Insights, News & Events

COURT TOSSES MOST CLAIMS IN HEALTHCARE PIXEL PRIVACY SUIT, RULING THAT WEBSITE VISITS DON'T REVEAL PHI: WHAT YOUR BUSINESS SHOULD DO

Insights
Dec 3, 2025

A California federal court recently handed healthcare businesses another victory in the ongoing wave of privacy lawsuits targeting website analytics and tracking tools. A California federal judge ruled on November 21 that data collected by pixels and similar website tracking technologies does not constitute protected health information (PHI) when it merely reflects a user's visits to public webpages. As long as the tracking does not reveal anything about the user's health conditions, care, or interactions that could plausibly relate to the provision of healthcare, the court ruled that businesses are in the clear and not liable for improperly gathering medical information under federal or state law. What do you need to know about the *Wright v. TrueCare* decision and what lessons can you learn?

Website Visits Lead to Lawsuit

In her Complaint, Amy Wright alleged she visited Truecare's website six times over the course of a year and that a social media pixel tracked her search terms entered on the website. Wright included a screenshot of her downloaded browsing data tracked by the pixel on Truecare's website, showing six tracked events categorized as searches, contacts, or page views. However, the browsing data did not reveal on its face any information about the content of the searches, contacts, or pages themselves.

Wright alleged that her right to privacy was violated when she was web browsing on Truecare's website because the pages she visited related to the topic of her health and thus constituted personal information of a private and

Related People

Anthony Isola
Partner
415.490.9018

Arielle Williams
Associate
214.220.8339

confidential nature. Significantly, however, Wright failed to allege the specific private information she believed was tracked by the social media pixel.

Wright filed suit in the Southern District of California, asserting claims for:

- wiretapping under the Electronic Communications Privacy Act (ECPA) and California Invasion of Privacy Act (CIPA)
- invasion of privacy under the California constitution
- violation of the Confidentiality of Medical Information Act (CMIA)

Truecare filed a Motion to Dismiss, which the court mostly granted in its November 21 decision.

The Court's Decision

In its decision, the court explained what information constitutes PHI – and what doesn't constitute PHI – in the context of third-party tracking software on a website:

- It is not PHI if the tracked data does not reveal something about the "past, present, or future physical or mental health or condition of an individual" or their healthcare.
- In order to allege PHI based on the use of a public webpage, a plaintiff must allege that their "interactions plausibly relate to the provision of healthcare, or that the information connects a particular user to a particular healthcare provider."

Invasion of Privacy and CMIA Claims

The court further explained that a claim based on tracking of PHI cannot survive a motion to dismiss if the claim contains only conclusory or hypothetical explanations of how the social media pixel could track alleged sensitive information on a healthcare website. The court found that Wright's allegations came up short because they only show that she used Truecare's website, but not how she used it or what her visits revealed about her healthcare information. This led the court to dismiss Wright's claims for invasion of privacy and under CMIA.

Wiretapping Claims

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Industry Focus

Healthcare

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills

Separately, the court addressed Wright's claims for wiretapping under the ECPA and CIPA. The court reasoned that her allegation that she accessed the Truecare's website is mere "record" information and her allegation that her social media ID was associated with her visits is mere "identifying" information. Neither allegation was sufficient to advance a claim that Truecare intercepted the "content of communication" as required to state a claim under federal or California wiretapping laws.

Pen Register and Trap-and-Trace Claim

However, the court denied the motion as to the CIPA pen register and trap-and-trace claim and allowed them to proceed to the next stage of litigation. The court relied on prior cases that found that certain allegations concerning the functionality of social media pixels satisfy the pleading requirements for a pen register or tap-and-trace. Notably, the court decided this issue without addressing a series of other court opinions that ruled in the exact opposite way.

Lessons Learned

Businesses in the healthcare industry and elsewhere can learn some critical lessons from this litigation. Three of the most critical lessons:

1. Healthcare websites should have opt-in consent for social media pixels

Healthcare websites generally should not turn on social media pixels without user opt-in consent. This is especially true where the third party is obtaining more details about the user than just metadata, such as their specific searches for medical providers or health conditions.

2. The privacy policy should clearly inform users that that data collection is being shared through cookies and pixels

You should adequately describe your data collection and sharing through cookies and pixels in your privacy policy. Make sure it is conspicuously presented to the user before they can interact with the website in a way that would reveal something about the user's health condition.

3. Compliance with consumer privacy laws does not avoid litigation

Mere compliance with comprehensive consumer privacy laws like the CCPA and similar laws in 18 other states will not insulate website operators from litigation risk for use of tracking technology on websites and apps. We recommend you work with your FP Privacy counsel to conduct a litigation risk assessment to spot the issues that may land you in expensive litigation.

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 direct to your inbox. 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, Consumer Privacy Team, or Healthcare Team.