eagle Outfitters,* Inc., 2023 WL 2469630, at *8 (C.D. Cal. Mar. 7, 2023). *See also*, *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 832 (N.D. Cal. 2021). Conversely, courts have held that there is a viable wiretap claim when a third-party embeds code that the third-party then uses to aggregate data for resale (typically by de-anonymizing it and matching it with other databases). *See Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019). *See also*, *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 607 (9th Cir. 2020), *cert. denied*, No. 20-727, ––– U.S. ––––, 141 S.Ct. 1684, 209 L.Ed.2d 464 (U.S. Mar. 22, 2021). Thus, the viability of this defense depends on the exact relationship that a defendant has with its marketing analytics vendors.

The vast majority of websites employ some form of these marketing analytic tools – whether session replay or chatbot applications. Given the sheer number of entities that could be the target of such wiretap claims, it is hardly surprising that lawsuits challenging them are being filed daily. Until the courts consistently find that use of session replay and chatbot tools is not wiretapping, it is important for companies to understand how they may be impacted by this class action trend. We therefore recommend reviewing vendor agreements to confirm what information is collected and what the vendor does with that information. Perhaps more importantly, companies should ensure that their website users receive appropriate notice and provide adequate consent for the use of session replay and chatbot tools, preferably through a banner or other such prominent notice.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber