Businesses Get Big Privacy Win in Tester Plaintiffs' Wiretapping Case: 3 Key Takeaways

Insights
4.14.25

In a big win for businesses, a California federal court just held that a "tester" plaintiff – someone who visits websites for purposes of initiating litigation – cannot bring a claim under the California Invasion of Privacy Act (CIPA). Tester plaintiffs have started to focus on consumer protection statutes in hopes of broadening CIPA's application to include internet communications, which would provide them a treasure trove of potential targets. But the recent decision in *Rodriguez v. Autotrader.com, Inc.* not only provides a defense for businesses facing lawsuits by tester plaintiffs but also bolsters another unrelated defense: setting privacy expectations with consumers. Here is what you need to know to best position your business to avoid (or successfully defend against) CIPA lawsuits, including three key takeaways you can put into place right away.

What is a Tester Plaintiff?

A "tester" plaintiff is typically a self-identified "consumer advocate" who takes specific actions to create a violation of a law and file a lawsuit (often, class actions) alleging violations of various consumer protection laws. Tester plaintiffs have been most prominent in the context of the Americans with Disabilities Act lawsuits. For example, tester plaintiffs often access businesses which they allege are not ADA complaint (e.g., they allege websites are not accessible for persons with visual disabilities, or buildings are not physically accessible due to things like doors being too narrow or counters too low for persons with wheelchairs) and then sue for the alleged violation. More recently, tester plaintiffs have used the same tactics to bring lawsuits alleging privacy violations, including under CIPA.

What Do You Need to Know About CIPA Litigation?

CIPA is a broad statute that, among other things, prohibits wiretapping along with certain collection or uses of personal information. While this nearly 60-year old statute has historically been thought of in the context of telephone lines or physical recording devices, a groundbreaking 2022 federal appeals court decision extended the reach of this statute to website usage. Since then, businesses operating businesses in California have faced an onslaught of CIPA litigation based on a website's use of third-party cookies, pixels, and other types of tracking technology (see Fisher Phillips' Digital Wiretapping Litigation Map here).

Court Holds A Tester's Lack of Privacy Expectation Defeats CIPA Claim

In *Rodriguez v. Autotrader.com, Inc.*, the plaintiff alleged two violations of CIPA:

- operation of a pen register on the website using tracking technology that could collect a user's IP address; and
- aiding and abetting wiretapping by disclosing website search terms to third parties. (A more comprehensive discussion of pen registers and monitoring software is available here).

The court dismissed both CIPA claims in an April 4 decision because a tester plaintiff who "actively seeks out privacy violations" does not have an expectation of privacy. The court rejected the plaintiff's argument that ADA and First Amendment decisions which allow plaintiff to claim injury "regardless of their expectations or intentions" should apply to CIPA. Because a tester plaintiff in a CIPA case visits the website and intentionally enters information into the website expecting her information to be "accessed, record, and disclosed," they cannot claim an injury. Critically, a tester necessarily expects – and invites – the injury to occur.

3 Key Takeaways for Businesses

Tester lawsuits in the privacy context can be costly and burdensome to resolve. The court's decision is a great victory for businesses fighting these claims. But not all CIPA plaintiffs are tester plaintiffs. With that in mind, your best defense is a good offense – which is to take steps to make your website a less likely target for lawsuits and, if you do get hit with a claim, have a fallback legal defense.

1. Review Your Website

Closely look at your website to evaluate the pixels, web beacons, cookies, and other tracking tools used.

- Identify the data each tracking tool discloses and who receives it.
- Ascertain what third parties do with your data once they receive it.
- This requires robust scanning of your website to identify this data and where it goes.

Often the problem lies in a lack of knowledge about what is on a particular website. Sometimes there are cookies and pixels left over from past initiatives, or sometimes vendors remain active on the website. Sometimes you don't know the full extent of what cookies are installed, since not all cookies are active at the same time. This is why deploying a scanning tool is a good place to start. But make sure you couple that with analysis and review, so you understand the results of the scan.

2. Display Appropriate Disclosures

Key to the court's decision in this case was the expectation of privacy. Your website can set appropriate expectations for non-tester plaintiffs by including disclosures that adequately describe:

- the parties to the communication;
- to whom the data is disclosed;
- the further use (if any) of the data; and
- where consumers can access your privacy practices – and all before the consumer enters or provides any information.

For example, cookie banners should state that data is disclosed to third parties for targeted ad purposes, if that is the case, instead of only stating that the website uses cookies to improve user experience.

3. Opt-In and Opt-Out Choices

Consider providing website visitors the option to choose whether they opt in or opt out of the use of data as described in the disclosures. Each of these options should be just as easy to accomplish as the other, known as symmetry of choice. This may involve turning off collection of data through cookies or pixels until a consumer opts-in by clicking a button.

Opt-in consent may not be required by applicable consumer privacy laws like the California Consumer Privacy Act (CCPA). However, putting website users in control of their privacy choices is another way to align user expectations of privacy with their experience on your website, mitigating against CIPA claims.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the author of this Insight, or any member of our Privacy and Cyber team.

Related People

Related People

Catherine M. Contino
Associate
610.230.6103
Email

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Danielle Kays
Partner
312.260.4751
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Litigation and Trials

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills