Insights, News & Events

MAJOR WIN IN CIPA CASE SIGNALS HIGHER HURDLES FOR PRIVACY PLAINTIFFS: WHAT YOU SHOULD DO TO PROTECT YOUR ORGANIZATION

Insights
Mar 4, 2026

Major Win in CIPA Case Signals Higher Hurdles for Privacy Plaintiffs: What You Should Do to Protect Your Organization

In a significant win for businesses fighting CIPA claims, a California federal court just held that searching sensitive health terms and distributing that information to third parties is not a legally protectable privacy interest, foreclosing a plaintiff from pursuing a class action lawsuit. Although the court allowed the plaintiff to amend his complaint and fix its deficiencies, the February 23 decision marks a significant shift in evaluating a plaintiff's so-called injuries in these cases. Rather than accepting plaintiff's threadbare allegations of harm, the court in *Maghoney v. Dotdash Meredith Inc.* dug into the allegations of the complaint and questioned whether the plaintiff had actually alleged awareness that his information had been shared with third parties and whether any data shared could have been associated with his name or other personally identifiable information. Here is what you need to know to use this decision to successfully defend against CIPA lawsuits, including takeaways you can put into place right away.

What's at Issue?

The California Invasion of Privacy Act (CIPA) was originally enacted in 1967 to combat traditional wiretapping and eavesdropping, primarily in the context of telephone communications. It was written prior to the internet and was never designed to address the complexities of the digital

Related People

Risa B. Boerner, CIPP/US, CIPM

Partner

610.230.2132

Catherine M. Contino

Associate

age or to regulate how businesses track user interactions on the internet.

In recent years, however, plaintiffs' attorneys have increasingly applied CIPA to modern online contexts. As you can see on FP's Digital Wiretapping Litigation Map, we've tracked thousands of lawsuits that used the statute to target routine website technologies such as cookies, pixels, search bar/form, chatbots, session replay tools, and software development kits (SDKs).

Recent Trends Are Increasing the Pressure

Plaintiffs' attorneys frequently target healthcare companies, often alleging that plaintiffs are entitled to privacy protection for their searches for symptoms, diseases, or treatment information, and that the sharing of such information with third parties is a privacy violation. Because courts are increasingly worried about unauthorized disclosure of personal health information, judges have sometimes allowed these claims to proceed past the initial pleading phase, requiring parties to engage in discovery even if a plaintiff's allegations are scarce on the details of how plaintiffs were actually harmed or injured.

A number of law firms specialize in filing CIPA and other privacy claims against businesses. They often send demand letters that may not result in litigation but lead companies to pay out millions of dollars in settlements to avoid litigation. Law firms operating in this area often file cookie-cutter complaints that repeat the same allegations in order to leverage a quick settlement. More firms are jumping on this bandwagon as these types of claims proliferate.

What Happened in This Case?

Plaintiff Tyler Maghoney alleges that he visited Dotdash's website, www.verywellhealth.com, two times in December 2024 and entered specific search terms on the website related the symptoms, contraction, and treatment of sexually transmitted infections. He alleges that he expected his searches to remain private.

When he visited the website, he alleges that the website's advertising platform intercepted his private information and transmitted it to third parties, including his search terms, page navigation history, and metadata which can include IP address and device identifiers. Maghoney claimed that the

610.230.6109

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Industry Focus

Healthcare

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

advertising platform is an advanced fingerprinting and profiling mechanism that can circumvent browser privacy protections and track users across sessions and properties.

He filed a class action lawsuit asserting violations of CIPA and the Confidentiality of Medical Information Act (CMIA), and invasion of privacy under the California Constitution, among other claims.

Case Turns on "Standing"

Article III standing is a legal rule that decides who is allowed to bring a lawsuit in federal court. It comes from Article III of the U.S. Constitution, which limits federal courts to hearing only "cases" or "controversies." In simple terms, not everyone who is upset about something can sue in federal court – there are specific requirements.

