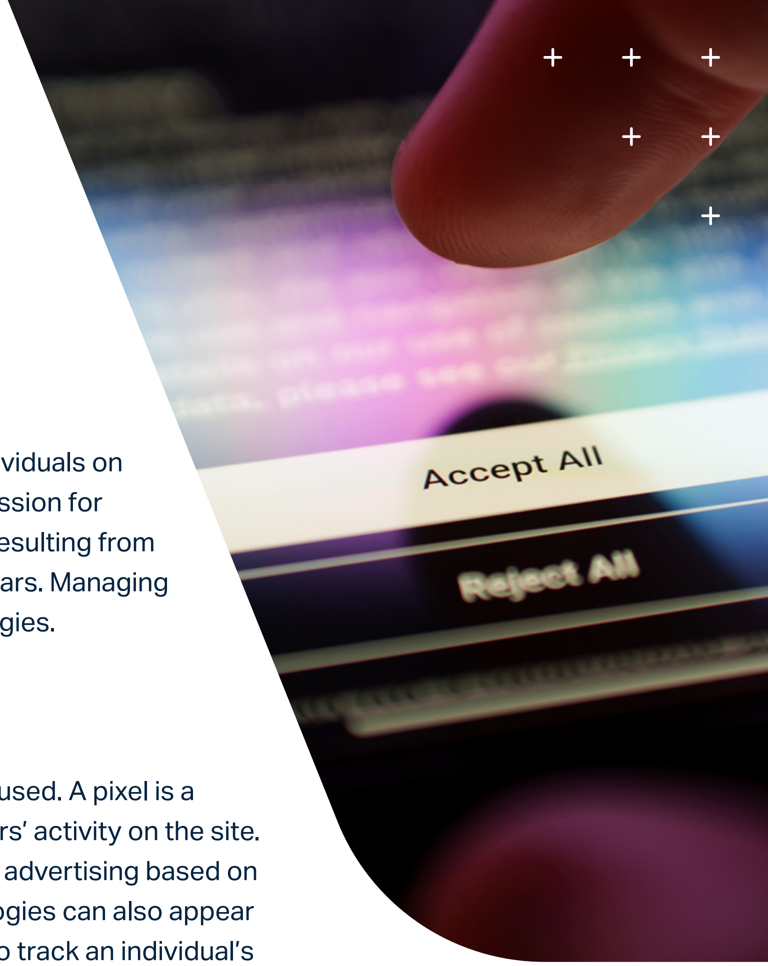
The Growing Risk of **Online Tracking Technologies**



Technologies such as pixels and browser cookies that track individuals on the internet have been an elevated part of the privacy risk discussion for over four years. Claims and lawsuits alleging privacy violations resulting from those technologies have been growing significantly in recent years. Managing that risk is now essential for organizations using those technologies.

Tracking Technologies in More Detail

Pixels are one of the better-known tracking technologies being used. A pixel is a small bit of computer code added to a website that tracks visitors' activity on the site. That information is captured and used to show visitors targeted advertising based on their activity and perceived interests. Pixels and similar technologies can also appear in email and mobile applications. Tracking technologies may also track an individual's browsing activity across the internet.

Organizations may be using tracking technologies without realizing it. Tracking technologies are part of services such as Google Analytics that provide information without the website owner necessarily being aware of how the information is obtained. Likewise, the technologies may be changed or upgraded without notice.

The Current Tracking Risk Environment

Tracking claims and lawsuits are largely premised on the California Invasion of Privacy Act (CIPA), a 1967 law protecting against unauthorized wiretapping and eavesdropping. Modern technologies have broadened the statute's reach, but its purpose to safeguard personal information and privacy remains.

A growing number of CIPA claims allege privacy rights infringement after interacting with a website or app claimants contend has tracking enabled without consent. The law allows consumers to directly sue defendants and carries statutory damages of $5,000 per violation regardless of whether the claimant was harmed.[1] Many of these claims are brought as class action lawsuits, while others are threats of lawsuits, with claimants seeking quick settlements.

