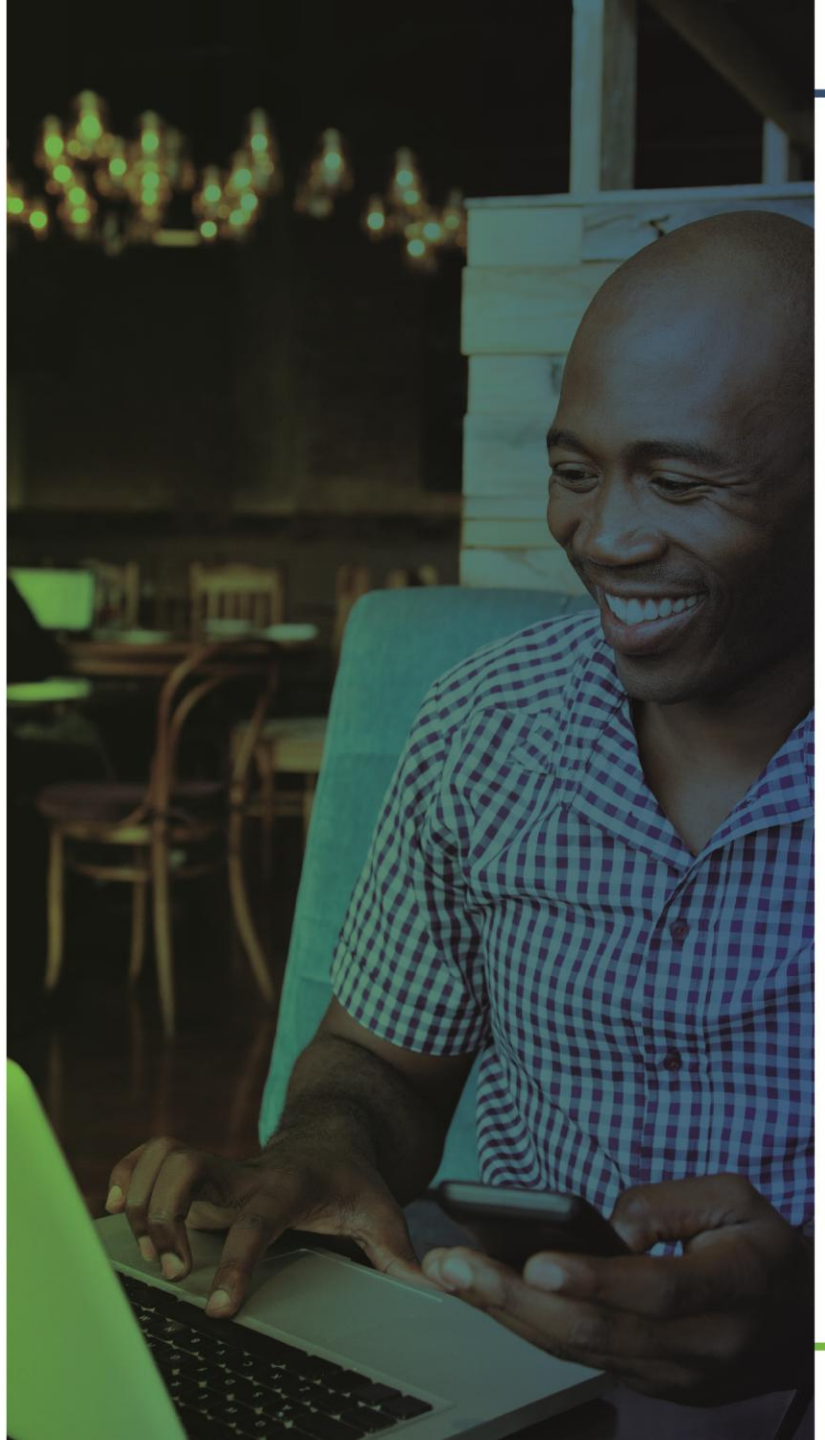


# You've Got Mail:
# From a Serial Privacy Plaintiff
## (A Privacy Pro's CIPA Playbook)

**Thursday, 10 September**
08:00–09:00 PDT
11:00–12:00 EDT
17:00–18:00 CEST

# Welcome & Introduction

Alex Proctor
AIGP, CIPP/E, CIPP/US, CIPM, CIPT, FIP
Chief Trust & Privacy Officer
Captain Compliance

www.captaincompliance.com

# One Month Ago…
# a Federal Court Had Enough!

*"…Plaintiff's purpose is to harass defendants into coercive settlements — rather than seek redress from the judiciary in good faith."*

(C.D. Cal., July 20, 2026)

*Reference: Order, Shah v. Crain Commc'ns, Inc., No. 2:26-cv-03070-RGK-CTS (C.D. Cal. Jul. 20, 2026)*

# Three Key Topics for This Hour

1

**What did the vexatious litigant ruling change, and what isn't changing?**

The July order partially restricts the CIPA wave's most prominent filer, but it's not the end of the story. The demand letters, arbitration pathways, and copycat filers are all likely to continue to challenge businesses.

2

**Is the CIPA claim in my inbox a real risk to my business?**

Most tested Shah-style claims failed on standing or the pleadings, but the theories behind them are not frivolous. We'll cover how to evaluate a letter's actual merit before deciding how, or whether, to respond.

3

**My website isn't very defensible...what do I fix first?**

CIPA claims are built on a handful of theories, mostly involving how your website shares data, how consent is enforced, and whether your notices are accurate. Close your gaps to avoid being targeted by serial filers.

# Web Tech & Litigation Risk

- **Litigation risks** stemming from tracking technologies, consent failures, and misrepresented privacy practices are amongst the most significant privacy risks.
- Opportunistic plaintiff's attorneys are targeting organizations at an unprecedented pace, targeting businesses across a wide variety of industries.
- Privacy lawsuits are leading to **multimillion-dollar settlements**, reputational damage, and significant operational disruptions - even when settled early.
- Businesses of all sizes face litigation risks - unlike the modern privacy laws, there are no revenue or processing thresholds to limit exposure.
- Privacy litigation risk cannot be completely eliminated, but it can be **greatly reduced** through the proactive management of simple privacy practices and controls.


