MASSACHUSETTS Lawyers Weekly

Part of the BRIDGETOWER MEDIA network JULY 13, 2023

VERDICTS & SETTLEMENTS

Massachusetts seeing wave of 'session replay' suits

Plaintiffs' bar seeks to apply wiretap statute to websites

■ Kris Olson

When a judge in the Superior Court's Business Litigation Session denied a motion to dismiss filed by BJ's Wholesale Club, it was just the latest sign that a proliferation of lawsuits over the use of "session replay code" to track the mouse clicks of website visitors is not going away anytime soon.

In Alves v. BJ's Wholesale Club, Inc., the plaintiff, on behalf of himself and all others similarly situated, is claiming that by using session replay code — JavaScript computer code embedded on a website that allows its operators to record, save and replay visitors' interactions — BJ's had violated the Massachusetts Wiretap Statute, G.L.c. 272, §99, and it was an invasion of privacy actionable under G.L.c. 214, §1B.

The same lead plaintiff and New York-based legal team is pursuing a similar case against Goodyear Tire and Rubber Co. in U.S. District Court in Boston, and cases are also popping up in other states where two-party consent — or at least two-party knowledge — is required to record conversations.

In support of its motion to dismiss the wiretap claim, BJ's pointed to several ways in which the language of the wiretap statute did not fit its use of session replay code. For example, it argued that the internet-based interactions did not constitute "wire communications," both because they were not communications at all and because they did not involve use of "a wire, cable or other like connection." Instead, it likened SRC to a surveillance camera that does not record audio.

BJ's also argued that it was not using an "intercepting device," nor was it recording the "contents" of any wire or oral communication.

But Judge Peter B. Krupp decided that the plaintiff's wiretap claim could not be dismissed at this early stage.

"The mouse movements, clicks, keystrokes, and other browsing activity that SRC records plausibly constitute an exchange of information between the website's owner and the website user," Krupp wrote.

Joseph D. Lipchitz

He added that unlike "cookies" — small text files that sit idly on a user's computer until contacted by a server, which a California federal judge ruled did not violate that state's wiretap statute — SRC "allegedly captures an individual's data in a manner that is much more active and invasive," making it look more like an "intercepting device."

Krupp similarly allowed the plaintiff's invasion of privacy claim to proceed, even as he noted that he was "somewhat skeptical" that the data BJ's collects is sufficiently personal or sensitive to establish such a claim.

Law just taking shape

Boston attorney Seth P. Berman noted that session replay

code lawsuits fit a pattern seen throughout the computer era, in which a party or prosecutor can make a "facially valid" argument that an older law should apply to new technology, leaving it to the courts to sort out whether it in fact applies. He likened it to the way early hackers were charged under criminal trespass statutes, at least until legislators could write and pass laws with more specificity.

According to Boston attorney Joseph D. Lipchitz, who has litigated several session replay lawsuits, any business with a public-facing website is a potential target for such claims, including hospitals and colleges and universities.

The lawsuits are the latest iteration of cases that members of the plaintiffs' bar has been bringing based on the use of cookies or pixels on their websites, Lipchitz said. Those "first generation" suits, which argued that the collection of visitors' data was an invasion of privacy, were largely unsuccessful, not surviving past the Rule 12(b)(6) motion to dismiss or summary judgment stage, as judges found that the technology was not particularly invasive or intrusive.

The plaintiffs' bar's strategic shift to trying to use wiretap statutes in dual-consent states makes strategic sense because it removes the requirement that a plaintiff show his privacy has been invaded. Rather, he need only show that his "communications" were "intercepted," Lipchitz said.

It will take some time for courts to catch up and analyze the degree to which these key terms should apply to technology that would have been inconceivable at the time Massachusetts' and other states' wiretap laws were written.

Krupp's decision is indicative of what Lipchitz senses is a widespread desire of courts for more "fulsome" factual records before ruling definitively on what the terms "communication" or "interception" encompass.

In time, it may well be that courts decide that of course there is no "interception" involved when a consumer visits a website, since everyone understands that communicating with the company in question — and having that interaction recorded — is the point of visiting the website in the first place, Berman said.

Boston attorney Joseph J. Laferrera agreed that the more interesting decisions in the Alves case will come when it gets to the summary judgment stage or an appellate court.

