Hashed & Salted | A Privacy and Data Security Update
July 2025

Understanding Session Replay: Legal Risks and How to Mitigate Them

Hashed & Salted | A Privacy and Data Security Update

In an increasingly data-driven digital landscape, businesses are constantly seeking tools to better understand and optimize user experiences. One such tool is session replay—a powerful technology that allows organizations to observe how users interact with their websites or apps in real time. However, while session replay can offer significant benefits, it also introduces serious legal risks, particularly concerning user privacy. Here's what businesses need to know.

Session replay tools record real-time user interactions on a website or mobile app. These tools track mouse movements, clicks, scrolls, keystrokes and page views to create a visual log—or "replay"—of a user's journey. These tools often rely on cookies and tracking technologies to capture user behavior. However, this form of surveillance has triggered growing scrutiny under privacy laws like the California Invasion of Privacy Act (CIPA).

A spike in litigation has impacted businesses across industries. From Feb. 5, 2022, through March 25, 2025, 1,853 federal and state wiretapping and pen register/trap and trace cases were filed, with a staggering 83% of them in California. Other high-activity states include Illinois, New York and Pennsylvania.

Given the high percentage of cases in California, the focus is on CIPA, which was originally enacted to protect the privacy of communications in California and is now being interpreted to include digital interactions. Several sections of the law are relevant. Section 631(a) prohibits the unauthorized interception and recording of the content of communications during transmission. Section 632(a) requires consent from all parties to record any confidential communications. And Section 638.51 prohibits the use of pen registers (devices that record outgoing communication data like dialed numbers) and trap and trace devices (which record incoming communication data) without a court order or user consent. Violations apply not just in business-to-consumer (B2C) settings but also to business-to-business (B2B) and business-to-employee (B2E) contexts. The penalties are significant at $2,500 per violation and up to $10,000 per violation for repeat offenders. Civil lawsuits must be filed within one year of the alleged offense, and class actions are permitted.

Plaintiffs increasingly argue that the use of digital tracking technologies amounts to unlawful wiretaps or surveillance. The core allegations include (1) recording the content of confidential communications, (2) recording record information (e.g., IP addresses, geolocation) and (3) doing so without user consent or a court order.

The courts are split, and defendants have no clear exit strategy. Some courts say a vendor providing replay software is a third-party eavesdropper under Section 631(a). Others rule that the vendor is merely an extension

Attorney Advertising

of the business and does not independently "intercept" communications. Courts are also split on whether session replay tools fall under the definition of a "pen register" per Section 638.51. Some find that embedded tracking software was a "process" under CIPA's definition of a pen register. Others granted the defendant's motion to dismiss, having rejected the plaintiff's argument that the defendant used a pen register to collect IP addresses from its website. Due to the unsettled state of the law, companies face ongoing legal ambiguity.

Despite the uncertain legal terrain, businesses can take concrete steps to reduce their exposure by implementing several key practices on their websites. Consent should be obtained through a cookie consent banner that appears immediately upon a user's arrival, with no tracking technologies—such as cookies, pixels or beacons—activating until the user provides explicit, affirmative acceptance. Transparency is equally essential: Privacy policies should offer clear and specific disclosures, informing users that their interactions, including clicks, keystrokes and scrolls, may be recorded in real time. These policies should name any third-party vendors involved, explain the purposes of data collection (such as analytics or user experience improvements) and describe how the data will be used. Following the principle of data minimization, businesses should only collect the minimum amount of information necessary for their stated purposes. Additionally, masking sensitive information is critical; session replay tools must be configured to exclude or obscure sensitive data like passwords, credit card details, Social Security numbers and health information. Organizations should also establish and enforce data retention policies to define how long session recordings are stored and when they are deleted. Lastly, terms of use should be updated to strengthen legal protection, incorporating provisions such as class action waivers and mandatory arbitration clauses where legally enforceable.

Session replay tools can dramatically enhance digital experiences, but their use demands careful consideration. With privacy laws in flux and no sign of abatement in plaintiff claims, businesses must tread carefully. By focusing on consent, transparency, data minimization and legal safeguards, companies can mitigate risks while continuing to gain valuable user insights. A one-size-fits-all "exit strategy" may not exist yet, but proactive compliance remains the best defense.

Related Professional

Allison Cohen . . . . . ahcohen@loeb.com