THE NATIONAL
LAW REVIEW

**Pixel-Tracking Gets its Third Stripe: Adidas Learns CIPA isn't Optional**

by: Keerti Jaya
Troutman Amin, LLP

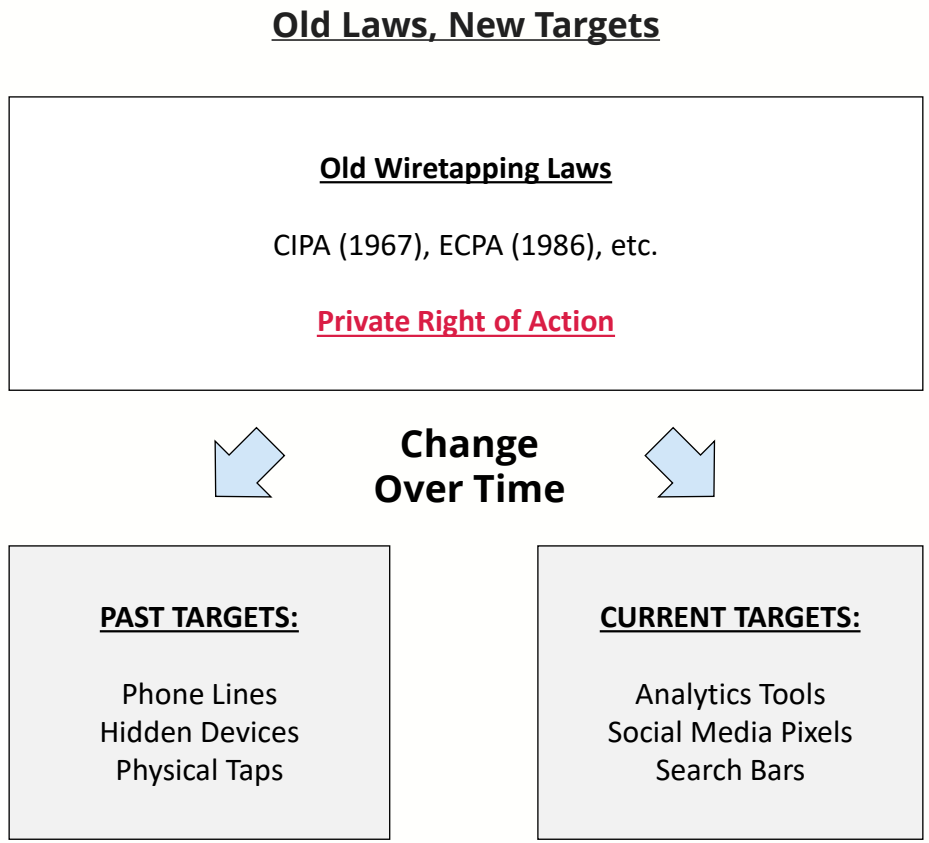
*Reference: https://natlawreview.com/article/pixel-tracking-gets-its-third-stripe-adidas-learns-cipa-isnt-optional*

# Compliance Risk v. Litigation Risk

| Consideration | U.S. Privacy Regulation | U.S. Privacy Litigation |
|---|---|---|
| **Scope of Applicability** | **Narrower:** State-level privacy laws apply to businesses meeting specific revenue or data processing thresholds, often with exemptions for certain industries. | **Broader:** Plaintiffs can generally target any organization handling consumer data - regardless of size or industry - if there is a perceived violation of privacy rights. |
| **Enforcement Likelihood** | **Lower:** Enforcement is increasing, with state agencies actively pursuing violations. However, enforcement is less frequent than litigation and some states allow cure periods. | **Higher:** Privacy-related class lawsuits are common and filed frequently, often in response to improper data sharing. Certain litigators have a strong financial incentive. |
| **Financial Impact** | **Lower:** Fines for non-compliance can be substantial (often $7,500 per violation). However, the largest penalties to-date are much lower than that of largest litigation settlements. | **Higher:** Class action settlements can be extremely costly, with some settlements costing tens of millions of dollars in high-profile data cases. Legal fees add to the burden. |
| **Reputational Impact** | **High:** Regulatory enforcement actions can damage an organization's reputation, especially when high-profile misuse allegations are highly publicized by state regulators. | **High:** Lawsuits can damage an organization's reputation, especially with high-profile data misuse allegations. Litigation can also lead to sustained public backlash. |
| **Overall Risk** | **Lower:** The risk of regulatory action is growing as more states enact privacy laws, but enforcement is still inconsistent, and smaller organizations may avoid scrutiny. | **Higher:** Privacy lawsuits are both common and expensive. Most organizations are viable targets, and many have website privacy gaps that can be exploited by litigators. |

