Websites Become New Litigation Battleground for Restaurant Industry: 5 Steps You Can Take to Avoid Problems in 2026

Insights
1.05.26

Restaurants have found themselves in the crosshairs of a nascent legal strategy targeting their use of commonplace tracking technologies like pixels, analytics, and session replay tools on their websites. Since 2022, hundreds of eating establishments, particularly those in California, have received demand letters claiming violations of state and federal wiretapping and privacy laws. These legal actions allege that the restaurant's website illegally collected visitor data through these technologies without proper consent, which amounts to illegal wiretapping or use of a "trap and trace" device. Businesses that underestimate the seriousness of this litigation trend and don't follow our five recommended steps may find themselves at the center of a very expensive lawsuit.

Privacy and Wiretapping Lawsuits Gain Traction

While the statutes being used as ammunition in these lawsuits predate the internet, some courts across the country are allowing them to move forward, exposing restaurants to expensive class action litigation and, in many cases, forcing costly settlements. This is part of a larger trend of privacy lawsuits targeting all websites across all industries.

A website is the public's first stop for information when looking for a restaurant's location, menus, hours, and contact information. The nature of how the food industry utilizes websites – to collect delivery addresses, payment information, and email, as well as data for advertising – has made it an easy target for these suits. Thousands of these claims have been filed across the country across all industries, and at least 70 of those lawsuits have been filed against restaurants. In addition to these known lawsuits, it is estimated that hundreds of restaurants have received demand letters or arbitration claims.

> **Want to learn more?** Join us for a webinar with the California Restaurant Association Legal Center on January 15, 2026 to hear from our privacy thought leaders directly.

Consumer Privacy Laws Require Permitting Users to Opt-out Of Tracking And Targeted Advertising

The California Consumer Privacy Act (CCPA), as well as 18 other similar state consumer privacy laws, generally require an opt-out mechanism for website cookies engaged in targeted advertising and certain types of data analytics. Under these consumer privacy laws, that means businesses are in the clear to allow cookies (or any other tracking software) to begin sharing data with third parties the second (or millisecond) a user accesses their website, so long as the user is provided with a clear and functioning opt-out mechanism. Such opt-out can simply be provided by a link or button on the screen or homepage, usually through a cookie banner as well as in the website's footer.

In other words, the laws that specifically regulate how businesses collect and share data through websites and apps do not require opt-in consent before data is collected and shared through cookies, pixels, beacons, tags, software development kits (SDKs) and other tracking technology, except potentially when the business is knowingly collecting data from minors. They only require notice through a privacy policy link and an opt-out process.

Compliance with Consumer Privacy Laws Is Not a Panacea for Wiretapping Claims: The Plaintiffs' Bar Is Attempting to Create an Opt-in Regime

But even if you are in compliance with the opt-out requirements under the CCPA and other state laws, your website tracking technology could still draw wiretapping litigation under the California Invasion of Privacy Act (CIPA) as well as other state and federal laws. In the Golden State, for example, it's illegal under CIPA to read, attempt to read, or learn the contents of a communication "without the consent of all parties to the communication." That law was enacted in 1967 to place guardrails around wiretapping and eavesdropping, primarily in telephone communications. It was amended in 2015 to bar the use of "pen registers" or "trap and trace" devices absent a court order, tools historically used by law enforcement to gather outgoing or incoming metadata from a telephone line.

But, after a 2022 federal appeals court ruling determined that visitor interactions with websites could be susceptible to third-party interception – and therefore are subject to CIPA or federal wiretapping laws – the floodgates opened. Since then, claims have snowballed, alleging that website tools that monitor visitors' interactions or track keystrokes (like website chatbots, search bars, or analytics) can amount to recording the contents of a communication. Lawsuits contending that software used to receive metadata or device IDs from website visitors (such as social media pixels and tracking software from data brokers) constitute a "pen register" or "trap and trace device or process" have also gained similar traction. The key difference in these types of claims is that wiretapping involves the real time interception of the contents of a communication, while pen registers and trap and trace devices merely collect metadata about the communication and the parties to it.

