The Computer & Internet Lawyer

Volume 41 ▲ Number 9 ▲ October 2024

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

State of Play in Website and Privacy Litigation

By Eva Yang and Jeffrey Margulies

These past two years have seen an influx of litigation claiming that commonly used tracking technologies and web analytics on websites give rise to potential liability under various state and federal laws.

Creative plaintiffs' lawyers have used not only consumer protection statutes, but pre-existing 20th century statutes concerning wiretapping, pen registers, trap-and-trace devices and video protection laws to bolster their claims for damages. As courts grapple with the viability of applying these claims to new technologies, inconsistent rulings have only further emboldened plaintiffs to file more cases. And to the extent there is consistency in dismissals, the ever-changing internet era has made it easier than ever for plaintiffs' lawyers to simply move onto the next technology that gives rise to such claims.

SESSION REPLAY LITIGATION

There has been a resurgence of lawsuits over the use of session replay software, which recreates a user's interaction with a website or mobile application. By recreating a user's interaction on a website, such as mouse clicks, keystrokes and scrolling, companies can improve and analyze user website experiences. As session replay software is generally provided by third party vendors, plaintiffs have used various state wiretapping statutes, such as the California Invasion of Privacy Act (CIPA), to allege that the use of the session replay software constitutes an illegal and unauthorized wiretapping that is the equivalent of an unlawful "interception" of the website user's communication with the website by the third party.

Defendants have fought back using a variety of defenses on motions to dismiss, which typically include:

1. The "party exemption," as only a third party can be liable for wiretapping a conversation;

2. Lack of standing, given that there is no concrete injury if personal information is not captured by the session replay technology;

3. There is consent for the purported wiretapping; and/or

4. There is no "content" at issue as required by the relevant wiretapping laws.

Lower courts have issued inconsistent rulings, with some allowing these claims to proceed while others tossing them out.[1]

The authors, attorneys with Norton Rose Fulbright US LLP, may be contacted at eva.yang@nortonrosefulbright.com and jeff.margulies@nortonrosefulbright.com, respectively.

Nonetheless, these defenses have continued to be relevant in wiretapping claims as applied to other technologies discussed below.

CHATBOTS

In the summer of 2022, plaintiffs' lawyers began flooding the courtroom with complaints over the use of chatbots on websites. Plaintiffs claimed that chatbots were simultaneously recording and storing conversations with customers who were unaware that their communications were being surreptitiously intercepted by third party chatbot providers. These claims have generally not fared well in light of the party exemption defense. Numerous courts found that chatbots are akin to a tape recorder, i.e. acting as party to the communication, as opposed to a third party interceptor that independently uses the information for its own benefit.[2]

Since these decisions, chatbot cases have slowed down with plaintiffs moving onto the next hot button tech.

TRACKING PIXELS

Litigation over the use of tracking pixels has been especially pervasive. Tracking pixels are snippets of code embedded on a website that collects data about visitors to a website for purposes of online marketing and web analysis. Not only are plaintiffs asserting violations of wiretapping laws, but depending on the website and services offered, plaintiffs are asserting a variety of other common law or statutory claims based on privacy concerns in light of the disclosure of such data to third party providers of the pixel tool.

For example, plaintiffs used the Video Protection Privacy Act (VPPA) to bring lawsuits arising from websites that play videos. The VPPA prohibits the knowing disclosure of personally identifiable information of a "consumer" by a "video tape service provider." "Consumer" is "any renter, purchaser, or subscriber of goods or services from a videotape service provider." "Video tape service provider" (VTSP) is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio-visual materials."

From 2012 to 2017, plaintiffs primarily brought suit against video-streaming websites and applications. Fast forward to 2023, plaintiffs began flooding the courthouse filing lawsuits against any business with a website that displayed videos, claiming that pixels were disclosing the viewer's personally identifiable information. After a series of decisions in motions to dismiss in favor of defendants, VPPA claims eventually slowed.

But wiretapping or other privacy related claims arising from the use of pixels continued to churn. Although most of these claims can be settled quickly and cheaply, some have taken a different form. For example, health care providers, which are obligated to comply with the Health Insurance Portability and Accountability Act, have been hit with a swath of class actions based on pixel tools. Plaintiffs have relied on the U.S. Department of Health and Human Services December 2022 bulletin, revised in March 2023, during which the Office of Civil Rights cautioned that "individually identifiable health information" may consist of an individual's IP address with a visit to a website addressing specific health conditions or health care providers, to argue that the use of pixels and subsequent disclosure to the pixel provider constitutes a violation of HIPAA.

