Insights, News & Events

CALIFORNIA BUSINESSES SCORE ANOTHER KEY PRIVACY WIN: 3 THINGS YOUR BUSINESS SHOULD DO AFTER LATEST CIPA COURT DECISION

Insights
Aug 5, 2025

Website operators secured another win in the protracted battle over third-party website cookies last week when a California state court held that these common tech features were not "trap and trace" devices and therefore a business did not violate the California Invasion of Privacy Act (CIPA) for having them. Significantly, the court's August 1 decision in *Heiting v. HP, Inc.* declined to grant leave to amend, meaning the case is dismissed and the plaintiff cannot file an amended complaint. Here is what you need to know about this decision, why it matters, and three important steps your business can take to avoid or defend against these lawsuits.

What Happened?

In *Heiting v. HP Inc.*, a plaintiff alleged that HP operated an illegal "trap and trace" by installing a third-party software on its website. A "trap and trace" is a device that captures incoming phone calls to particular number. Typically, these devices are used by law enforcement when illegal activity is suspected, and authorities typically need to acquire a court order before they can install the device.

The plaintiff brought suit under CIPA, which defines a "trap and trace" device as a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonable likely to identify the source of a wire or electronic communication, but not the contents of a communication."

Related People

Catherine M. Contino
Associate
610.230.6109

Usama Kahf, CIPP/US
Partner
949.798.2118

The plaintiff alleged that HP installed software on its website that de-anonymized her without her consent. Specifically, she alleged that HP partnered with a social media platform to install software on its landing page to identify the location, source, and identity of consumers who visit the website. The plaintiff alleged that the software gathers visitor information and sends the details to the social media platform – and this fits the definition of a "trap and trace" device.

The Decision

The court's August 1 decision found that plaintiff's allegations could not possibly establish that HP put any sort of tracker on plaintiff that allowed HP to monitor who else contacts her. The court's decision was based on the following reasons:

- A trap and trace device, by its statutory definition, prohibits the use of a device or process that identifies the *incoming* source of communications, such as phone numbers.
- The statute describes that the device has to identify who is contacting the target, not the contents of the communications.
- Therefore, the court found that the "statute prohibits receiving unauthorized information about incoming communications from other parties – not information that passes between plaintiff and defendant when plaintiff contacts the defendant."

Importantly, the court rejected plaintiff's arguments to expand the definition of CIPA to include third-party cookies and trackers within the definition of wiretapping, noting that:

> *"If CIPA broadly prohibits any process by which anyone identifies any 'originating number,' then every cell phone in the world – which identify the phone number of incoming calls – would be a prohibited trap and trace device. So would every website interaction that identifies electronic information about the user in a manner that allows the website to function. There is no indication that, in enacting the trap and trace device prohibition, the California Legislature meant to cover such devices."*

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

Impact of Decision

Notably, the court dismissed plaintiff's case without leave to amend, despite this being plaintiff's first filed complaint. Typically, courts will give plaintiffs the opportunity to file an amended pleading, especially if this is the first filed complaint in the case. However, the court did not do that here.

The court's decision to dismiss without leave to amend signals that the court is not buying what plaintiff is selling, and even an amended complaint would not change the fact that a trap and trace device does not apply to third-party software on a website. This decision should send a signal to plaintiffs' lawyers that California state courts are becoming savvier when evaluating CIPA claims by digging into to what exactly plaintiffs are alleging.

Further, it demonstrates the challenges of trying to apply a statutory scheme to new technology that was not contemplated at the time the statute was enacted. The court made specific reference to the fact this case is "one of many before this Court and other California trial courts in which plaintiffs allege that software used by websites to handle the communications when a user logs on to the website are either a 'pen register' or 'trap and trace device.'"

In another recent case, a Los Angeles court noted the variety of decisions trial courts have issued on this subject and noted the lack of appellate authority that would assist courts in making consistent decisions. The March 2025 decision in *Palacios v. Fandom, Inc.* saw the court note that it would "benefit from appellate guidance" on the scope of pen register and trap and trace devices. However, it's not clear if courts or practitioners will get any kind of guidance from California appellate courts or the federal 9th Circuit Court of Appeals.

What Can Your Business Do To Mitigate Risk?

It may be some time before either federal or state courts issue clear guidance on pen register or trap and trace claims. It's always a good idea to have practices and policies in place to avoid or mitigate risk of lawsuits like these to make sure your business is not a target or, if you do get a claim, you have a strong 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 authors of this Insight, or any member of our Privacy and Cyber team.