

TYPES NOT MAPPED YET November 14, 2024 | TTR not mapped yet | Brittney K. Mollman, Luke Sosnicki, Aya Elalami

The Recent Massachusetts Court Holding in Vita is a Win for Businesses and a Look at Trends in Novel U.S. Wiretapping Litigation

The *Vita* cases

The Massachusetts Supreme Judicial Court (SJC) recently addressed whether the term “communications” in Massachusetts’ 1968 Wiretap Act (MWA) includes when a patient interacts with a hospital’s website and determined that such interactions did not qualify for protection under the statute. This is a significant decision for businesses that have been fending off a recent wave of litigation based on website-tracking technologies.

In [*Vita v. New England Baptist Hospital*](#) and *Vita v. Beth Israel Deaconess Medical Center*, Plaintiff Kathleen Vita filed two class action complaints against the named institutions alleging each of the hospitals’ websites contained tracking software—Meta Pixel and Google Analytics—that collected and transmitted information about Vita’s interactions with the websites to third parties without her consent, in violation of the MWA. Defendants filed motions to dismiss arguing that plaintiff failed to plead facts sufficient to state a claim under the MWA and, in particular, that Vita’s interactions with the defendants’ websites did not constitute “communications” under the statute. In relevant part, defendants took the position that the drafters of the MWA did not intend the definition of communication to extend to web browsing, which is substantively different than a private conversation in one’s house or on the telephone. Justice Helene Kazanjian of the Suffolk County Superior Court disagreed and denied defendants’ motions.

The SJC took up the cases on direct appellate review to address discord among the Massachusetts lower courts regarding whether an individual’s website interactions constitute “communications” under the MWA. Oral arguments took place in April 2024.

On October 24, 2024, the SJC [reversed](#) Justice Kazanjian’s dismissal, holding that the term “communication” in the MWA *does not* extend to the interception of web browsing and other similar website interactions. In particular, the majority wrote “[a]ctivities such as entering a URL, accessing a specific webpage, clicking on links, and scrolling through a webpage are clearly not the type of person-to-person conversation or messaging unambiguously protected by the act.” The majority instead held the MWA’s definition of “communication” was limited to an individual’s communications with another person (whether it be on the phone, via e-mail, text message, chat, instant message or the equivalent). “If the legislature intends for the wiretap act’s criminal and civil penalties to prohibit the tracking of a person’s browsing of, and interaction with, published information on websites, it must say so expressly.” Notably, the decision left open the door for plaintiffs looking to pursue other claims for similar conduct.

A closer look at wiretapping litigation trends

Vita is just a recent example of plaintiffs attempting to bring claims relating to the use of newer tracking technologies under decades-old state wiretapping laws. Other states that have seen an increase in wiretapping litigation include states with wiretap laws that require the consent of all parties involved in communications before recording or interception, e.g. California, Pennsylvania, Massachusetts, Washington and Florida. For purposes of this article, we’ll take a closer look at the state of novel consumer wiretapping litigation under the [California Invasion of Privacy Act](#) (CIPA), California’s 1967 state wiretapping law.

Litigants bringing claims under CIPA typically argue, not unlike plaintiffs in *Vita*, that website operators that employ modern website tracking technologies without first obtaining a website visitor’s consent violate CIPA. There have been CIPA cases alleging that website operators engage in illegal wiretapping when using the following technologies where they do not first obtain visitor consent:

- Chatboxes [monitored by a third party](#)
- Session replay software [that tracks interactions with the site \(i.e. mouse movements, clicks, scrolls and keyboard entries\)](#)
- Meta pixels that [track visitor interaction with site](#)

Many businesses have argued that plaintiffs' theories are in conflict with the California Consumer Privacy Act (CCPA), which only requires that companies provide consumers with an opportunity to *opt out* of having their personal information collected for targeted advertising, as opposed to asking consumers to *opt in* to such collection. California state and federal courts have issued mixed rulings on these issues.

In 2022, the [Ninth Circuit](#) gave some credence to plaintiffs' novel wiretapping theories. In *Javier v. Assurance IQ, LLC et. al*, plaintiffs brought a putative "session-replay" class action alleging that the use of "session-replay" software (in this case TrustedForm) constituted an illegal wiretap under CIPA because it permits the site to track website users' communications without obtaining prior consent to do so. Plaintiff in this case allegedly visited an insurance quoting website that used "session-replay" software to record a video of users' website interactions and only obtained consent to do so *after* plaintiff filed out an insurance questionnaire on the site. The Ninth Circuit addressed whether CIPA consent can be obtained after a website user has begun interacting with the site and concluded it could not. In doing so, the Court stated that CIPA extended to internet communications.

A key factor distinguishing the analysis in *Javier* from *Vita* is how the respective statutes define covered confidential communications. Under CIPA, "confidential communication" is broadly defined as "any communication" that is conducted in a way that participants intend it to be confined to the parties to the communication. On the other hand, under the MWA the legislature chose to specifically prohibit the interception of "wire communications" and "oral communications," when there is not prior consent of all parties to the communication. While it remains to be seen how defendants in other jurisdictions will attempt to leverage the *Vita* holding, it is likely they will attempt to analogize their state wiretapping statutes' definitions of communication to the more narrow MWA definitions and distinguish it from CIPA.

The MWA, CIPA and similar state statutes impose criminal and civil liability (up to \$5,000 *per statutory violation*) on anyone who "reads, or attempts to read, or to learn the contents" of a communication "without the consent of all parties to the communication." Given the uncertainty in the legal landscape, allegations against defendants under CIPA and similar state statutes expose companies to potential liability of up to millions of dollars for statutory violations.

Key Takeaways

The surge of internet-based wiretapping lawsuits is unlikely to end any time soon unless the higher courts and/or legislatures decide to weigh in. While the defendants in *Vita* ultimately prevailed, the uncertain legal landscape surrounding the use of website tracking software in other jurisdictions, and in particular California, brings significant exposure to businesses with consumer-facing websites. In states that have a wiretap law requiring the consent of all parties, businesses should be particularly thoughtful about their use of modern tracking technologies on their websites and, where they do opt to use such technology, be sure to obtain prior consent from site visitors to track their website interactions.

About Cybersecurity Bits and Bytes

This blog covers the latest trends and events in cybersecurity law. We'll provide tips, tricks, and tactics for handling cybersecurity situations, and analysis of recent cybersecurity case law, statutes, and regulations.

Contributors

- [David Duffy](#)
- [Milada Goturi](#)
- [Matt Hafter](#)
- [Mark Mattingly](#)
- [Brittney Mollman](#)
- [Jennifer Post](#)
- [Luke Sosnicki](#)



authorsTest

brittney

Brittney K. Mollman

luke

Luke Sosnicki

aya

Aya Elalami