The Computer & Internet Lawyer

Volume 43 ▲ Number 4 ▲ April 2026

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Is Florida the New Hotbed for Digital Wiretapping Lawsuits? 6 Steps You Can Take to Minimize Your Risk

By Michael E. Bonner, Usama Kahf, Alissa Kranz and Lindsay Massillon

Florida has suddenly become flooded with "digital wiretapping" lawsuits or demand letters targeting companies that use standard tracking technologies on their websites or in marketing emails. While historically many of these claims zeroed in on industries like healthcare, a new lawsuit filed in the U.S. District Court for the Southern District of Florida signals a critical shift in the legal landscape. The *Magenheim and Neil v. Nike Inc.* case presents a cautionary tale of how these claims may now implicate *any* consumer-facing company operating in Florida that uses common digital marketing tools. This article explains the allegations, the expansion of digital wiretapping claims in the Sunshine State, and six essential steps you can take to minimize the risk of these claims.

The authors, attorneys at Fisher & Phillips LLP, may be contacted at mbonner@fisherphillip.scom, ukahf@fisherphillips.com, akranz@fisherphillips.com and lmassillon@fisherphillips.com, respectively.

THE "SURREPTITIOUS" HARVESTING OF DATA

The *Nike* lawsuit alleges the company's website surreptitiously triggers the installation of invasive software on a visitor's web browser the moment they land on the page. This software then captures personal data to be shared with third parties for Nike's commercial benefit. According to the complaint, which was filed December 16, Nike does not use traditional "cookie consent banners" to seek permission before deploying these tracking technologies.

Nike's website is configured to ignore "Global Privacy Control" signals that are universal browser flags used by consumers to opt out of tracking, the plaintiffs say. Moreover, the suit claims that even when a user navigates to the privacy link on the website and manually opts out, the website continues to harvest data and share it with third-party partners. This data, which includes IP addresses and browsing habits, is being used to fuel a multi-billion-dollar "identity resolution" industry, they allege.

LARGE-SCALE IMPLICATIONS FOR COMPANIES DOING BUSINESS IN FLORIDA

The *Nike* case, along with another class action filed in Florida federal court against a restaurant brand, represents a major expansion of legal theories that were once largely concentrated in California. Plaintiffs in Florida are now aggressively using the state's wiretapping law and the Florida Security of Communications Act (FSCA) to claim tracking pixels and "session replay" software "intercept" electronic communications without consent.

While the first wave of these Florida lawsuits targeted healthcare providers for using tracking pixels on patient portals, the *Nike* case confirms that any consumer-facing website using common digital marketing tools is now a potential target. For companies doing business in Florida, the financial risks of being hit with one of these lawsuits could be substantial. For example, the *Nike* suit alone seeks to represent "hundreds of thousands" of class members, with the amount in controversy exceeding $5 million, including claims for punitive damages. Could your industry or business be next?

CLASS ACTION DEMAND LETTERS BASED ON "TRAP AND TRACE" THEORY UNDER FLORIDA LAW

In addition to the recent class actions filed against Nike and a restaurant brand, businesses have started to receive demand letters threatening a class action under Florida wiretapping law based on the "trap and trace" theory. The claim is that use of very common trackers in marketing emails that report back to the sender (usually through a vendor) whether and when the recipient clicked on the email. This technology is in use by millions of businesses and likely embedded in billions of marketing emails (or more).

Yet plaintiffs are claiming this technology constitutes an illegal "trap and trace" device under the state's wiretapping law. It is no coincidence that this is the same theory that has trapped (pun intended) thousands of businesses in expensive litigation and settlements under California law, as California and Florida wiretapping laws have similar prohibitions on trap and trace devices.

