Shumaker

JUNE 29, 2026 | PUBLICATION

Client Alert: Your Website May Be a Lawsuit Waiting to Happen: The CIPA Demand Letters Flooding Businesses

A website feature need not resemble surveillance technology to become the subject of a privacy lawsuit.

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

C. Jade Davis
Brian C. Focht

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Businesses are increasingly receiving lawsuits and pre-litigation demand letters alleging that ordinary website tools violate the California Invasion of Privacy Act (CIPA)—tools such as analytics software, advertising pixels, cookies, session replay technology, chat functions, search bars, and online forms.

Many of the newest claims argue that these tools operate as unlawful "pen registers" or "trap-and-trace devices." Others allege that a website unlawfully intercepted information typed into a search field or form before transmitting it to a third party.

Our firm has seen a rise in reports from clients receiving lawsuits or demand letters, often involving claims by Vivek Shah. These include demands for informal resolution, proposals for payment, and draft complaints threatening litigation.

The fact that these demands often follow a similar format does not mean that businesses should ignore them, nor does it mean that every demand is legally or factually valid.

A standardized demand still requires a serious response. It does not prove a valid claim nor does it justify silence or an automatic payment.

The better approach has two parts:

1. Address the immediate claim. Seek dismissal, withdrawal, or a favorable resolution.
2. Correct the website activity behind the claim. Reduce the risk of another demand from a different serial plaintiff.

Why Ordinary Website Tools Are Being Called Wiretaps

For a more thorough discussion of the California Invasion of Privacy Act and its application to website interactions, see our previous Client Alert on the subject: The California Invasion of Privacy Act Meets the Modern Web: What Businesses Need to Know Now.

CIPA predates commercial websites, analytics platforms, and digital advertising. Plaintiffs now apply its language to modern website technology.

Two theories appear frequently in the demands and complaints now being sent:

1. ***Claims Based on Website Communications***

Section 631(a) of CIPA generally prohibits unauthorized interception or reading of a communication while it is in transit. Recent claims allege that third-party code embedded in a website intercepts information entered into a search bar, chat window, contact form, job-search field, or similar feature.

A visitor may type a name, health-related term, employment phrase, or product search into a website. Embedded code may send the entry to Google Analytics, Meta, HubSpot, an accessibility vendor, or another service provider. A demand may call that transmission an unlawful interception.

Many recent demands involving Mr. Shah rely on this theory.

2. ***Pen-Register and Trap-and-Trace Claims***

A separate group of claims relies on Sections 638.50 and 638.51 of CIPA. Section 638.51 generally prohibits installing or using a "pen register" or "trap-and-trace device" without a court order, subject to several exceptions, including certain uses by communications providers.

Traditional pen registers captured information about outgoing telephone calls. Traditional trap-and-trace devices identified the source of incoming calls. Plaintiffs now compare website tracking tools to digital versions of those devices.

The disputed data often includes:

- Internet Protocol addresses;
- Browser and device identifiers;
- Referring URLs;
- Cookies and advertising identifiers;
- Approximate location data;
- Timestamps;
- Page navigation activity; and
- Information used for a device fingerprint or user profile.

What Sets CIPA Apart

CIPA permits a private plaintiff to seek the greater of $5,000 per violation or three times actual damages. The statute does not require proof of actual monetary loss for the statutory remedy. Plaintiffs often use this damages provision to create settlement pressure. Some demand letters also allege a separate violation for each visit, transmission, or tool activation.

The Law Remains Unsettled

Courts have not reached a uniform answer on whether ordinary website technologies qualify as pen registers or trap-and-trace devices.

Some courts have dismissed these claims, particularly when the complaint involves only an IP address or information necessary for the basic operation of a website, including a recent case brought by Mr. Shah. Mr. Shah has appealed that decision.

Other courts have allowed claims to proceed when the technology allegedly collects additional device information, creates a persistent fingerprint, builds a profile, or sends information to third parties for advertising or analytics purposes.

The result is an inconsistent body of trial-court decisions. Outcomes often turn on the exact data, the recipient, the purpose, the tool configuration, and the consent process.

There are defenses to these claims, both procedural and substantive. A strong defense can reduce exposure, but it cannot erase response costs. A business may still face evidence preservation, technical analysis, motion practice, insurance notice, vendor disputes, and internal disruption.

We recommend proceeding on two parallel tracks:

Track One: Resolve the Immediate Demand or Lawsuit

The first objective is to evaluate and contain the matter before it affects the business.

Our firm can review the demand, draft complaint, website configuration, and available evidence to determine what information was actually collected and whether the claimant's allegations align with the site's operations. Relevant issues may include:

- What information the claimant entered into the website;
- Whether and when the information was transmitted to a third party;
- Whether the alleged transmission involved communication content or only technical metadata;
- Whether the relevant technology was active at the time of the visit;
- Whether the claimant received notice or provided consent; and
- Whether the claimant can establish standing or jurisdiction, among others.

Businesses should preserve relevant evidence before changing the website. That evidence may include tag management configurations, consent platform settings, analytics records, website versions, vendor documentation, server logs, and records showing when particular scripts were installed or removed.

Preservation does not mean that a known problem must remain active. It means the business should document the existing configuration before making changes, so it can later establish what the website did and did not do during the relevant period.

