The Computer & Internet Lawyer

Volume 43 ▲ Number 2 ▲ February 2026

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

Your Website Chatbot Could Cost Your Business: What You Need to Know About Rising Digital Wiretapping Risks in Florida and Beyond

By Risa B. Boerner, Danielle Kays and Lindsay Massillon

Does your company's website use automated bots to interact with visitors? A wave of Florida-based privacy litigation has created new compliance considerations for businesses that use what are now commonplace website tools. If you operate a website that uses live chat, customer service bots, or third-party tracking systems, your company may already have a target on its back, even if it is not based in the Sunshine State. Here is what your business should know about an uptick in digital wiretapping litigation in Florida and beyond, plus five compliance steps you should consider taking now.

UNDERSTANDING THE EVOLVING LANDSCAPE

The Florida Security of Communications Act (FSCA), which has been on the books since 1969, was originally designed to prevent illegal wiretapping of telephone communications. But recent court decisions apply it in ways that attack modern technological advances, and Florida cases involving website tracking tools have increased substantially: from just five in 2021 to 28 in 2024, and hundreds filed in this year alone.

The landscape of privacy laws evolves daily. Plaintiff lawyers are taking old laws from decades ago, before all this technology was ever thought of, and repurposing them to apply to modern technology.

Commonplace technology is under attack, and the courts are providing mixed decisions on whether these old laws apply to new technology. It is very important to have a conversation with counsel and not just assume you're safe because everybody's doing it.

So, what lit the spark that ignited the plaintiffs' bar to pursue this avenue? On top of the recent nationwide influx in privacy litigation (with California leading the pack), a Florida federal judge's decision in March spurred additional digital wiretapping lawsuits across a number of industries. That ruling allowed a class action lawsuit to proceed based on claims that a healthcare organization's website tracking technologies and chatbots violated the FSCA by intercepting internet communications without consent.

The authors, attorneys with Fisher Phillips, may be contacted at rboerner@fisherphillips.com, dkays@fisherphillips.com and lmassillon@fisherphillips.com, respectively.

KEY POINTS FOR BUSINESSES ABOUT THE FSCA'S FRAMEWORK

The FSCA was modeled after the Federal Wiretap Act but includes a key distinction: Florida requires all parties to consent before any communication can be intercepted, while federal law allows one-party consent. Although digital wiretapping lawsuits have been filed in various jurisdictions across the country, two-party consent states like Florida and California have been the most popular venues to date.

The FSCA provides for statutory damages of $1,000 minimum per violation or $100 per day (whichever is higher), plus the possibility of punitive damages and attorney's fees. In class action scenarios involving thousands of website visitors, these amounts can accumulate quickly.

WHY WEBSITE CHATBOTS ARE DRAWING ATTENTION

The Florida federal district court's decision in March was particularly significant because the court found that search queries and user inputs – captured by tracking technologies offered by social media networks and search engines – could constitute substantive communications rather than mere technical data collection.

Individuals bringing these cases typically argue that chatbot vendors and analytics tools record conversations without adequate consent, that third-party tools intercept user communications, and that standard privacy policies may not meet Florida's consent requirements. This can include the collection of data through pixels and cookies on websites, as well as trackers embedded in marketing emails.

LITIGATION RISKS FOR ALL INDUSTRIES

Litigation over data tracking has touched various sectors. Healthcare providers face heightened scrutiny due to the sensitive nature of medical information. However, no business that utilizes this technology is safe from attack. Lawsuits have been filed in Florida across a variety of industries, including not only healthcare, but also technology, personal services, retail, professional and technical services, and transportation, among others. While certain industries may be more prone to catching a plaintiff's attorney's gaze, all companies should take time now to audit their website terms and conditions.

LITIGATION RISKS FOR BUSINESSES NATIONWIDE

Some recent lawsuits have been filed in Florida against businesses based in other states that do not have operations based in Florida but operate their websites nationwide. In those matters, the plaintiffs have claimed jurisdiction based solely on the alleged accessibility of the businesses' websites to the Florida-based plaintiff and Florida residents.

KNOW WHAT YOU ARE DISCLOSING

Many businesses unwittingly collect and share data, not realizing that third-party tools used to manage the website, track visitors to the website, or gather information for the business's own marketing purposes are also copying and retaining that data, and possibly selling or sharing it with others. Plaintiffs' lawyers have tools to identify the collection and sharing of this data, even if it is not obvious to either website visitors or the business operating the website.

The best way that a company can protect themselves is to contact their privacy lawyer and do an audit of their technology. It is important to learn where your data is going and how it complies with these laws.

5 STEPS YOU CAN TAKE TO GET AHEAD

Businesses should consider implementing the compliance measures discussed below.

1. *Audit Third-Party Website Tools.*

Take inventory of vendors that interact with your website, including live chat platforms, customer service bots, session replay tools, analytics and tracking pixels, and form tracking tools. Understanding which third parties have access to user data can help you assess your compliance posture.

2. *Review Your Consent Requirements.*

Consider implementing clear, conspicuous consent notices before chatbot interactions begin. Effective notices typically inform users that their chat conversation will be collected and recorded and may be monitored by third-party service providers. The notice should reference your privacy policy and be presented before any data collection starts.

3. *Consider Affirmative Consent Options.*

Rather than relying on passive acceptance through continued browsing, consider using active checkboxes or click-to-consent buttons that require users to take an affirmative action before engaging with chat features.

4. *Review Vendor Contracts.*

Your agreements with chatbot and analytics vendors should clarify their role as service providers

rather than independent parties, specify limitations on how they can use visitor data, and address consent and compliance obligations.

5. *Update Privacy Disclosures.*

Consider whether your privacy policy specifically identifies third-party vendors with access to chat data and clearly explains what information is collected and how it is used.

SPECIAL CONSIDERATIONS FOR SENSITIVE INDUSTRIES

Healthcare providers and financial services firms may want to take additional precautions given the additional targeting of these industries and unique considerations of data intense industries.