# Old Wiretapping Laws? But…Why?

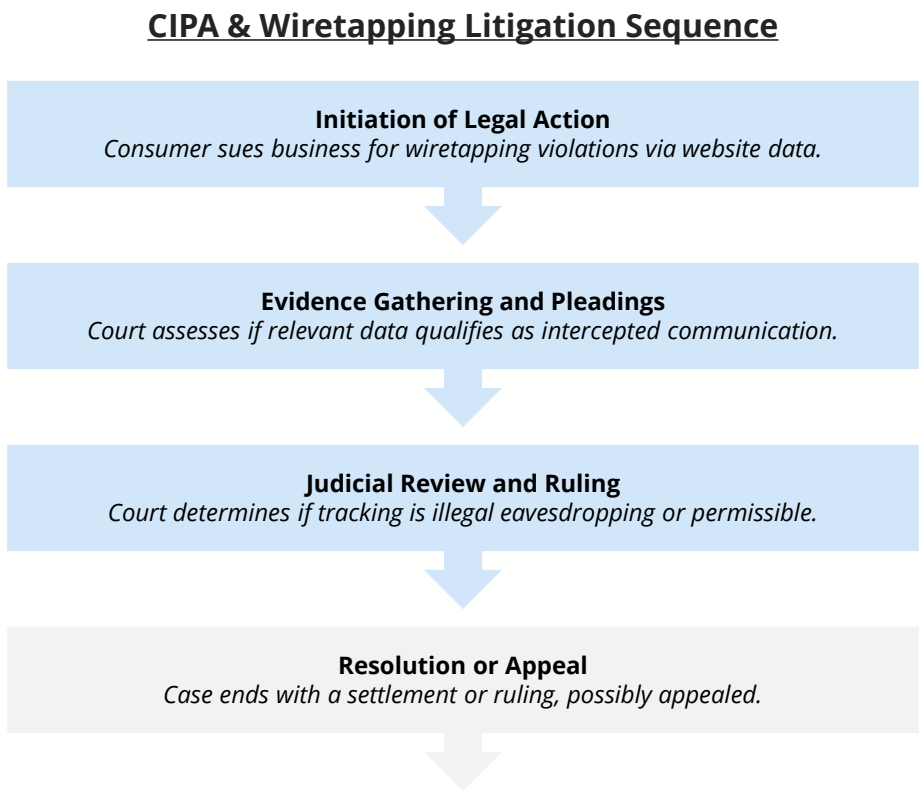
- **Wiretapping laws** (like California's CIPA) are at the center of hundreds of website-related lawsuits targeting tools like pixels, chatbots, and analytics.
- Ironically, these decades-old laws are being applied to modern tracking technologies despite being written long before the Internet existed.
- Plaintiffs' attorneys favor wiretapping statutes because they include a private right of action, which most of the modern privacy laws do not include.
- With limited enforcement options under modern laws, wiretapping claims have become a key legal pathway for **challenging website practices**.
- There has been a surge in wiretapping lawsuits against websites, and the long-term viability of these claims remains uncertain as courts issue conflicting rulings.




*References: Cal. Penal Code §630 et seq. (1967); 18 U.S.C. §2510 et seq. (1986); 18 U.S.C. §2710 (1988)*

# CIPA: Californian Wiretapping Law

- The **California Invasion of Privacy Act** (CIPA) is a 1960's wiretapping law at the epicenter of modern website privacy litigation, with over a thousand lawsuits filed since 2022.
- CIPA prohibits the unauthorized interception of communications, and courts have allowed claims that third-party tracking tools function as digital wiretaps when not properly disclosed.
- The law provides statutory damages of **$5,000 per violation**, which can escalate quickly in class actions if each website visit is treated as a separate offense.
- Courts are divided on how CIPA applies to website tracking, with inconsistent rulings on whether session data, clickstream events, or metadata count as intercepted communications.



# Frequently-Cited CIPA Sections

| CIPA Section | CIPA Section Summary | Modern Considerations |
|---|---|---|
| **631(a)(i)** | Prohibits intentional tapping of any telegraph, telephone wire, line, cable, or (...) communication system instrument. | 1. Using session replay tools may be seen as illegal wiretapping if not disclosed.<br>2. Clearly inform users about tracking tools and offer an opt-out to reduce risk. |
| **631(a)(ii)** | Prohibits unauthorized interception and reading of any message, report, or communication contents while in transit. | 1. Tracking real-time user data (mouse movements, etc.) may be seen as an interception.<br>2. Some courts may allow tracking of metadata, like IP addresses and timestamps. |
| **631(a)(iii)** | Prohibits use of intercepted communication contents without authorization. | 1. Using data from trackers without user consent can lead to liability.<br>2. If the data is only used to benefit the business, CIPA may not apply. |
| **631(a)(iv)** | Prevents a party to the communication from aiding or abetting a third party in committing the above prohibited acts. | 1. You may be liable if your tools help others intercept user data without consent.<br>2. Limit what third parties can do with user data to avoid aiding illegal tracking. |
| **632(a)** | Requires consent from all parties before recording any confidential communications | 1. Not getting consent before recording interactions (e.g., via chatbots) can violate CIPA.<br>2. Use opt-in tools to reduce legal risk and improve compliance. |
| **638.51(a)** | Prohibits use of a pen register without a court order or the user's prior consent. | 1. Tracking IP addresses or device fingerprints may count as using a pen register.<br>2. Courts might dismiss if the data isn't personal or the plaintiff lacks standing. |

*Reference:* https://iapp.org/resources/article/us-litigation-series-website-tracking/

# ECPA: Federal Wiretapping Law

- The **Electronic Communications Privacy Act** (ECPA) is a federal law passed in 1986 that protects against unauthorized interception and access to electronic communications such as phone calls, emails, and certain internet activity.
- ECPA is cited less frequently in website tracking lawsuits because it allows one-party consent, making it harder to claim unlawful interception.
- Unlike California's CIPA, which requires all-party consent and provides statutory damages, ECPA offers fewer remedies and may be less optimal for litigators. Still, it is called upon regularly.
- Like CIPA, ECPA's protections were written before the rise of modern web technologies, which has led to growing criticism that the law is outdated and poorly suited to today's digital privacy risks.

