



Be in the Know:
**HOW TO
PROTECT
YOUR
BUSINESS
FROM
PREDATORY
LAWSUITS**

By Kathryn Rattigan and Janet Kljyan, Robinson+Cole



Predatory lawsuits are brought by entrepreneurial litigants (or, sometimes, their entrepreneurial attorneys) not because they believe they have been wronged but rather for the purpose of extracting relatively quick settlements. Recently, there has been an uptick in three types of claims raised in predatory litigations that can affect food and beverage businesses: copyright infringement claims, “trap and trace” claims relating to online data tracking and targeted advertising, and website accessibility claims. It is important for businesses to be informed of these types of lawsuits so they can act efficiently and effectively if they are targeted.

Copyright “Trolling” Claims

Predatory copyright infringement claims are often brought by plaintiffs who purchase the rights to photographs or images and then use technology to “troll” the Internet for uses of those photos or images. This can be a concern for restaurants who use stock images on their websites or food delivery mobile applications, or where their expired licenses to use the images have gone unnoticed.

Under current law, these lawsuits are attractive for predatory plaintiffs for three main reasons. First, a copyright owner could bring a lawsuit for damages for an infringement that has been occurring for many years if they only recently discovered the infringement. For example, if a restaurant has had the infringing image on its website since 2001, but the copyright owner just

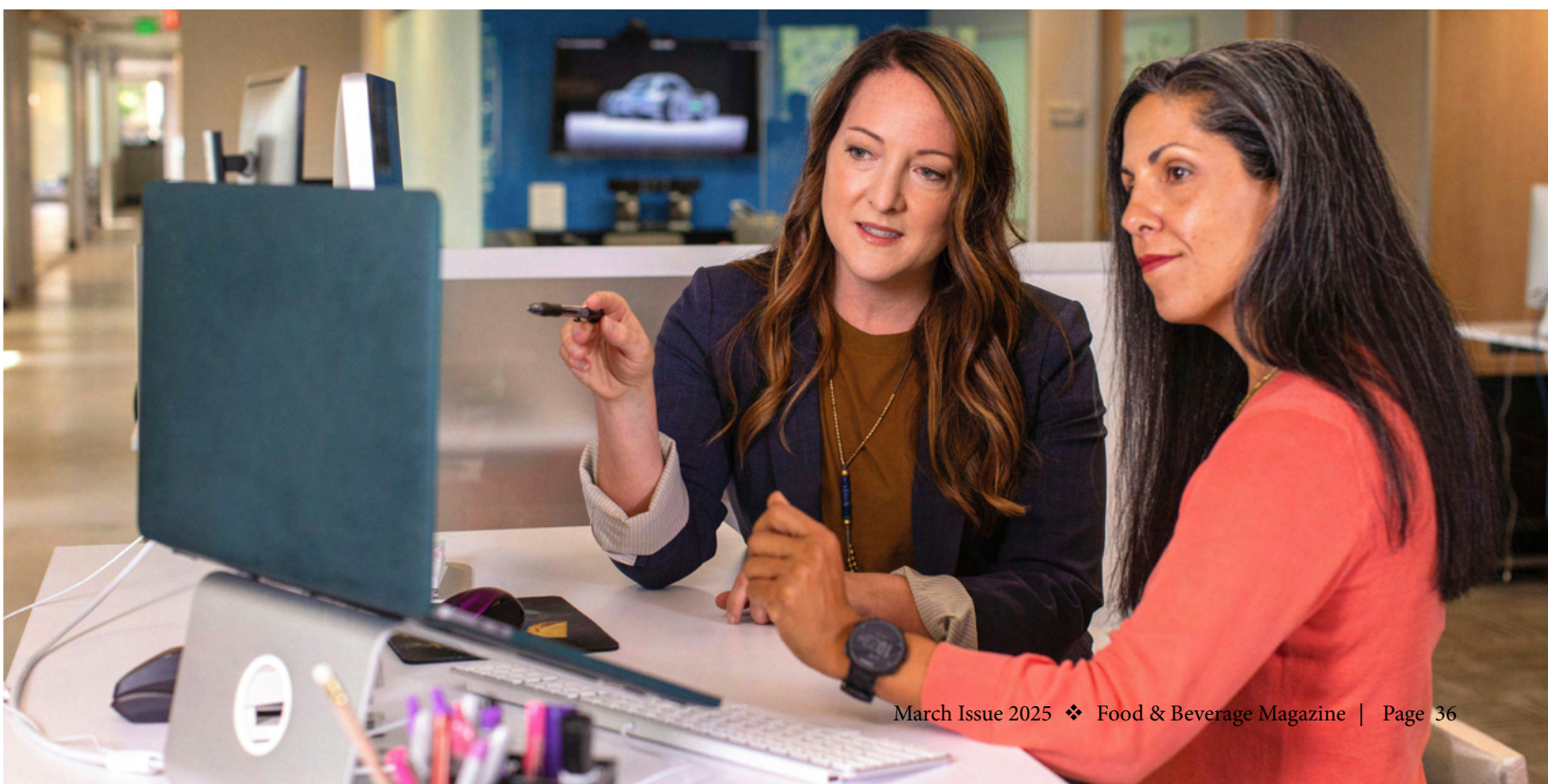
discovered the infringement in 2023, the copyright owner can potentially sue for 25 years’ worth of damages. However, this law has been called into question by recent court decisions.

Second, copyright plaintiffs do not need to provide evidence of damages, since the Copyright Act provides damages of at least \$750 (and possibly much more) for each copyrighted image. Third, the plaintiff’s attorney gets paid a percentage of the damages recovered from the defendant, which means it does not cost the plaintiff any money to carry on with the lawsuit.

