Privacy Litigation Trend: The Latest on Session Replay Lawsuits, and Practical Considerations for Risk Mitigation

Alysa Z. Hutnik

May 21, 2021

Over the last few months, a wave of consumers have filed putative class action complaints against a long list of consumer-facing website owners/operators and their software providers alleging invasion of privacy rights under statutes focused on wiretapping and eavesdropping.

Our team has represented both website and software defendants in these cases. However, this post is not intended to reflect on any specific claim, website, or software. Rather, our goal is to provide an introduction to the general nature of the consumer claims and current landscape of these litigations.

This post summarizes (1) the "session replay" technology at issue in these claims; (2) arguments presented by the Complaints; (3) an overview of common defenses; and (4) where things stand. With that context, we then provide our list of practical considerations for the use of session replay software.

What is "Session Replay" Software?

A significant branch of the Software-as-a-Service (Saas) industry has arisen to support website owners/operators in effectively maintaining and leveraging their consumer-facing websites. These software products are generally scripts placed in the JavaScript of a given website to capture specific information related to a consumer's interactions with a given page. The software can capture consumer's keystrokes and mouse movements to provide information on everything from broken links or error messages to support IT teams, create heat maps showing website usage, and/or capture consumer information for validating consent to be contacted or agreement to receive products and services.

Despite how these products are often described, the software does not actually *record* the consumer's session in the way that a security camera in a brick-and-mortar store would capture a consumer's movements. Rather it captures the consumer's interactions with the website at regular intervals and allows those movements and data points to be laid over an existing image of the website so that owners/operators can review a recreation (or dramatization) of an individual consumer's experience.

What are the Allegations?

Generally, Plaintiffs in these cases have alleged that session replay software are improper

wiretapping and eavesdropping devices that are recording consumer communications without required consent. These cases have arisen where state law requires both parties to a communication to consent to any recording. Thus, California and Florida have become hot beds for these claims.

Both the California Information Privacy Act ("CIPA") and Florida Security of Communications Act ("FSCA") were designed to prevent improper interception of telephone calls. These statutes were crafted before the advent of the internet and focused on improper tapping into telephone lines to listen into or record conversations. Over time, the statutes have been interpreted to protect certain other forms of communication, including interception of emails or text messages in transmission. The Courts have essentially analogized those communications to the written transcript of the telephone conversation intended to be protected by the statutes.

But these new claims seek to expand the statutes further to restrict the capture of information using session replay software. The statutes are appealing targets for plaintiffs because they include statutory damages that, on a class wide basis, can escalate quickly. In California, plaintiffs have also relied upon the state's constitution, which protects citizens' right to privacy.

What are the Defenses?

There are many arguments that defendants have raised and each situation is unique; however, several trends have started to emerge as more motions to dismiss have been filed:

Consent is a complete defense to any of these claims. That can be in the form of browsewrap acceptance of a website's Privacy Policy that disclosed the use of such software. Or it could be affirmative consent to that policy and/or the site's terms of use at the time of account creation, purchase, or other information submission. The first court to weigh in on a motion to dismiss of claims based on session replay allegations leaned heavily on the consumer's affirmative consent in dismissing the claims. *Javier v. Assurance IQ, LLC et al.,* No. 4:20-cv-02860-JSW, 2021 WL 940319 (N.D. Cal. Mar. 9, 2021).

Defendants have also successfully challenged whether the information captured by session replay software is actually recording the *contents* of a communication. For example, information concerning consumer's IP address, device model, and operating system are not, themselves, the content of communications. Similarly, mouse movements and keylogging software have, in other contexts, been found to not capture the "content" of a communication.

To bring a valid statutory (or constitutional) claim, consumers must also show that the communication at issue is confidential. Plaintiffs' claims are vulnerable both because any information input to the website is direct at, and intended for, the website's owner/operator and therefore, how could the contents be considered confidential from those owners/operators? Additionally, multiple courts have found that there is no *per se* reasonable expectation of privacy for communications over the internet. One Court has also confirmed (in multiple, similarly-pled cases) that any distinction between the website owner/operator and their software provider is irrelevant; therefore, that fact pattern cannot give rise to a claim of third-party eavesdropping. *See, e.g., Graham v. Noom,* No. 20-cv-06903-LB, 2021 WL 1312765 (N.D. Cal. Apr. 8, 2021).

On a more technical level, defendants have also challenged whether the software at issue is actually *intercepting* any information while it is in transmission between two parties, as required by the statutes. To meet the elements of these particular statutes, the data cannot simply be captured from the consumer's browser or hard drive, but must be recorded while in transit. And evidence supports finding that is not how these software products operate.

Finally, as a procedural matter, where a consumer affirmatively accepts terms of use or creates an account, the defendant may have a valid claim to compel arbitration.

Where Do Things Stand?

As with any new, developing area of the law, there are lingering unknowns. Thus far, Courts have shown skepticism of Plaintiffs' claims and rejected several of the Complaints at the pleading stage. Some cases have been resolved and others abandoned following the filing of motions to dismiss or to compel arbitration. We expect that the interested parties will continue to jockey for position and litigate these issues over the next several years to flesh out a more complete body of law.

Practical Considerations for Using Session Replay Technology

As any company evaluates the use or sale of session replay products, answers to the following questions will be informative:

- What information is the software capturing about consumers or otherwise individual user-level activity?
- What consumer/user level information captured is necessary for the business purpose?
- Is the software capturing any additional consumer/user-level data that is not shared with the first-party company, but could be reviewed/used by the provider?
- How do the terms address ownership rights and permissions (and any restrictions) on the consumer/user-level data collected via the software?
- Are any potential contents of communications captured?
- What are the individual steps enabling the capture of data on the websites? Does the capture of the data occur during transmission?
- What specific individual pieces of consumer/user-level data are captured?
- How does the software avoid collecting information that we do not want to capture?
- What disclosures are we providing to consumers concerning the use of session replay software (and other similar programs)?
- How and where is the disclosure presented to the consumer?
- Regardless of whether it's required, are we obtaining consent for use of the software, and if so, how so?
- Are we complying with all contractual requirements concerning disclosures and data?
- Does our contract protect our interests should litigation arise over the software?
- Would our insurance policies cover any potential claims?

This list is not comprehensive. Each business and software is unique. If you have questions about your specific circumstance, please reach out to one of us and we would be happy to discuss these issues further.

* * *

Subscribe here to Kelley Drye's Ad Law Access blog and here for our Ad Law News and Views newsletter. Visit the Advertising and Privacy Law Resource Center for update information on key legal topics relevant to advertising and marketing, privacy, data security, and consumer product safety and labeling.

Kelley Drye attorneys and industry experts provide timely insights on legal and regulatory issues that impact your business. Our thought leaders keep you updated through advisories and articles, blogs, newsletters, podcasts and resource centers. Sign up here to receive our email communications tailored to your interests.

Follow us on LinkedIn and Twitter for the latest updates.