Legal Backgrounder

Vol. 38 No. 7 April 28, 2023

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Lawsuits Accusing Online Session Replay of Criminal "Wiretapping" Implicate Serious Constitutional Concerns

by Gerard M. Stegmaier, Mark D. Quist, and Alan D. Bart

Under the guise of protecting individual privacy interests, enterprising plaintiffs' lawyers have long sought to use existing, pre-Internet laws and the specter of expensive class action discovery to squeeze nuisance value from businesses with public-facing websites. Websites owned by an array of businesses including airlines, auto manufacturers, tech companies, retailers, and other major consumer brand names that use "session replay" software have become the latest targets in this decades-old pattern. The theory of liability? In most cases, the claim is that session replay software violates state and federal wiretapping statutes and otherwise infringes consumer privacy rights. This particular litigation trend glosses over the plain meaning of criminal wiretapping statutes that were enacted to shield First Amendment-protected speech from unlawful and speech-chilling surveillance.[1] Courts' embrace of this theory of "wiretapping" would criminalize the ordinary operation of the Internet without constitutionally required fair notice to affected website operators. Further, if lawsuits under state wiretapping statutes succeed, the decisions would threaten interstate commerce by allowing states to impose unduly burdensome Internet consent standards on out-of-state website operators.

Session Replay Software Is a Commonplace Tool Used by Website Operators to Analyze How Visitors Use Their Sites

Session replay software enables a website operator to reconstruct users' visits to a site for certain purposes including to better understand how users navigate the site, learn which features are working or not working well, and build an improved user experience. A single session replay recording is not a literal video record of a user or the user's activities. Rather, it is an analytical reconstruction pieced together from the logs of a user's visit to the site—the sequence of "events" that is logged as a user's web browser visits a website and, in doing so, transfers information about that visit to the site. Captured event data may include the details of a user's mouse clicks and swipes, as well as the user's scrolling patterns, window resizes, and other site movements.

Despite the ordinary use of session replay software for anonymous analytics purposes, imaginative lawsuits from the plaintiffs' bar claim that session replay software violates users' privacy rights in one of two ways: either by recording information they claim is "sensitive" or "private" without user consent

[1] A related, but separate trend has also emerged under the 1988 federal Video Privacy Protection Act, 18 U.S.C.S. § 2710 ("VPPA"). Though the statute was enacted to prohibit "video tape service providers" from unlawfully disclosing consumers' private viewing histories to third parties, the class action plaintiffs' bar has sought to construe the VPPA to apply not only to streaming services and other modern iterations of the traditional video rental store that rent, sell, and offer subscription video content, but to virtually any commercial website that allows site visitors to view and access video content, from product advertisements to how-to videos.

Gerard M. Stegmaier is a partner, and **Mark D. Quist** and **Alan D. Bart** are associates, with Reed Smith LLP.

and transmitting that information to a third-party session replay vendor and/or by authorizing session replay vendors to directly collect data from unsuspecting users. Though the most widely used session replay tools are configured by default to mask or anonymize individual users' data, the typical putative class action lawsuit touts a list of conjectural privacy violations: from the possible capture of credit card data and social security numbers, private health information, and other sensitive data to the recording of text entries that users supposedly thought better of sending and deleted. Plaintiffs' lawyers are suing under laws that were not intended to regulate session replay technology and are being interpreted in ways that threaten to upend established, beneficial practices in the tech industry that enhance and improve user experiences.

Session Replay Software Is Not Criminal Wiretapping and the Lawsuits Implicate Serious Constitutional Considerations

These lawsuits are questionable for a number of reasons. First, generally speaking, the lawsuits fail to describe any non-anonymous, private, or sensitive information the session replay software recorded, and thus fail to show any concrete privacy injury. And from a merits perspective, state and federal wiretapping laws that were generally drafted in the 1960s and 1970s—even if they were amended to cover electronic communications in the 1980s and 1990s—were intended to protect the substantive "contents" of intentional party-to-party communications, not basic web navigation activity and public websites' automated fulfillment of visitors' informational requests.[2] The automated recording of basic website activity information does not appear to implicate the same First Amendment speech concerns that state and federal wiretapping statutes are largely designed to protect.[3]

Moreover, the wiretapping laws impose *criminal* liability for the interception of the contents of communications. Reinterpreting these criminal statutes to grant a windfall to the plaintiff's bar would have massive criminal repercussions. First, it would criminalize the conduct of millions of commercial website operators without fair notice and contrary to the rule of lenity.[4] Second, expanding the established scope of application of criminal wiretapping laws' core definitions would not only impact websites that use session replay, but would potentially over-criminalize other online activities in ways that defendants could not otherwise have reason to know or believe would be wrongful.[5] Interpreting courts must consider and avoid precisely these sorts of constitutionally unsound statutory interpretations.[6]

Courts faced with interpreting wiretapping laws should also be wary of construing state laws in ways that unduly burden interstate commerce. Such interpretations may, by effect, impose nationwide Internet privacy compliance standards far in excess of what federal law and other states' laws require.[7] If a court interpreted a state wiretapping statute to either prohibit the use of session replay software or to impose burdensome compliance requirements under pain of severe criminal and civil penalties,

---

[2] *See, e.g.*, Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. § 5701 *et seq.* ("WESCA"); Electronic Communications Privacy Act, 18 U.S.C.S. §§ 2510-2523 ("ECPA").