Demand letters about copyright claims can be exaggerated and threatening. But the devil is in the details of the copyright and any related licensing rights, which should be reviewed closely.

“Trap and Trace” Litigation

Trap and trace litigation in privacy involves legal proceedings related to the use of devices that capture dialing, routing, addressing, or signaling information from electronic communications. These devices do not capture the content of the communication but identify the source of the communication. Why is a company’s use of such technologies of interest to plaintiffs’ attorneys? The use of these devices may raise privacy issues, as they involve monitoring communication metadata, which can reveal information about individuals’ activities and associations online.



Specifically, many recent claims against the consumer food and beverage industry cite the California Invasion of Privacy Act (CIPA). CIPA prohibits the installation or use of a pen register or a trap and trace device without first obtaining a court order. Law enforcement agencies have historically used pen registers to track the telephone numbers of outgoing calls from a particular telephone line and “trap and trace” devices to record incoming telephone numbers. CIPA specifically 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 reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication.” However, CIPA could apply to website trackers used by nearly all businesses with an online presence.



Lawsuits alleging violations of CIPA typically allude to the following:

The problem with websites using these types of tracking technologies is that it is nearly impossible to provide prior notice or obtain prior consent; websites instantly send communications to third parties as soon as the user lands on the page (even if the cookie consent manager pop-up appears at the same time). Those milliseconds matter.

To protect your company, consider remediating your website by ensuring transparency in your Privacy Policy about the website's data collection practices; obtaining explicit user consent for any tracking activities on your website (i.e., “Accept All Cookies” or “Update My Cookie Preferences”) and implementing a mechanism to allow users to opt-out of tracking for targeted advertising purposes; and regularly reviewing and update your Privacy Policy to reflect current practices.

Also remember that California isn't the only state where these lawsuits hail from; several other states in the U.S. have laws regarding the use of pen registers and trap and trace devices.

INTERCEPTION OF COMMUNICATIONS:

CIPA prohibits the interception of communications without consent. If a website tracker intercepts user communications, such as browsing habits or search queries, without explicit consent, it may violate CIPA.

EXPECTATION OF PRIVACY:

Users have a reasonable expectation of privacy in their online activities. If a website tracker collects data without informing users or obtaining their consent, it could be seen as an invasion of privacy under CIPA.

CONSENT REQUIREMENTS:

Websites must ensure that users are informed about data collection practices and have given consent. Failure to do so can lead to allegations of eavesdropping or unauthorized data collection.

DEVICE FOR EAVESDROPPING:

Tools like Google Analytics, Meta Pixel, and TikTok Web Beacon have been argued to be devices designed for eavesdropping if they collect detailed user information without knowledge or consent, potentially violating CIPA.

The rise in these types of predatory lawsuits stems from the state consumer privacy rights laws popping up across the country (starting in California with the California Consumer Privacy Act/California Privacy Rights Act). To stay ahead of these claims and protect your company, be aware of the requirements under each of these state consumer privacy rights laws and update your Privacy Policy to include all the required disclosures; in particular, any disclosures about data sharing and/or sales, and a user's ability to opt-out of certain types of tracking and data use.

Website Accessibility Claims

When most people think about disability accessibility, they think about buildings that are physically accessible through ramps and automated doors. However, in many cases, digital content, like websites or food delivery phone applications, must also be accessible.

While some website accessibility claims involve legitimate claims, predatory litigations are brought by plaintiffs who do not actually use the website or order on the application. Instead, they are often paid by interested law firms to “test” the website for accessibility and then act as a plaintiff in the lawsuit. Restaurants are frequent targets of these claims because most restaurants have an online presence and ordering function. There has been a steady uptick in these types of lawsuits since 2023 in New York.

Many such businesses run on tight budgets and the plaintiffs gamble on the assumption that the business will prefer to quickly settle the lawsuit rather than spend funds to hire an attorney.

Predatory website accessibility claims usually allege that the website is not accessible to visually impaired or hearing-impaired individuals. Many blind or visually impaired individuals who use the internet to rely on software programs called screen readers that allow the users to read the text that is displayed on the screen with a speech synthesizer or braille display. Websites that are incompatible with this software are arguably inaccessible. Claims related to the hearing-impaired generally allege that video content on websites is not captioned.

The law might be changing for website accessibility claims, as many have questioned whether “testers” have legitimate claims if they have no intention to use that website in the future. These claims are often legally complex, and businesses should be wary of quick settlements that require the business to “fix” the website to be accessible.

Conclusion

It is important for food and beverage businesses who are targeted to be aware that these lawsuits are often predatory in nature. Many such businesses run on tight budgets and the plaintiffs gamble on the assumption that the business will prefer to quickly settle the lawsuit rather than spend funds to hire an attorney. With the help of an experienced attorney, however, these lawsuits can be resolved in the most favorable way to the business.



Kathryn Rattigan

Kathryn Rattigan is a member of Robinson+Cole’s Artificial Intelligence Team and Data Privacy + Cybersecurity Team. She advises clients on data privacy and security, cybersecurity, and compliance with related state and federal laws. Kathryn also counsels clients in assessing risks related to technology and software contracts, as well as with compliance-related issues with outsourcing and vendor management.



Janet Kljyan

Janet Kljyan is a commercial and civil litigator with extensive experience helping businesses and other institutional clients litigate and resolve their disputes across an array of industries, including food and beverage, education, technology, financial services, healthcare, manufacturing, and commercial real estate. She is a member of Robinson+Cole’s Business Litigation Group.