Notably, on June 20, 2024, a Texas district court judge vacated the HHS bulletin's description of the combination of an individual's IP address and a website visit addressing specific health conditions or providers as "individually identifiable health information."[3] It is currently unclear whether this will slow or deter pixel litigation against healthcare providers, but at least for now, the decision removes one critical piece of arsenal for the plaintiff's bar.

COOKIES AND OPT-OUT

Plaintiffs have also pursued a kitchen-sink variety of claims alleging that websites' use of cookies illegally disclose private information to third parties. These claims have been brought against websites that use cookie banners that present users with an option to opt-out, but allegedly either transmit information before the user can opt-out, or continue to use cookies that transmit information to third parties despite the user's selection to the contrary. There is scant guidance to rely on, as many of these claims are settling pre-litigation or being arbitrated privately and are not resulting in reported court decisions. However, defending these claims require an analysis of the underlying cookie technology on the website and the relevant disclosures, which companies may typically link to other terms and conditions, such as a privacy policy.

OTHER ANALYTICAL AND TRACKING TOOLS

The newest wave of privacy related lawsuits focus on provisions of CIPA concerning pen registers and trap-and-trace devices. Plaintiffs have been recently flooding the courts with purported class actions under the novel theory that common tracking technologies that collect information regarding a person's location and personal information, are acting as illegal pen registers and trap-and-trace devices. Pen registers and trap-and-trace devices, at least historically, have been thought of

as physical devices that were used by law enforcement to record outgoing and incoming phone numbers and other signaling information.

These claims stemmed from a California district court's decision in *Greenley v. Kochava, Inc.*, [4] that held that the plaintiff had adequately alleged the software at issue – a software development kit developers could use to make apps, and through which the defendant was purportedly provided with geolocation, IP address and other information about app users – was a pen register.

Notwithstanding *Greenley*, defendants have filed early motions seeking dismissals of such cases, primarily arguing that tracking technologies and pixels do not fall within the intended definition of "pen registers" or "trap and trace" devices under CIPA. Unsurprisingly, the lower courts have been inconsistent, with at least one court sustaining a demurrer and another overruling it.[5]

As these cases continue to make their way through court, we can expect continued litigation.

TAKEAWAY

With the rapid digitization of all things on the internet and the proliferation of new technologies, one thing is for certain – plaintiffs' attorneys will continue to be creative in policing privacy rights as applied to modern ways of life. No matter the flavor of the month, there are ways to mitigate risk across all claims. At a minimum, this includes understanding and assessing the different technologies being used on websites that may collect data about users, making sure that a robust clickwrap privacy policy is in place, and complying with the terms of the privacy policy.

Notes

1. See, e.g., Saleh v. Nike, Inc., 562 F. Supp. 3d 503 (C.D. Cal. Sept. 27, 2021) (party exception did not apply to the software provider); Graham v. Noom, Inc., 533 F. Supp. 3d 823 (N.D. Cal. April 8, 2021) (party exception applied because session replay software provider was an extension of the website); Cook v. Gamestop, 2023 WL 5529772 (W.D. Penn. Aug. 28, 2023) (plaintiffs must plausibly allege the interception of personal information to demonstrate a concrete injury for standing purposes).
2. Licea v. Cinmar, LLC, No. CV 22-6454-MWF, 2023 WL 2415592 (C.D. Cal. Mar. 7, 2023); Martin v. Sephora USA Inc., 2023 WL 2717636 (E.D. Cal. Mar. 30, 2023); Licea v. Am. Eagle Outfitters, Inc., 2023 U.S. Dist. LEXIS 42549, at 21 (C.D. Cal. Mar. 7, 2023).
3. American Hospital Association v. Becerra, 2024 U.S. Dist. LEXIS 108847, at *52 (N.D. Tex. June 20, 2024).
4. Greenley v. Kochava, Inc., 2023 WL 4833466 (S.D. Cal. July 27, 2023).
5. See Licea v. Hickory Farms, LLC, No. 23STCV26148 at *# (Cal. Super. Ct. Oct. 25, 2023); Casillas v. Transition Optical, Inc., No. 23STCV30742 at *# (Cal. Super. Ct. Dec. 15, 2023).