A growing number of CIPA claims are brought by serial plaintiffs. One notable serial claimant is a former actor, Vivek Shah. Mr. Shah visits organizations' websites and then alleges privacy violations based on their use of tracking technologies. Estimates indicate he has brought thousands of claims since the Fall of 2024. He is not alone, as this is a cottage industry that may grow as states adopt restrictive privacy laws. Recipients have found many of these claims frivolous, and courts are starting to agree. In July of 2026 the U.S. District Court for the Central District of California found Vivek Shah's litigation activity to be frivolous and harassing, and declared him to be a vexatious litigant.[2]

Responding to Online Tracking Claims

If your organization receives an online tracking claim, it must be taken seriously. Do not respond directly. Instead, report the claim to your insurers and work with them to retain legal counsel with experience handling such claims. Counsel may recommend ignoring any demands until a lawsuit is filed. You should not delay reporting the demand to your insurers. Doing so may jeopardize any available coverage.

WHAT INSURANCE POLICIES MAY COVER A TRACKING CLAIM

A cyber policy is the best bet. That policy is designed to cover privacy claims. However, coverage is by no means certain. While coverage for any insurance claim depends on the facts alleged, if a cyber policy does not cover claims based on the wrongful collection of information (many don't), then it is likely the policy will not cover the online tracking claim.

A directors and officers liability policy might cover a tracking claim if it includes coverage for the organization, the scope of coverage is broad enough to include the allegations made, and there is no exclusion pertaining to privacy violations. D&O policies can include endorsements adding absolute cyber/privacy exclusions.

Errors and omissions policies conceivably could cover a tracking claim if the tracking was part of a professional service provided by the insured. Exclusions for cyber events and intentional acts may affect the existence or extent of any available coverage.

Personal and advertising injury coverage in commercial general liability (CGL) policies may be triggered by an online tracking claim. Unfortunately, many CGL policies are now issued with absolute cyber/privacy exclusions that are likely to defeat coverage. Other exclusions may apply as well.

Managing the Risk

Online tracking claims succeed because the defendant organization does not require individuals' consent before they are tracked online. Those wishing to avoid tracking claims must disclose that tracking takes place on the website and obtain consent. The most frequently recommended steps for organizations to take are:

1. Understand and catalogue any tracking technology that your organization is using. It is not uncommon for the marketing department to utilize these solutions without leadership being aware. There are a number of websites that will examine a URL and report on any tracking technologies found. While we cannot endorse the accuracy of any such site, Blacklight by The Markup[3] is one that is commonly used.
2. Ensure that tracking is fully addressed in the organization's publicly available privacy policy.
3. Display a banner on the website that informs each visitor that tracking takes place and asks for visitors' consent by requiring them to click "yes" or "no".
4. Avoid any tracking before consent is given.
5. Regularly check that tracking technologies are performing consistently with the organization's privacy policy and consent provisions seen by site visitors.
6. Review the privacy policy on a regular basis and when new tracking technologies are deployed to make certain the policy completely describes the tracking taking place and the organization's policy to allow site visitors to grant or withhold consent.

Final Thoughts

Online tracking data is valuable to the organizations that ensure it is captured. That tracking will continue to raise significant privacy concerns that are addressed in consumer privacy laws. The tension between the two will continue to result in online tracking claims. Organizations concerned about such claims must take steps to manage the risk. It is also incumbent on organizations to conscientiously monitor and comply with new and updated laws affecting their obligations to users being tracked. Not taking these steps will significantly increase exposure to privacy claims.

AUTHORS

WILLIAM BOECK

EVP, Cyber Product Leader

BRET OMMODT

VP, Senior Claim Executive

SOURCES

1. Jodka, Sara H. (2026, April 13). *Your website is a satisfying target: What you need to know about pixel-tracking litigation in 2026.* Reuters. https://www.reuters.com/legal/legalindustry/your-website-is-satisfying-target-what-you-need-know-about-pixel-tracking--pracin-2026-04-13/
2. Oberly, David J., and White, Matthew G. (2026, July 24). *California Federal Court Declares Serial CIPA Plaintiff Vivek Shah a Vexatious Litigant: What You Need to Know.* Baker Donelson. https://www.bakerdonelson.com/california-federal-court-declares-serial-cipa-plaintiff-vivek-shah-a-vexatious-litigant-what-you-need-to-know
3. Blacklight. (n/a). *Blacklight: A Real-Time Website Privacy Inspector.* The Markup. https://themarkup.org/blacklight