Florida Federal Court Greenlights Nationwide Digital Wiretapping Claims: 5 Steps Businesses Should Take Now

Insights
1.16.26

Another federal court just gave privacy plaintiffs exactly what they've been looking for: a green light to pursue nationwide digital wiretapping claims based on common website tracking practices. In a January 14 decision in *Cobbs v. PetMed Express, Inc.*, a Florida federal judge allowed federal wiretapping (ECPA) and California wiretapping (CIPA) claims to proceed against a company based on its use of common, third-party website tracking tools. We can now confidently say that at least one Florida court is receptive to digital wiretapping theories, and plaintiffs' attorneys will no doubt take notice. This means that your routine website tracking actions can create nationwide class-action exposure –potentially in California, Florida, or beyond. Indeed, even before this decision, Florida ranked second behind California for number of lawsuits filed alleging privacy claims based on use of digital tracking technology. This decision likely will further fuel this litigation trend in Florida. What do you need to know about this decision and what five steps should you take to guard yourself against this latest danger?

What Happened?

The lawsuit began when a group of California-based consumers allegedly visited PetMed's retail website to browse and purchase products.

- They searched for items, clicked buttons, filled out online forms, and added products to their carts, exactly the type of routine interactions businesses rely on every day.
- Unbeknownst to those users, however, they allege that common third-party tracking technologies embedded in the website were simultaneously capturing and transmitting detailed information about their activity to outside vendors in real time as they navigated the site.
- According to the complaint, that data included search terms, page URLs revealing what users were looking for, form field entries, and other content that reflected the substance of their online communications.
- The plaintiffs claimed they never meaningfully consented to this alleged interception and that the data sharing went far beyond basic analytics.
- Instead, they argued the information was used to build detailed profiles about them and fuel targeted advertising.

The Decision

The plaintiffs filed a nationwide putative class action in Florida federal court asserting claims under the Federal Wiretap Act (the Electronic Communications Privacy Act) and California's wiretapping laws, along with several related state-law claims. Even though the three plaintiffs are California-based, they filed their suit in Florida, where PetMed is incorporated. The plaintiffs most likely selected this venue because they saw an opportunity to advance their claim in what they hope is an increasingly receptive legal environment.

The company moved to dismiss the case at the outset, arguing that the plaintiffs lacked standing, that no "interception" of communications actually occurred, that the data at issue was not protected content, and that users had consented through privacy disclosures.

In its January 14 ruling, the court rejected many of those arguments – at least for now. While it dismissed a few ancillary claims, the court allowed the core federal and California wiretapping claims to proceed.

- **Federal wiretapping claims (ECPA)** – The court found plausible allegations that third-party tracking tools intercepted users' electronic communications in real time.
- **California wiretapping claims (CIPA §§ 631 and 632)** – The court accepted that URLs, form entries, button clicks, and search terms can constitute the "contents" of a communication, not just routing data.
- **Standing** – The court rejected arguments that plaintiffs must show financial loss or misuse of their data in order to have sufficient standing to pursue litigation. Simply alleging that the business intercepted their online communications was enough for the court to give the plaintiffs the right to proceed. This conflicts with other federal court rulings (including in California) that emphasize standing to sue requires showing more than mere disclosure of information or a technical statutory violation.
- **Consent** – Finally, the court ruled that the question around whether consumers consented to the tracking could not be resolved early, despite the presence of a privacy policy and alleged consent mechanisms. That means businesses may be forced into costly discovery before getting another chance to exit the case.

Is Florida the New California? We Hate to Say We Told You So, But…

We just published an Insight last week asking the question: *Is Florida the New Hotbed for Digital Wiretapping Lawsuits?* The answer, as this latest decision makes clear, is unfortunately yes.

California has long dominated digital wiretapping litigation. But Florida is catching up, second only to California when it comes to the number of digital wiretapping lawsuits. At the current pace and with more rulings like this one, it could overtake California within a year or two. You can track these

trends in real time on our FP Digital Wiretapping Litigation Map, which shows where these cases are being filed and how quickly they're spreading.

5-Step Action Plan for Businesses

Here's how businesses should respond in light of this ruling.

1. Audit Your Website and App Tracking Technologies

Conduct a comprehensive review of pixels, session replay tools, embedded analytics scripts, marketing automation tracker, and email and SMS tracking technologies. Understand what data they collect, when it is transmitted, and who receives it. We recommend outside counsel conduct or direct such review to invoke the attorney-client privilege and attorney work product protections. The last thing you need in this litigious environment is a discoverable, non-privileged report of where all the bodies are buried. Not to mention that your privacy counsel would be more in tune with litigation risks and how the technical issues are playing out in court than non-lawyer experts.

2. Reevaluate Consent Mechanisms, Especially Timing

This decision reinforces that privacy policies alone may not be enough, and passive disclosures may not establish consent. Instead, aim for clear, conspicuous, and timely consent. You should use this as an opportunity to pay attention to cookie banners, pop-ups, click-through disclosures, and review when consent occurs.

3. Scrutinize "Content" Data Collection

Tracking tools that capture items beyond basic analytics (like search queries, form inputs, URLs revealing user intent, and button clicks tied to sensitive topics) are targets and may pose higher litigation risk. Minimize or reconfigure these tools where possible.

4. Tighten Vendor Contract Terms

Ensure agreements with your vendors clearly allocate compliance responsibility and address wiretapping and consent obligations. Where possible and appropriate, you should include an indemnification clause.

5.Monitor Florida Developments Closely

Florida is no longer a fringe jurisdiction for these cases. Businesses should treat Florida developments with the same urgency traditionally reserved for California, forming relationships with Florida-based privacy counsel (such as those at Fisher Phillips) and monitoring litigation with a close eye. The legal landscape of these claims changes by the day so it is important to stay up to date (with the help of your counsel) to best mitigate your risks.

Conclusion

To stay informed, subscribe to Fisher Phillips' Insights System for timely updates on digital wiretapping litigation and other privacy-related trends. For personalized guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Florida offices or on our Digital Wiretapping Litigation Team. You can also explore additional resources on our US Privacy Hub.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Danielle Kays
Partner
312.260.4751
Email

Brett P. Owens
Partner
813.769.7512
Email

Service Focus

Privacy and Cyber

Litigation and Trials

Consumer Privacy Team

Digital Wiretapping Litigation

Trending

U.S. Privacy Hub

Related Offices

Orlando

Tampa

Fort Lauderdale