EPIC
Insurance Brokers & Consultants

PROFESSIONAL, EXECUTIVE AND CYBER SOLUTIONS

Navigating the Continuing Surge of VPPA & CIPA Lawsuits

In early 2022, opportunistic plaintiffs' attorneys began an aggressive legal campaign targeting businesses that utilize the Meta Pixel and other standard digital marketing tools that track website visitor activity. This strategy relies on weaponizing two pre-internet statutes—the 1988 Video Privacy Protection Act (VPPA) and the 1967 California Invasion of Privacy Act (CIPA)—and applying them to modern web analytics, tracking tags, and session-replay scripts. Because these statutes carry steep statutory damages of $2,500 to $5,000 per violation, the financial stakes for businesses can be high.

This litigation model gained significant momentum through 2023 and 2024, resulting in thousands of claims. Today, CIPA and VPPA lawsuits continue to surge, plaguing companies of all sizes across virtually every industry. Businesses and professional service firms are currently still facing an influx of pre-litigation demand letters, draft complaints, and class-action lawsuits. Court rulings across jurisdictions vary wildly, making these cases expensive to defend against with unpredictable and inconsistent outcomes.

VPPA Lawsuits: Targets companies that embed video content on their websites while using third-party tags like the Meta Pixel. Plaintiffs allege that transmitting a user's video-watching history alongside identifiers (like a Facebook ID or IP address) without specific standalone consent violates the VPPA. Primary target companies include traditional media companies, streaming services, retailer, and sports and entertainment companies.

CIPA Demand Letters: Targets businesses utilizing standard website cookies, analytics, and chat features. Serial plaintiffs (such as Vivek Shah) send pre-litigation demands, claiming that everyday data transmission (like text typed into a search bar) to third parties constitutes an unlawful wiretap or unauthorized use of a "pen register" or "trap and trace" device. Primary targets for CIPA demand letters and lawsuits include consumer-facing companies in the healthcare, finance, and technology space and professional service firms (accounting and law).

Given VPPA and CIPA claims are continuing to surge, businesses and firms should proactively seek to mitigate their risk.

Practical Risk Mitigation Tips:

- Proactively Audit Website Tracking Technologies
  Map out all deployed pixels, tags, and other tracking tools across your websites and email domains. Website developers often incorporate tracking technologies into websites without considering potential legal and regulatory compliance risks. The audit should identify every tool, its activation triggers, the data it collects, and the final destination of that data. Focus on high-risk features like session replay software, search bars and AI chatbots. These features tend to pose a higher risk to user privacy and cybersecurity than static pages.

- Review and Refine Consent Mechanisms
  Websites must obtain clear, legally valid consent from users before tracking them. Users must be presented with an appropriate privacy notice and actively consent to data collection. Review the consent mechanisms now to ensure legally defensible notice and consent workflows are in place *before* any tracking tool initiates.

- Update Public Privacy Policies
  Explicitly and transparently disclose the use of session replay software, analytics, and third-party tracking networks in your public facing Privacy Policy and ensure they are consistent with actual practice. Discrepancies between public claims and actual technical operations often serve as the foundation for demand letters and class-action complaints.

- Consider Isolating California Web Traffic
  One way to mitigate California Invasion of Privacy Act (CIPA) wiretapping risk is to segregate or geofence incoming web traffic from California IP addresses. Consider suppressing pixel and session replay deployment entirely for these users. While this may somewhat limit your California marketing data, it will significantly reduce your exposure to CIPA litigation.

- Review Risk Transfer Mechanisms
  Carefully audit and review your insurance portfolio and vendor contracts with this specific risk in mind. Review relevant vendor indemnification and insurance requirement provisions and consider your own insurance protection. Keep in mind, many cyber insurance policies contain Web Tracking Exclusions or Wrongful Collection Exclusions.

- Consider Coverage Mapping and Insurance Notifications
  If coverage is not available under your cyber policy due to an exclusion, consider whether there are other sources of coverage for these types of claims – for example, a professional liability (E&O) or management liability policy (D&O). Map out all potential sources of recovery now so you can immediately file appropriate and required notices. Although all policies contain unique definitions of "Claim", most definitions would encompass lawsuits as well as demand letters and draft complaints. Closely review and understand the notification requirements of your policies so you do not jeopardize insurance recovery.