**CIPA vs. ECPA**

| Feature | CIPA | ECPA |
|---|---|---|
| **Relevant Jurisdiction** | California Law | Federal Law |
| **Consent Standard** | All-Party Consent | One-Party Consent |
| **Web Privacy Litigation** | Extremely Prominent | Often Paired with CIPA |
| **Statutory Damages** | $5,000/Violation / Actual Damages | $100/Day / Actual Damages (Max $10,000 /Violation) |
| **Private Right Of Action** | Yes | Yes |

# CIPA Case Law Foundations

- In **Javier v. Assurance IQ** (9th Cir. 2022), the court held that consent must be obtained before recording begins; and that retroactive consent is invalid.
- In **Yoon v. Lululemon** (C.D. Cal. 2021), the court held that embedded session-replay vendors can be third parties; aiding-and-abetting claims under §631(a)(iv) were allowed to proceed.
- In **Greenley v. Kochava** (S.D. Cal. 2023), the court held that software could function as a pen register under §638.51; no physical device is required, opening the door to claims over metadata logging.
- Together, these rulings handed serial filers a repeatable template; consent timing, third-party status, and pen registers can survive early motions, which creates settlement leverage.

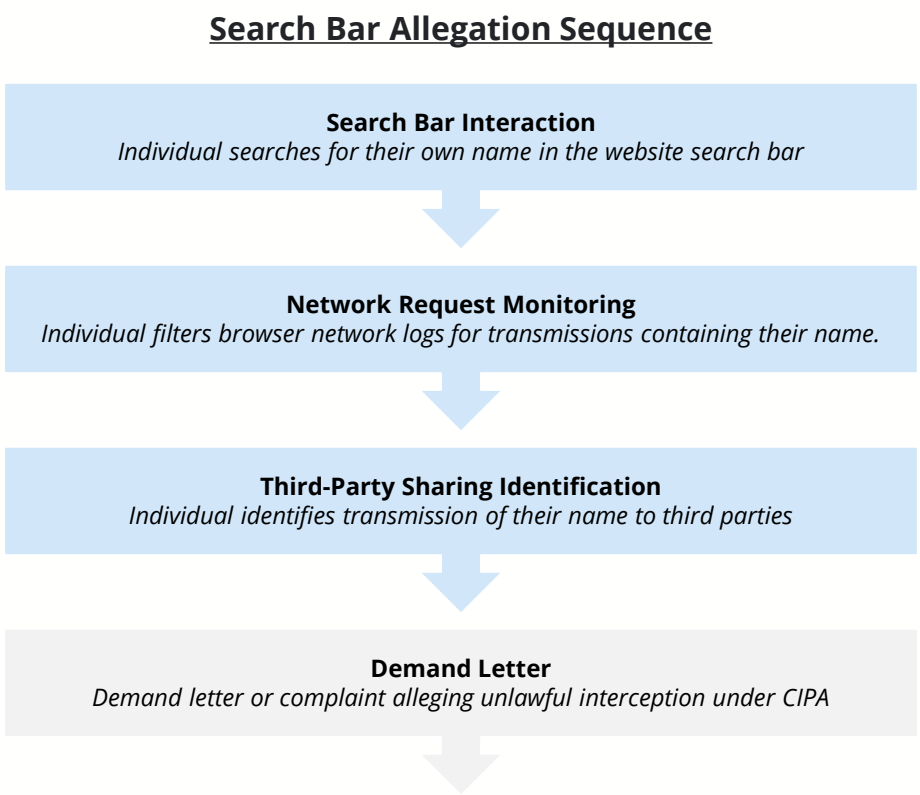
**Three Notable CIPA Cases**

| Case | How Serial Filers Use the Case Law |
|---|---|
| **Javier v. Assurance IQ** | Serial filers use Javier to attack consent timing. If any tracker fires before the visitor accepts the banner, the letter frames that data flow as a wiretap that later consent cannot cure. **This sits in direct tension with the opt-out defaults that modern U.S. privacy laws generally allow for.** |
| **Yoon v. Lululemon** | Serial filers use Yoon to reframe everyday vendors as eavesdroppers. Every embedded analytics or replay tag becomes a potential violation, with the site owner cast as the one who let them listen. |
| **Greenley v. Kochava** | Serial filers use Greenley to turn routine records into violations. Once software alone can be a pen register, ordinary IP addresses and device IDs become unlawfully captured routing data. |

*References: Javier v. Assurance IQ (9th Cir. 2022); Yoon v. Lululemon (C.D. Cal. 2021); Greenley v. Kochava (S.D. Cal. 2023)*

# 2026 Trend: Search Bar Allegations

- A recent wiretapping litigation trend targets website search bars. Plaintiffs opt out of tracking (if available) and then **search their own name on the website**.
- If the website builds a URL containing the search term and sends it to third parties (i.e., analytics vendors), plaintiffs can observe this via network monitoring and allege an unauthorized wiretapping "interception".
- Courts have allowed these theories to proceed: in Heerde v. Learfield, search queries transmitted in real time to an embedded third-party operator supported a §631(a) claim.
- Risk can be reduced by removing search terms from URLs, limiting transmission of search data, and gating scripts behind consent logic, including cookieless scripts.




*Reference: Heerde v. Learfield Commc'ns, LLC (C.D. Cal. 2024)*

# A Show of Hands:
# Any Close CIPA Encounters?

Have you, or a company you know, had a run-in with a serial website wiretapping filer? Drop your answer in the chat.

**A.** Yes, but the matter didn't escalate.

**B.** Yes, and it resulted in a settlement.

**C.** Yes, and it was contested (court or arbitration).

**D.** No, every company I know has avoided this!

# Where Things Stand Today

- Templated letters have been sent out by the thousand, and because demands are priced *below the cost of a defense*, many recipients choose to settle.
- The claims have shifted from cookies to search bars and pen registers: §631(a) interception and §638.51 theories built on self-run browser tests.
- The newest letters steer toward arbitration rather than court, a structural answer to judicial pushback.
- One month ago, the Central District of California declared Vivek Shah (the CIPA litigation wave's most prolific plaintiff) a **vexatious litigant**.
- California lawmakers are *considering SB 690*, a bill that would amend CIPA to curb these lawsuits.