As the case law develops, Laferrera said one thing that may prove tricky is the tendency of judges to manufacture a certain standard to get to a certain result that feels comfortable, when there is a whole litany of ways in which analytics on how visitors are using websites is tracked — and will come to be tracked as technology develops further — that may defy bright-line rules.

Lipchitz suggested you might also see defendants increasingly challenge plaintiffs' standing using the U.S. Supreme Court's 2021 decision in TransUnion LLC v. Ramirez, arguing that plaintiffs cannot demonstrate the type of concrete harm the test announced in TransUnion requires to be entitled to statutory damages.

Even if plaintiffs can get over the TransUnion hurdle, they may have a challenge convincing juries that they deserve anything more than nominal damages, Berman noted.

"I feel like this kind of case runs the risk of being a Pyrrhic win," he said.

However, in the near term, that will not stop the flood of cases, Berman added.

Minimizing exposure

Lipchitz said website operators may be able to insulate themselves to a large degree by obtaining consent from users — preferably in the form of pop-ups that must be clicked through — acknowledging that they are aware SRC is being used. When a privacy disclosure is less conspicuous, the fact that the plaintiff could not reasonably have been expected to see the disclosure inevitably becomes part of their allegations, he said.

Given that, Lipchitz said it is a good idea for businesses and institutions to do an audit of

their privacy and data collection practices.

Laferrera said he is sure of one thing: that website operators' use of analytics is here to stay. What may change is how things are done at the margins, he said, with the kinds of disclosures website operators provide and consent they obtain.

There may be a "little turmoil" during the current "transition period," but at the end, it will become clear what the government intends to require of website operators.

"And the website owner will say, 'Sign me up,'" Laferrera predicted.

Neither the plaintiff's attorney in Alves v. BJ's Wholesale Club, Joseph P. Guglielmo of New York, nor the defendant's lawyer, Geoffrey M. Raux of Boston, responded to Lawyers Weekly's request for comment.

Boston attorney Michael T. Maroney, who is defending Goodyear against Alves' federal lawsuit, declined to comment.

Going beyond the text

To the extent that it can be determined at this point, Massachusetts' appellate courts will at least be inclined not to be such strict textualists that they summarily dismiss the suggestion that the state's wiretap statute might apply to SRC, Laferrera said.

"We do not depart lightly from the express wording of a statute, but in the unusual circumstances appearing here… a deviation is justified," the Appeals Court wrote in its 2000 decision Dillon v. Massachusetts Bay Transp. Auth.

Nonetheless, absent guidance from a higher authority, Krupp was not ready to latch onto BJ's attempt to use Dillon to argue that its SRC, which it obtained from a third party, falls under the law's telephone equipment exception.

SRC, he noted, "has characteristics quite different from telephone equipment."

As the case law in this context develops, Laferrera suggested that it will be fascinating to see whether courts in more politically conservative states begin to take a more textualist approach to interpreting their wiretap statutes than their more progressive counterparts.

Even though Alves' invasion of privacy claim survived dismissal, too, the wiretap claim is the more interesting one, given the less settled legal landscape, attorneys suggest.

The language Krupp used, even as he kept the invasion of privacy claim on life support, reinforces that idea.

The judge said that, despite his reservations, he was keeping the claim alive for three reasons.

"First, the question of whether the intrusion transgresses the privacy statute is a fact question," he wrote.

Second, Krupp acknowledged statistics in Alves' complaint, which indicate that "what constitutes acceptable data collection on the Internet appears to be evolving."

Among those statistics are a KPMG report in which 86 percent of respondents reported a growing concern about data privacy, while 78 percent expressed fears about the amount of data being collected.

Alves' complaint also noted that Apple recently rolled out a new version of its iPhone operating software that asks users for clear, affirmative consent before allowing companies to track them. Once the feature became available, 85 percent of users worldwide and 94 percent in the United States chose not to allow such tracking, the complaint states.

Finally, Krupp said he was also guided by practical considerations, noting "the scope of discovery will not differ if plaintiff's claim under G.L.c. 214, §1B remains."

He added that he could not resolve at this stage of the litigation a question raised by the defendant of whether the Legislature intended for the wiretap statute to provide the exclusive civil remedy for those "whose personal or property interests or privacy were violated by means of an interception" or whether the plaintiff could pursue both claims, even though they are based on the same facts.