[3] *See Bartnicki v. Vopper*, 532 U.S. 514, 542-43 (2001) (Rehnquist, C.J., dissenting).

[4] "[T]he canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997).

[5] Criminal statutes and statutes with both criminal and civil applications must be construed strictly and uniformly, even where being interpreted in a civil context. *See Clark v. Suarez Martinez*, 543 U.S. 371, 380 (2005); *Leocal v. Ashcroft*, 543 U.S. 1, 11-12 n.8 (2004).

[6] *Clark*, 543 U.S. at 380-81.

[7] *See* U.S. Const. Art. I, Sec. 8, cl. 3; *Pike v. Bruce Church*, 397 U.S. 137, 140-42 (1970) (local and state laws that appear facially neutral may not burden interstate commerce in a way that is clearly excessive in relation to any local benefit).

that standard would *arguably* impose liability on any website accessible in-state—in other words, *any website*. While the cost of compliance with such a law would be high, any putative local benefit likely "could be promoted as well with a lesser impact on interstate activities.[8]

The Third Circuit Breathes New Life Into Session Replay Cases

Despite the statutory and constitutional objections and a generally poor record of surviving dispositive motions, the plaintiffs' bar has found some success in asserting its new theory of session replay as wiretapping. Following the Third Circuit's reinstatement of claims under WESCA in *Popa v. Harriet Carter Gifts, Inc.*,[9] what was once a trickle of session replay lawsuits generally confined to Florida, California, and to a lesser extent Pennsylvania has swollen to a nationwide torrent of new filings.

In *Popa*, the plaintiff alleged that Harriet Carter Gifts used session replay software operated by Navistone, which Popa alleged sent simultaneous communications from Popa's device to Navistone's server without first notifying Popa of Navistone's use of session replay software on the website. On summary judgment, the Western District of Pennsylvania ruled that there was no "interception" as a matter of law because Navistone was a direct recipient of Popa's communications and that, even if there had been an "interception," it occurred not in Pennsylvania where Popa resides, but instead where Navistone's servers are located in Virginia.

The Third Circuit reversed on two grounds. First, it read WESCA narrowly and found there was no direct-party exception from liability except under certain circumstances not present and having to do with law enforcement. That interpretation of WESCA contrasts with ECPA, which contains a direct-party exception from liability.[10] Second, it determined that the point of "interception" (assuming one occurred) was the location at which the user accessed the website, not the location where the data was stored.

Importantly, the Third Circuit left open critical questions regarding disclosure and actual and constructive notice, as well as jurisdictional and constitutional issues. Since the Third Circuit's ruling in *Popa*, over 100 "me too" suits have been filed nationwide, many of which are virtual facsimiles of the *Popa* complaint. Though all of them generally suffer from the same infirmities, there is substantial risk that the lawsuits may survive initial motions practice and subject companies to drawn-out class action litigation and costly settlements.

Reducing Risk: Require Affirmative Consent to Terms of Use, Including Full Disclosure Regarding Use of Session Replay Software and a Class Action Waiver

Website operators can help reduce the risk of being targeted with session replay claims in a number of ways, including: (1) obtaining affirmative consent to the site's terms of use and privacy policy prior to allowing access to the site; (2) conspicuously disclosing the site's privacy policy and taking steps to ensure that key provisions are clear and easy to understand; (3) providing detailed disclosures about analytics-related activities and site usage monitoring including the use of session replay or similar website analytics tools and related data sharing with vendors; and (4) employing class action waiver terms, arbitration and governing law provisions, which may make a website a less tempting target for an opportunistic strike suit.

---

[8] *See Pike*, 397 U.S. at 142.

[9] 45 F.4th 687 (3d. Cir. 2022).

[10] *See* ECPA, 18 U.S.C. § 2511(2)(d).

Courts can usually take judicial notice of the text of publicly available terms of use, and the ability to clearly and succinctly show a tribunal that the use of session replay software was explicitly disclosed and actually or impliedly consented to should greatly reduce the likelihood of a successful class action lawsuit.