**CIPA Litigation Snapshot: August 2026**

**1,000+**

Templated Demand Letters in Circulation

**80+**

Active Matters at Single Defense Firm

**2**

Dominant Theories: §631(a) Interception & §638.51 Pen Register

**July 20**

Vexatious Litigant Order: C.D. Cal. (Shah v. Crain)

*References: Fisher Phillips (Jul. 6, 2026); Order, Shah v. Crain (C.D. Cal. Jul. 20, 2026); CIPAWorld (Jul. 3, 2026)*

# One More Wildcard: SB 690

- California **Senate Bill 690** would amend CIPA to curb website-tracking lawsuits, making it the most direct legislative response to the letter wave so far.
- A federal judge called CIPA's language "a total mess" that gets bigger "as the world continues to change."
- While it does have support, the bill keeps shrinking: each round of amendments has narrowed it, and the current version would mostly end private pen-register claims, not broader wiretapping claims.
- Retroactivity has gone in and out of the bill along the way, but under every version so far, §631(a) claims, the core of most demand letters, survives.
- Even if SB 690 passes, it may arrive too late and too narrow to reduce current exposure.

**California Senate Bill 690 (2025–2026 Session)**

| Milestone | Comment |
|---|---|
| **Early 2025:** Bill Introduced (Sen. Caballero) | Business coalition push to modernize CIPA |
| **June 2025:** Passed the Senate unanimously | Bipartisan agreement that the litigation wave is a problem |
| **Late 2025:** Stalled in the Assembly (Retroactivity stripped) | Privacy-advocate pushback; pending claims preserved |
| **July 2026:** Broad "commercial business purpose" exemption eliminated | Surviving core ends private pen-register claims only |
| **August 2026:** Pending in the Assembly, then the Governor | §631(a) wiretapping claims unaffected under every version |

*References: CIPAWorld (Jul. 3, 2026); Covington, Inside Privacy (Jul. 2026); Volokh Conspiracy, Reason (Oct. 21, 2025)*

# The Vivek Shah Campaign & the Ruling

History, Patterns, Business Challenges, and What Actually Changed

# Vivek Shah: A “Colorful” History

- Shah began as an aspiring actor in West Hollywood, orbiting the industry he would soon target.
- In 2012, Shah mailed "Extortion Notice" letters to seven wealthy figures, threatening to kill their families unless $4M–$35M was wired to offshore accounts.
- Shah pleaded guilty to federal extortion charges and was sentenced to 87 months in prison.
- The CIPA campaign began in September 2024, with template suits in Los Angeles Superior Court, followed by thousands of demand letters through 2025-2026.
- On July 20, 2026, the Central District of California declared him a **vexatious litigant.**

**Press Release: 2012 Extortion Scheme Sentencing**

United States Attorney's Office
Southern District of West Virginia

About USAO-SDWV | Find Help | Contact Us

Search

About | News | Services & Programs | Jobs | Contact Us

Justice.gov > U.S. Attorneys > Southern District of West Virginia > Press Releases > Goodwin Announces California Man Sentenced To 7+ Years In $122 Million Extortion Plot

PRESS RELEASE

## Goodwin Announces California Man Sentenced To 7+ Years In $122 Million Extortion Plot

Wednesday, September 11, 2013

Share

**For Immediate Release**

U.S. Attorney's Office, Southern District of West Virginia

***Vivek Shah threatened to kill family members of seven wealthy extortion targets***

BECKLEY, W.Va. - U.S. Attorney Booth Goodwin today announced that Vivek Shah, 26, of West Hollywood, Calif., was sentenced to 7 years and 3 months in federal prison for orchestrating a multimillion-dollar extortion scheme. Last year, Shah threatened to kill family members of seven prominent victims, including movie producer Harvey Weinstein, Groupon co-founder Eric Lefkofsky, and coal executive Chris Cline, unless his targets wired tens of millions of dollars into offshore bank accounts.

"Imagine how terrifying it would be to open the mail and find a threat to kill your spouse or your children," said U.S. Attorney Booth Goodwin. "This defendant carried out a carefully planned scheme designed to frighten his victims out of more than $120 million. It was an extraordinarily brazen crime, and I'm pleased, for the victims' sake, that we were able to put a stop to it so quickly."

Shah's other victims included oil and gas billionaire Terry Pegula, from whom he demanded $34 million; Playtone film company co-owner Gary Goetzman, from whom he demanded $9.6 million; Ryan Kavanaugh, founder of Relativity Media, from whom Shah demanded $11.3 million; and Dannine Avara, daughter of a prominent Texas oil-industry executive, from whom Shah demanded $35 million.

*References: DOJ, U.S. Atty's Office S.D. W.Va. (Sept. 11, 2013); LegalClarity; Order, Shah v. Crain (Jul. 20, 2026)*

# The Modern Vivek Shah Method

- Shah's core test is to visit a website with browser developer tools open and to record which third-party tools fire by default and where visitor data flows.
- Deep testing is generally not conducted, as the exhibits are often quick captures of a default page load, sometimes without consent banner interaction.
- Sometimes Shah types a term into the site's search bar, whether tied to his identity ("VIVEK") or merely sensitive-sounding ("felony-friendly jobs"), to capture a "communication" being shared, which is the setup for §631(a) interception claims.
- Alternatively, the trackers are framed as "pen registers" collecting IP and device data under §638.51, which is what the sample letter on the right alleges.

**Vivek Shah Demand Letter Introduction**

1301 N BROADWAY STE 32167 | LOS ANGELES, CA 90012
224.246.2874 | NEWVIVEKSHAH@GMAIL.COM

[redacted], 2026

Via First-Class Mail

*Re: Informal Dispute Resolution*

To Whomsoever This May Concern:

This is regarding your violation of California's Invasion of Privacy Act ("CIPA") Cal. Penal Code § 638.51(a). You have installed and used multiple pen registers on your website without consent. Seeking injunctive relief, declaratory relief and statutory damages. The attached Complaint is prepared and ready to be filed with the Los Angeles Superior Court should this matter remain unresolved.

