Insights, News & Events

FROM SEARCH TO SHARE: COURT HOLDS THIRD-PARTY INTERCEPTION OF SEARCH BAR TERMS CAN SUPPORT CIPA CLAIM

Insights
Apr 11, 2025

As the privacy litigation landscape continues to take shape, search bars have quietly become a Trojan horse in online data collection, carrying new legal theories into the California Invasion of Privacy Act (CIPA) arena. The legal interpretation of what constitutes "contents" of a communication is evolving under CIPA, and this issue has taken on a greater significance for website owners and operators. So, if your business operates a website with a search bar, you should consider reassessing your website data collection and disclosure practices and implementing compliance measures. Otherwise, you may risk exposure to costly litigation. Here's what you need to know about recent developments in this area.

How Did We Get Here?

In *Heerde v. Learfield Communications*, the court held that search terms entered into a search bar constitute "contents of a communication" for the purposes of a CIPA claim, and a third party's interception of those search terms (through website cookies) could create legal liability.

CIPA prohibits people from using electronic means to learn the contents or meaning of any communication without consent or in an unauthorized manner. In *Heerde*, the defendants were website developers and operators of college athletic websites. The Team Websites, as the plaintiffs argued, appeared to be run by the schools, but in this case, the Operators were managing them.

Related People

Vivian Isaboke, CIPP/US, CIPM

Associate

908.516.1028

Anthony Isola

Partner

415.490.9018

The plaintiffs filed a class action lawsuit alleging that the Operators violated CIPA, the Federal Wiretap Act, and California constitutional privacy rights by intercepting search terms entered into search bars built into the Team Websites and feeding those search terms to third-party tracking entities.

They alleged two theories:

- The Operators willfully and without consent read or attempted to learn the contents of a communication (search terms), which were intended for the owners of the Team Websites (the schools), not the Operators; and
- The Operators aided and conspired with third-party tracking entities to unlawfully intercept the search terms by installing search bars on the Team Websites, knowing the search terms would be transmitted to third-party tracking entities.

How Did the Court Rule?

In making its decision to allow the CIPA claim against the Operators, the court addressed three critical questions:

> (1) whether the plaintiffs had a reasonable expectation of privacy in their search terms;
>
> (2) whether the search terms constituted "contents" of a communication; and
>
> (3) whether the Operators were parties to the communication and not third-party eavesdroppers, thus shielding them from liability.

Reasonable Expectation of Privacy: The court found the plaintiffs had a reasonable expectation of privacy regarding their search terms. The court cited precedent from the 9th U.S. Circuit Court of Appeals indicating that "users have a reasonable expectation of privacy over URLs that disclose either unique search terms or the particular document within the website that a person views." Moreover, the court found that, without notice or disclosure, the plaintiffs were not provided "any opportunity to consent to [the] use of a Search Bar [that] would cause their Search Terms to be shared with various parties."

Contents of a Communication: The court also found the plaintiffs' search terms constitute "contents" of a

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

communication under CIPA and the Federal Wiretap Act. Specifically, the court defined "contents" as "any information concerning the substance, purport, or meaning of a communication" – and the court found the search terms intended to convey a communication.

Third-Party Eavesdroppers: Lastly, the court explained that the Operators could be considered third-party eavesdroppers where it concerned interception of the plaintiffs' entry of search terms into the Team Websites. The **"party exception" to liability** for violating CIPA applies to parties to a communication and **not** third-party eavesdroppers. The court reasoned that the plaintiffs believed the Team Websites were run by the schools and their search terms were being communicated only to them.

How Can Businesses Mitigate Their Risks?

With legal theories under CIPA continuing to expand, businesses operating websites must closely examine online data collection and sharing practices. To mitigate the growing risks, you should consider taking the following steps:

Data Mapping: Conduct regular data mapping (or data inventory) exercises to understand how data is collected, stored, and shared, allowing for proactive compliance strategies.

Consumer Facing Policies: Review and revise consumer facing policies to include clear provisions on data collection, user consent, and dispute resolution.

- **Notice and Disclosure**: Review and revise online privacy policies and terms of use to explicitly inform users about the collection and sharing of search term data collected through website search boxes.
- **Class Action Waivers**: Help mitigate potential legal exposure and control litigation risk by incorporating class action waivers into terms of use.
- **Dispute Resolution**: Include specific dispute resolution procedures, such as mandatory arbitration, to further protect against litigation risks.

Digital Wiretapping Tracker: Closely monitor new and progressing privacy litigation claims to stay ahead of legal risk. To assist with this, Fisher Phillips has developed a

Wiretapping Litigation Tracking Map to help businesses gain insight into legal trends by state, industry, and court jurisdiction. Understanding litigation trends can help you plan proactive measures that balance online business needs and consumer privacy expectations.

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.