The central argument made in these lawsuits is that opt-in consent is required before disclosing data to a third party about a user's interaction with a website because of a reasonable expectation of privacy in the information. Plaintiffs claim that third parties use this data to track people across the internet, create an electronic fingerprint that follows users online, sell user data to others, and

target ads to users based on the fact they visited a certain website and what they did there. An opt-out mechanism is ineffective, they argue, because users do not have a chance to consent before at least some of their private data is collected and passed on to third parties; therefore, you can't simply provide an opt-out mechanism and disclose the data sharing in a privacy policy that is linked at the bottom of the webpage.

But the courts have been divided on what information counts as private. Several recent decisions from California federal district courts have ruled that there is no expectation of privacy in IP addresses, device and browser information, and geolocation data (among other identifiers), and thus individuals can't be harmed by the data collection. But, the Southern District of California recently split from that trend, greenlighting a case after determining that website-based trackers can be considered pen registers, without addressing other conflicting case law. And numerous other state and federal courts have declined to dismiss these claims, even in cases where expensive discovery later confirms the lack of any factual merit in the claims.

What Restaurants Can Do

Restaurants can take several steps to help shield themselves from these types of lawsuits.

1. California-based restaurants should consider adopting an opt-in consent framework for all non-essential third-party cookies or other tracking technologies on their websites and apps. This would mean that no third-party software, cookie, pixel, tag, beacon, or similar tracking technology would be collecting data or have data disclosed to it until a user has affirmatively opted in through a cookie banner. While opt-in consent is not required by the CCPA and most other states' comprehensive consumer privacy laws, the plaintiffs' bar will continue to assert digital wiretapping claims against restaurants on the premise that wiretapping laws require opt-in consent.

2. Consider strategies specific to high-risk states. While the above step can be implemented in all jurisdictions, it can also be scaled back to apply only in high-risk states like California, Pennsylvania, New York, Florida, and a few others where this type of litigation has taken off. For example, California accounts for approximately 85% of all lawsuits alleging privacy violations based on use of tracking technology on websites and apps. One state-specific strategy could be to geofence your website to scan for visitors from California (or other high-risk states) to ensure no data is shared with third parties until the user opts in.

3. Restaurants should frequently test the consent management banners on their websites to ensure they are functioning properly, especially after website updates. Your business is responsible for ensuring that the opt-out mechanism actually works as intended. Consider hiring an independent third-party engaged through outside counsel (for attorney-client privilege purposes) to regularly test your cookie consent process – you can't rely on your website operator or consent management platform alone. It could be considered an unfair business practice in addition to a violation of opt-out rights under certain consumer privacy laws if your tools don't work. One company recently paid $1.55 million to resolve allegations brought by the California's Attorney

General that it allowed consumers to opt-out of tracking cookies but didn't actually implement their preferences.

4. Programming a website to only share data after a delay could also potentially protect businesses from wiretapping claims that are premised on real time interception of an electronic communication. Courts have held that wiretapping requires having a third party access the contents of the communication in transit, not after the fact (i.e., it is like having another person listen in on the call live instead of listening to a recording later). In one case, a San Francisco-based federal judge acknowledged that a 0.2 second delay in transmitting data from a website to a third-party social media platform was long enough to be considered "after" the communication had traveled to its initial recipient. Restaurants should consider programming their websites so that data transmitted from a user to the website's server is not simultaneously made accessible or transmitted to a third party. Rather, it goes to the third party at some point after the user has "communicated" with the website and the data has been stored on the server.

5. Utilize tools to help minimize the ability of litigants to identify the visitor based on the data they collect. For example, URL sanitation technology removes potential identifiers like user IDs or website activity (via redirects) that may be included in a URL, before storing or transmitting URL data to third parties.

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 directly 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 Practice Group or Consumer Privacy Team, or any member of our Hospitality Industry Team.

A version of this Insight is being published in California Restaurant Association's Industry Insights.

Related People

Darcey M. Groden, CIPP/US
Partner
858.597.9627
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

California Litigation and Appellate

Privacy and Cyber

Litigation and Trials

Industry Focus

Hospitality

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Silicon Valley

Woodland Hills