Regards,

VIVEK SHAH

References: Fisher Phillips (Jul. 6, 2026); Shah v. Talentbridge, 2026 WL 1507888 (C.D. Cal. May 28, 2026)

# How Has the Shah Method Performed?

Vivek Shah has sent thousands of demand letters and initiated at least 29 proceedings since 2021. What is Shah's publicly-known recovery?

**A.** $2,900,000

**B.** $450,000

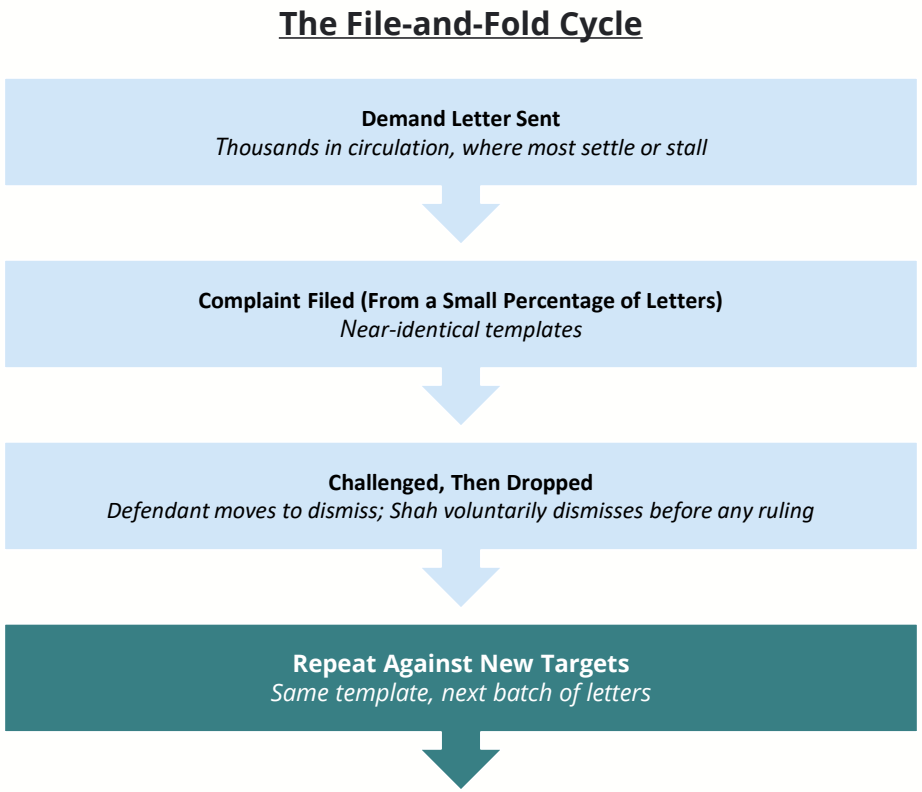
**C.** $50,000

**D.** $3,000

*References: Order, Shah v. Crain (Jul. 20, 2026); Fisher Phillips (Jul. 6, 2026)*

# When Shah Files…He Often Folds

- **The Vivek Shah model leans primarily on early settlements at the letter stage**. Thousands of letters are estimated to be in circulation, and most resolve quietly or stall without a lawsuit ever being filed.
- Filing has been an exception, with only a few dozen proceedings since 2021 (in contrast with thousands of delivered letters).
- When he does file, Shah submits templated complaints, several of which the court called "*near copies of class action complaints filed by unrelated plaintiffs*", often drawing a motion to dismiss and voluntarily dismissing before any ruling.
- Defendants who fight back tend to win, whether through dismissal for lack of standing, granted motions to dismiss, or Shah's own walk-aways.
- Lately, he has been using arbitration as an alternative escalation path (we'll discuss this next!).




*Reference: Order, Shah v. Crain (Jul. 20, 2026), quoted in Duane Morris alert (Jul. 2026)*

# How Some of Shah's Claims Fared

| Case | Outcome |
|---|---|
| **Shah v. TalentBridge** | **Dismissed** (May 2026). The court found no standing, calling out a self-administered, manufactured injury.<br><br>*Standing challenges are the first line of defense against tester-style claims.* |
| **Shah v. Harvard Drug Group** | **Dismissed** (April 2025). The motion to dismiss was granted on the pleadings.<br><br>*The claims failed the moment they were tested on the pleadings.* |
| **Shah v. Card Delivery** | **Dropped** (November 2025). Shah voluntarily dismissed his own case with prejudice.<br><br>*Procedural pressure alone was enough to make him fold.* |
| **Shah v. Mondelez** | **Resolved** (July 2025). The case ended in a joint stipulation of dismissal with prejudice, consistent with a settlement.<br><br>*The occasional settlement is what funds the volume play.* |
| **Shah v. Crain Communications** | **Pending.** His active case continues, and it produced the vexatious litigant order on July 20, 2026.<br><br>*This order is the source of the findings, and it can be cited in negotiation or arbitration.* |

*References: Shah v. Talentbridge (C.D. Cal. 2026); docket summaries per LegalClarity; Order, Shah v. Crain (2026)*

# Shah v. Crain Communications

- On July 20, 2026, Judge R. Gary Klausner granted Crain's motion and declared Shah a "**Vexatious Litigant"** in Shah v. Crain Communications.
- The Prefiling Order requires judicial approval before Shah files any new case in the Central District of California alleging **CIPA or related claims**.
- Earlier in the order, the court found his purpose was to *"harass defendants into coercive settlements"* rather than seek redress from the judiciary in good faith, citing templated complaints and voluntary dismissals.
- The designation weakens every letter Shah sends. Anyone who receives one can now reference this federal court's order. Still, it changed less than the headlines might suggest…

**The Order (Shah v. Crain, Dkt. 34)**



UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

**CIVIL MINUTES - GENERAL**

| Case No. | 2:26-cv-03070-RGK-CTS | Date | July 20, 2026 |
|---|---|---|---|
| Title | *Vivek Shah v. Crain Communications, Inc* | | |

restrictions on the present case pending in this Court, as any such restriction would be premature at this time, in light of the current procedural posture of this case.

