Massachusetts Supreme Judicial Court Rejects Use of Wiretap Statute in Data Privacy Class Action Lawsuits

Alexander (Sandy) R. Bilus, Joseph D. Lipchitz

Published 10/30/2024

Over the past decade, businesses and institutions with public-facing websites have increasingly turned to internet tracking technologies, such as cookies, pixels, and session replay tools, to optimize their websites and offer website visitors a more efficient and personalized experience, as well as monetize the data about website visits. With the rise of internet tracking came a nationwide surge in data privacy class action lawsuits. Initially, the class actions were based on common-law or statutory invasion of privacy claims, but courts frequently dismissed cases unless plaintiffs could demonstrate that the data collection and disclosure involved personally identifiable information (PII) or protected health information (PHI).

What You Need to Know:

- The SJC has limited the use of the Massachusetts Wiretap Statute in data privacy class-action lawsuits to only conduct where interpersonal communications or messages are secretly intercepted, as opposed to conduct that tracks website visits and interactions between the visitor and the website.
- Although the SJC held that the Wiretap Statute did not encompass the conduct at issue, it expressed serious concerns raised by the use of website tracking technologies and emphasized that such conduct "may indeed violate various other statutes and give rise to common-law causes of action."
- Businesses, colleges, and other institutions, particularly HIPAA-covered entities, should review their data privacy policies, procedures, and notices to limit the risk of litigation.

In response, plaintiff-side attorneys began filing federal class actions based on dual-consent

wiretap statutes, claiming that website owners and the companies that provide tracking technologies were secretly "intercepting communications" related to users' interactions—such as mouse movements, clicks, and keystrokes—entitling them to statutory damages and attorney's fees. However, following the U.S. Supreme Court's ruling in TransUnion v. Ramirez, 141 S. Ct. 2190, 2205 (2021), which determined that mere statutory violations do not confer Article III standing, federal courts began dismissing these cases unless plaintiffs could demonstrate actual injury separate and apart from the statutory violation.

Consequently, plaintiffs pivoted their privacy claims under wiretap statutes to state courts. In 2023, this shift was highlighted in a pair of consolidated cases in Massachusetts Superior Court involving plaintiff Kathleen Vita's class-action lawsuit against New England Baptist Hospital and Beth Israel Deaconess Medical Center. Ms. Vita alleged that the hospitals violated the 1968 Massachusetts wiretap statute, M.G.L. c. 272, §99, by intercepting users' online interactions with and searches on the hospitals' public websites through the use of pixels, cookies, and other internet tracking devices.

Ms. Vita alleged that she, and those similarly situated, used the websites to obtain information about doctors, symptoms, conditions, and medical procedures, and to access her medical records. As part of that interaction, she alleged that the hospitals captured her IP addresses, web browsing history, the contents of searches made on the website, and various selections made when accessing the websites using third-party tracking software which then disclosed the data to vendors. Ms. Vita did not allege that any messages to doctors or medical staff had been captured, nor did she allege that any PHI had been captured by third parties.

On October 31, 2023, Justice Hélène Kazanjian of the Superior Court's Business Litigation Session denied the hospitals' motions to dismiss, holding that a violation of the statute, alone, constitutes injury sufficient to confer standing. At the same time, she certified to the Massachusetts Supreme Judicial Court (SJC) the novel question of whether the Massachusetts wiretap statute applies to various internet tracking practices. The SJC accepted the case for direct appellate review.

On October 24, 2024, the SJC issued a 47-page decision in Vita v. New England Baptist Hosp., -- Mass. - - (2024), reversing the lower court's denial of the hospitals' motion to dismiss. As an initial matter, the SJC agreed with Justice Kazanjian that the plaintiffs had standing because the wiretap statute allows any "aggrieved person" whose communications are intercepted to pursue a private cause of action, even without showing actual damages. However, the majority ultimately ruled that the wiretap statute does not extend to the alleged internet tracking unless personal messages or conversations are secretly intercepted.

The thrust of the majority's holding is rooted in the interpretation of the term "communication," which they held does not extend to web browsing activities because the wiretap act was

enacted to criminalize the secret interception of "person-to-person conversations and messaging," particularly private ones. As a result, an individual's web browsing is not a "communication" because the interaction is person-to-website, as opposed to person-to-person. Moreover, the majority found nothing in the text of the statute which makes it unambiguously clear that the legislature intended to "reach so far as to criminalize the secret recording of such web browsing activity."

While the SJC held that the Wiretap Statute did not encompass the conduct at issue in Vita, it expressed serious concerns raised by the hospitals' alleged conduct, which it emphasized "may indeed violate various other statutes and give rise to common-law causes of action more specifically directed at the improper handling of .... confidential medical information."

The attorneys in Saul Ewing's Cybersecurity and Privacy Group are here to help your company implement effective data privacy measures, navigate compliance strategies, and defend against lawsuits in the evolving legal landscape of internet tracking practices.

Authors

Alexander (Sandy) R. Bilus
Partner
(215) 972-7177 |
View bio

Joseph D. Lipchitz
Partner
(617) 912-0916 |
View bio

Related Services

Cybersecurity & Privacy