To have standing, a person must show three things:

1. Injury: You must have suffered, or will soon suffer, a real and specific harm. This harm can be physical, financial, or even a violation of your rights, but it can't be just a general complaint about the law or government.

2. Causation: The harm you suffered must be directly linked to the actions of the person or group you are suing. In other words, your injury must be caused by what the defendant did (or didn't do).

3. Redressability: The court must be able to do something to fix your injury. If the court's decision can't help you, then you don't have standing.

What Did the Court Decide?

The court dismissed the case for lack of standing, providing Maghoney leave to amend. The court found that:

- His searches relating to sexually transmitted infections on the website do not form a legally protectable privacy interest, and the alleged distribution of that information cannot establish a concrete injury under Article III of the U.S. Constitution.
- Maghoney failed to sufficiently allege that he was at risk of future harm (such as identity theft or digital profiling) as a result of the website's sharing of his information.

- Alleging that he was deprived of control of his private online activities is not a concrete harm sufficient to confer Article III standing.
- Allegations of anxiety, without any detail or specificity, are insufficient to demonstrate an injury-in-fact to establish standing.

Rather than taking Maghoney's allegations at face value, the court examined the allegations of the complaint. The court found that despite alleging that his health searches were intercepted and shared with third parties, he did not allege how he became aware of this information sharing, that anyone contacted him relating to these inquiries, or that his searches were made publicly visible.

Further, Maghoney did not allege that any of his contact information, personal identifiers, or metadata were associated with his searches. The court found it significant that he merely searched sensitive health terms, noting that the website is not a patient portal nor were the searches tied to his medical history. The court also found that even if the IP address or other metadata was linked to the searches, that information is not personally identifiable information.

What's Next?

The court gave Maghoney leave to amend his complaint to address its deficiencies. It is unclear if he will be able to do so, or whether he can assert an injury sufficiently concrete to establish standing even if he does. The court honed in on the speculative and conclusory allegations that are regularly asserted in CIPA cases and asked "where is the harm?" Other courts facing similar claims may start to take guidance from this court's decision to interrogate plaintiffs' allegations that appear amorphous and abstract.

Key Takeaways:

1. Higher Bar for Privacy Claims Under CIPA: The court held that searching for sensitive health terms and the alleged sharing of that information with third parties does not, by itself, create a legally protectable privacy interest or a concrete injury under Article III of the U.S. Constitution. This raises the standard for plaintiffs to bring CIPA claims in federal court.

2. Speculative or Generalized Harm Is Not Enough: Plaintiffs must allege specific, concrete harm – such as actual identity theft or demonstrable misuse of personal information – to establish standing. General claims of anxiety or loss of control over information, without detail, are insufficient.

3. Courts Are Scrutinizing "Cookie-Cutter" Complaints: The decision signals that courts may no longer accept generic or conclusory allegations in privacy lawsuits. Plaintiffs must provide detailed facts showing how they were harmed, not just that information was shared.

4. Metadata and Non-Identifiable Information May Not Trigger Liability: The court found that sharing metadata (like IP addresses) or search terms, without linking them to personally identifiable information, is unlikely to support a privacy claim under CIPA or Article III.

Recommendations for Businesses

In light of this decision, here are some recommendations for you to best position your organization to avoid CIPA claims and defend them if asserted against you:

- **Review and Document Data Practices:** Ensure your data collection, sharing, and privacy practices are well-documented and transparent. Be prepared to demonstrate that any shared data is not personally identifiable.
- **Update Privacy Policies and Disclosures** Clearly explain to users what information is collected and how it may be used or shared, especially regarding sensitive topics like health.
- **Monitor Legal Developments:** Stay informed about evolving case law and regulatory guidance on digital privacy, as courts may continue to refine what constitutes a protectable privacy interest.
- **Prepare for Litigation Strategically:** If faced with a CIPA or similar privacy lawsuit, scrutinize the complaint for lack of concrete harm or specific allegations. Consider challenging standing early in the litigation process.

Conclusion

We 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 directly to your inbox. You can also visit FP's Digital Wiretapping Litigation Map for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group or Digital Wiretapping Litigation Team.