Second, Defendant asks that the Court order Plaintiff to post a security of costs in this action. The Court **DENIES** this request. However, it should be noted that any judge presiding over any future action falling under the Prefiling Order will have the discretion of imposing this requirement on Plaintiff.

**V. CONCLUSION**

For the foregoing reasons, the Court **GRANTS** Defendant's Motion to Declare Plaintiff a Vexatious Litigant. The Court **ORDERS** as follows:

(1) The Court declares Plaintiff Vivek Shah a vexatious litigant;

(2) A Prefiling Order is hereby entered against Plaintiff for any new case filed in the Central District of California that alleges any claims arising under the California Invasion of Privacy Act ("CIPA") or other related digital privacy claims.

**IT IS SO ORDERED.**

Initials of Preparer JRE/vc

*Reference: Order, Shah v. Crain Commc'ns, Inc., No. 2:26-cv-03070-RGK-CTS (C.D. Cal. Jul. 20, 2026)*

# What Does the Ruling Change?

- The "**Vexatious Litigant"** order is significant, but narrow. It is a filing screen in one federal district, and it doesn't necessarily mean an end to the campaign.
- For pending matters, the findings are immediately useful. Defense counsel can cite them in motions, attach them to responses, and lean on them to support fee-shifting and sanctions arguments.
- California has its own vexatious litigant statute, so the federal designation supports a parallel state-court motion if he shifts venue.
- The order does not reach arbitral forums, which is exactly where newer demand letters are steering.
- The order also hands future targets a roadmap. What worked against Shah was documenting his pattern across dockets rather than fighting each case alone, and that same playbook may apply to copycats.

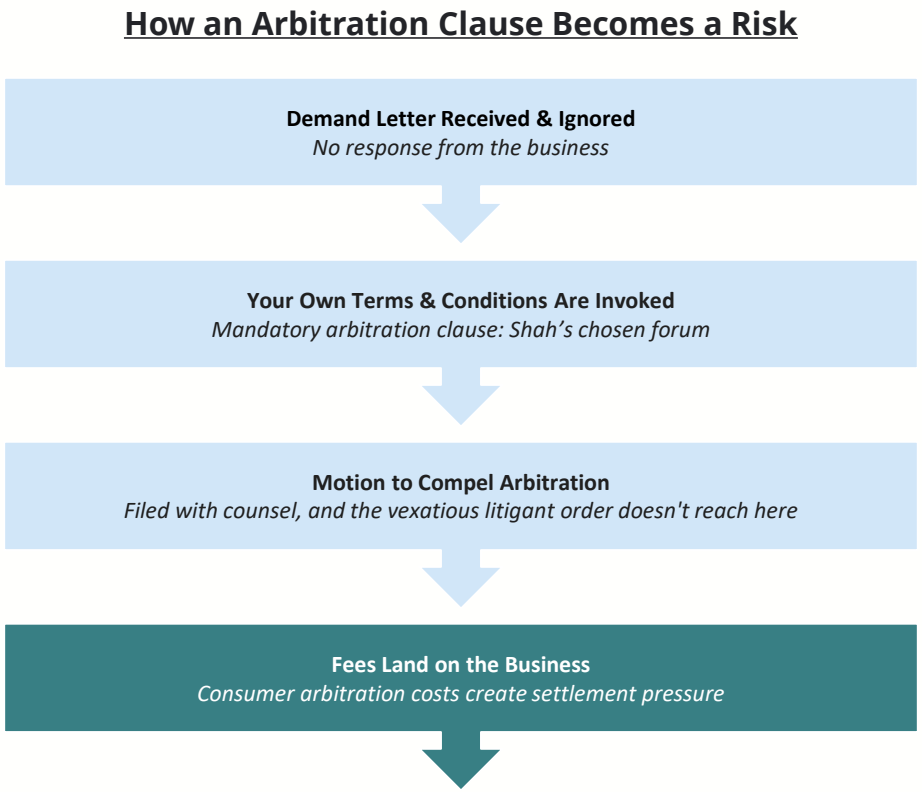
**The Vexatious Litigant Ruling: Changed v. Unchanged**

| What Changed | What Didn't Change |
|---|---|
| • New CIPA suits in the Central District now need pre-filing approval<br>• The screen covers his home venue, the district where his federal CIPA cases have been filed<br>• His letters arrive with weakened credibility<br>• Defendants can cite the court's findings<br>• Fee-shifting and sanctions arguments are stronger | • The legal theories themselves are untouched, and §631(a) and §638.51 claims remain available to anyone<br>• Demand letters can still go out at volume<br>• State courts and other federal districts remain open<br>• Pending cases proceed normally<br>• Arbitration is untouched<br>• Copycat filers are unaffected |

*References: Duane Morris (Jul. 2026); CIPAWorld (Jul. 21, 2026)*

# The Arbitration Pivot

- Your own terms of service can be weaponized by Vivek Shah (and copycats). When website T&Cs contain *mandatory arbitration clauses*, Shah invokes them, and the vexatious order does not follow him there.
- He has already moved to compel arbitration against businesses that previously ignored his letters, retaining counsel for those proceedings when useful.
- Consumer arbitration fees often land on the business, so even a weak claim carries a real-world price tag, and that cost provides Shah with settlement leverage.
- Newer letters may steer toward arbitration from the outset, anticipating court-level restrictions like the Crain ruling. So, it's an important time to **review the scope of your own arbitration clause**, including carve-outs, fee-allocation, and mass-filing protections.