"TESTER" PLAINTIFFS HAVE FILED HUNDREDS OF LAWSUITS IN FLORIDA SMALL CLAIMS COURT

Recently, several "tester" plaintiffs through the same law firm have filed hundreds of nearly identical lawsuits in small claims courts in Florida with a jurisdictional limit of under $8,000 in damages. The claims are all wiretapping under Florida's Security of Communications Act based on recording of "live chat" electronic communications through a website chat feature. Plaintiffs claim the chats were recorded without prior consent. These cases are dragging in many small businesses, and even businesses that have no presence or operations in Florida.

More troubling is that a business facing one of these lawsuits must appear in court for a pretrial conference within a week or two of being served with the summons. Plaintiffs' counsel have used this tactic to pressure businesses into quick and relatively cheap settlements regardless of the merits, as it would cost businesses more to investigate and defend against the claims.

6 WAYS TO MINIMIZE THE RISK OF DIGITAL WIRETAPPING CLAIMS IN FLORIDA

To protect against this surge of Florida-based digital wiretapping lawsuits, consider the following proactive measures to ensure you're in compliance:

1. Implement Clear and Conspicuous Consent Mechanisms

- Affirmative consent – such as clicking "I agree" to terms or privacy policies – can help demonstrate that users were informed and agreed to data collection practices.

- Use prominent cookie banners or pop-ups that require users to affirmatively consent to the use of tracking technologies (such as pixels, cookies, and similar tools) before any data collection occurs. We refer to this as a "gatekeeper cookie banner," where a user is unable to access anything on the website without making a choice on the cookie banner, except for being able to view the privacy policy and terms of use.

- The wording of a cookie banner is also critical to establish consent. We recommend explicit language in the display disclosing the use of tracking technology, that data is being shared with third parties, and the purposes for which data is shared such as targeted advertising and analytics.

2. Regularly Review and Update Privacy Policies and Terms

- Ensure that privacy policies and terms of use are up-to-date, accurately describe all tracking technologies in use, and are easily accessible and

understandable to users. Privacy counsel can assist in crafting a balanced privacy policy that is specific, but readable for the average consumer.

3. Limit Data Collection to What Is Necessary

- Evaluate the necessity of each third-party pixel or tracker on your website. Limit the collection of personal information (such as IP addresses, device identifiers, and metadata) to what is strictly necessary for business operations.

4. Conduct Regular Compliance Audits of Website Tracking Technologies

- Periodically audit your website to identify all active tracking technologies, including those deployed by third parties, and ensure they comply with applicable privacy laws and your own policies. Regular audits help maintain compliance and demonstrate good faith efforts to protect user privacy.

- Regularly test your cookie banner and cookie consent process to make sure it works as intended. Technology changes over time, and with every addition to the website, you may inadvertently cause cookies to be misclassified or to share data when they're not supposed to.

- Obtain legal advice regarding website audits rather than completely relying on a vendor or consultant to complete them. Outside counsel who are in the trenches of digital wiretapping litigation will be more in tune with the specific issues that increase risk, as well as new legal theories being pushed in these lawsuits.

5. Monitor Legal Developments and Seek Legal Guidance

- The legal landscape is rapidly evolving, and courts may interpret statutes differently. You can stay informed about new case law, regulatory guidance, and legislative changes by consulting with legal counsel, who can help you assess risk and update practices as needed. Proactive monitoring and legal review can help businesses adapt quickly and avoid costly litigation.

6. Get Involved in Efforts to Amend Florida's Wiretapping Law

- Tennessee, New Hampshire and Alaska have already amended their state wiretapping laws to clarify that it is not a violation of the law for a business to deploy third-party cookies and pixels on its website. Florida is primed for a similar clarification of its law. Contact your Florida business industry association, such as the Florida Chamber of Commerce or the Associated Industries of Florida, to voice your concerns regarding this troubling litigation trend.

Copyright © 2026 CCH Incorporated. All Rights Reserved.
Reprinted from *The Computer & Internet Lawyer*, April 2026, Volume 43, Number 4, pages 8–10 with permission from Wolters Kluwer, New York, NY, 1-800-638-8437, www.WoltersKluwerLR.com