Our firm can also communicate directly with Mr. Shah or other claimants and attempt to resolve the matter. We have successfully negotiated outcomes ranging from reduced settlement amounts to complete withdrawal of the demand. The appropriate strategy depends on the strength of the allegations, the available defenses, the cost of litigation, and the company's broader risk profile.

No particular result can be guaranteed, but an informed response is generally more effective than ignoring the demand, paying it without investigation, or allowing uncoordinated communications between the claimant and company personnel.

Track Two: Eliminate the Website Activity That Created the Risk

Resolving one demand does not prevent another claimant from visiting the same website and raising the same allegation.

The second part of the response, therefore, focuses on the underlying website.

A useful review should identify:

Every Script and Tool Used. This includes analytics tools, advertising pixels, chat software, session replay tools, accessibility tools, embedded videos, social media integrations, form processors, tag managers, and scripts added by marketing agencies or other vendors.

The information each tool receives. The review should determine whether a tool receives only basic page information or also receives search terms, form entries, full URLs, user identifiers, device fingerprints, account information, health information, employment information, or other potentially sensitive data.

When the tool begins collecting data. A cookie banner does not reduce risk if the relevant scripts load and transmit information before the visitor has an opportunity to make a choice.

Whether the site honors the visitor's selection. The website should be tested after the visitor accepts, rejects, or customizes tracking. The technical operation must match the language displayed to the visitor.

Whether each tool is necessary. Businesses often discover scripts that are outdated, duplicative, improperly configured, or no longer used. Removing unnecessary tracking is frequently the simplest and most defensible control.

Whether sensitive pages receive additional protection. Search fields, login pages, checkout pages, patient portals, job applications, financial forms, and contact pages may require different configurations than ordinary informational pages.

Whether notices and contracts match reality. Privacy disclosures should accurately describe the tools in use and the information disclosed to vendors. Vendor agreements should address permitted data use, security, cooperation with claims, indemnification, and responsibility for configuration changes.

A privacy policy is not a magic shield; it is evidence of the company's public statements. Inaccurate language can increase risk rather than reduce it.

Do Not Wait for a Legislative Fix

California lawmakers have considered legislation, including SB 690, that would include a proposed commercial business purpose exception for certain website data processing. Proposed legislation, however, does not resolve an existing demand or excuse current non-compliant site practices.

Businesses need a response based on current law and current site behavior.

What Businesses Should Do Now

A business with a CIPA demand should take several immediate steps:

1. Route the matter to legal counsel.
2. Calendar every response deadline.

3. Preserve website and vendor evidence.
4. Notify relevant insurers.
5. Limit direct communications with the claimant.
6. Document the current website configuration.
7. Begin a focused technical review.
8. Correct the risky activity.
9. Update notices, consent tools, and vendor terms.
10. Retest the site and preserve proof of the changes.

The legal response and the technical response serve different purposes. The legal response addresses the current claimant. The technical response reduces repeat exposure.

A business needs both.

Proactive Steps for Businesses That Have Not Yet Received a Demand

Businesses do not need to wait for a demand letter to reduce their exposure. The following steps can help identify and address website risks before they become litigation.

1. *Immediate Risk Assessment*
    - Conduct an internal audit of all third-party scripts, pixels, and tracking tools currently active on your website.
    - Identify which website features collect user input—such as search bars, chat functions, forms, and job applications—and determine where that data is transmitted.
    - Review whether your cookie consent banner actually blocks tracking before a visitor makes a selection. A banner that loads after scripts have already fired provides limited protection.
2. *Insurance and Documentation*
    - Review cyber liability and general liability policies for potential coverage of CIPA claims before a demand arrives.
    - Maintain historical records of website configurations, including screenshots and tag manager exports, to establish a defense timeline if a claim arises.
3. *Vendor Management*
    - Audit vendor contracts for indemnification provisions, cooperation requirements, and data use restrictions.
    - Identify which vendors have access to visitor data and confirm their data handling practices align with your privacy disclosures.
    - Remove or disable any third-party tools that are outdated, duplicative, or no longer necessary. Eliminating unnecessary tracking is often the simplest risk-reduction measure.
4. *Privacy Compliance Enhancements*
    - Ensure your privacy policy accurately describes every tool collecting visitor data. Inaccurate disclosures can increase risk rather than reduce it.
    - Apply heightened protections to sensitive pages, including login portals, checkout pages, patient portals, job applications, and financial forms.
    - Test your website after visitors accept, reject, or customize tracking to confirm the site behaves as promised.
5. *Proactive Legal Posture*
    - Establish a response protocol so that any CIPA demand is immediately routed to legal counsel rather than handled by internal personnel who may inadvertently make damaging admissions.
    - Do not assume a templated demand letter is invalid but also do not pay without investigation. A

serious response is required regardless of the format.
    - Consider proactive website remediation now, rather than waiting for a demand, to reduce the risk of repeat exposure from multiple claimants.

The Bottom Line:

The current wave of CIPA demands turns ordinary website technology into an expensive litigation risk. The law remains unsettled. Many claims face meaningful defenses. The defense still costs time, money, and attention.

Our firm can assist with both parts of the response. We can negotiate or defend the immediate claim and identify and eliminate the website activity behind the demand. Our team has obtained outcomes ranging from reduced penalties to withdrawal of the demand.

A two-part response can reduce the cost of the current matter and lower the risk of the next one.

Contact Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line today to discuss how we can help your business respond to a CIPA demand and reduce the risk of future claims.

Shumaker