*References: Fisher Phillips (Jul. 6, 2026)*

# The Model is Bigger than Shah

- The economics that made the Shah campaign work (cheap letters, expensive defenses, quiet settlements) did not disappear with the ruling. The playbook is public and repeatable.
- Almost nothing is needed to start. The test is browser-based, the template is circulating, and thousands of broken websites remain easy targets.
- Counseled plaintiff firms are the more durable threat, since they can more easily absorb the motion practice that makes pro se filers fold.
- Copycats learn from the Crain ruling too, steering toward arbitration, filing in state court, and adjusting venue to route around pre-filing screens.

**Same Playbook; New Names**

| Entity | Commentary |
|---|---|
| **Vivek Shah** | New CIPA suits in the Central District now require pre-filing approval, but his demand letters, pending cases, and arbitration path are all unaffected. |
| **Srinivas Rangam** | Actively circulating demand letters built on the same search-bar and wiretapping template. Named alongside Shah in a published survey of prolific CIPA claimants. |
| **Plaintiff Firms & Tester Plaintiffs** | Running the counseled version of the model, filing under recurring tester-plaintiff names. One survey counts more than 40 firms and repeat plaintiffs. |
| **Next Entrants** | Nothing prevents a new sender from adopting the template tomorrow. Expect venue shifts, arbitration-first letters, and filings outside the Central District. |

*References: Buchanan Ingersoll & Rooney (Jan. 10, 2025); Duane Morris (Jul. 2026)*

# Litigation Beyond California

- CIPA already reaches beyond California, since any website with California visitors can receive a letter. And the economics are portable, because several states pair all-party consent wiretap acts with statutory damages, the same factors CIPA provides.
- Florida is the fastest riser, where the FSCA now fuels pixel and session-replay claims, and "privacy advocates" are already active in the letter economy.
- Pennsylvania and Washington are following the same recipe, since both pair all-party consent laws with fresh plaintiff momentum.
- The practical takeaway is that geography is not a defense. The same tracking data flows trigger different statutes in different states, so remediation scoped only to California visitors under-protects.

**High-Risk States for Website Privacy Litigation**

| State | Commentary |
|---|---|
| **California** | CIPA's private right of action and $5,000 per violation power the demand-letter wave, with reform (SB 690) still pending. |
| **Florida** | The FSCA offers all-party consent plus liquidated damages and fees, and it is the fastest-rising source of new claims. |
| **Illinois** | BIPA targets biometrics rather than wiretapping, but its per-violation damages proved the volume litigation model works. |
| **Massachusetts** | Long considered high-risk, until the state's high court narrowed its wiretap act for website browsing in Vita (Oct. 2024). |
| **Pennsylvania** | WESCA requires all-party consent, and class filings have climbed since Popa (3d Cir.) revived third-party tracking claims. |
| **Washington** | A strict all-party consent act now sits alongside the My Health My Data Act, whose first class action hit Amazon in early 2025. |

*References: Fla. Stat. §§934.03, 934.10; Popa v. Harriet Carter, 52 F.4th 121 (3d Cir. 2022); Privacy Daily (Apr. 7, 2026); Orrick (Feb. 2025); 740 ILCS 14 (BIPA)*

# The Letter Is in Your Inbox… Now What?

Evaluating the Claim, Responding Deliberately, and Reducing Exposure

# The Letter Arrived: Be Deliberate!

- Try not to lose sight of what Shah wants, which is a quick, quiet settlement priced below your cost of defense. The complaint and the accompanying urgency are engineered to produce that outcome.
- Route the letter to **experienced privacy litigation counsel** who know this claimant, CIPA litigation history, and the technology being challenged.
- Evaluate the claim before deciding anything, including standing, party exception, consent timing, and whether the alleged data flow occurred as described.
- Preserve the technical record before remediating. HAR files, consent configurations, and tag exports should be captured before any changes are made to the site.
- Decide deliberately and without being pressured. Whether you contest, negotiate, or stand down should come down to the actual strength of the claim, your organization's resources, and your risk tolerance.

## Potential Demand Letter Response Mistakes

1. **Panicking and paying**: Handing over the settlement before gathering all the facts.
2. **Replying informally**: Poor responses from well-intentioned teams can create admissions.
3. **Fixing the site first**: Remediating issues before preserving evidence can complicate the defense.
4. **Forgetting insurance**: Cyber and E&O policies may cover this, but only if you notify the carrier in time.

*References: Jeffer Mangels (Apr. 1, 2026); Fisher Phillips (Jul. 6, 2026)*

# Evaluating the Underlying Claim

- A letter is on its weakest footing when the alleged injury is a self-administered test, you maintain a strong privacy notice, and your consent management tooling worked as-described by your website.
- The letters to take most seriously are the ones where multiple negative factors stack, such as trackers firing before consent, search terms leaving in URLs, and vendors being free to use the data for themselves.
- Vendor contracts are important. Whether your provider acts strictly as your service provider or uses the data for its own purposes can decide party status.
- Walk the five questions internally, using records from the day of the alleged visit, before the letter's deadline and before serious outside spend. The answers usually show how strong the claim is and in contrast, how strong your position is.

**A Five-Factor CIPA Claim Evaluation Checklist**

| Factor | Question to Ask |
|---|---|
| **Interception** | Was data captured in transit, in real time, as the visitor used the site? Data pulled from storage generally is not an interception. |
| **Content v. Metadata** | Does the claim involve communication content under §631(a), or routing and device data under §638.51? Which theory it is determines which defenses apply. |
| **Consent Timing** | Was consent obtained before any tracking fired? Consent gathered afterward does not necessarily cure an earlier interception. |
| **Party Status** | Is the vendor a direct participant serving your site, or a third party benefiting from the data independently? Contracts often decide this. |
| **Standing** | Can the claimant show concrete injury, or was the harm manufactured through a self-run test? Courts increasingly dismiss “testers”. |

*References: Javier (9th Cir. 2022); Yoon (C.D. Cal. 2021); Greenley (S.D. Cal. 2023); Talentbridge (C.D. Cal. 2026)*

# Potential Options (…Not Advice!)

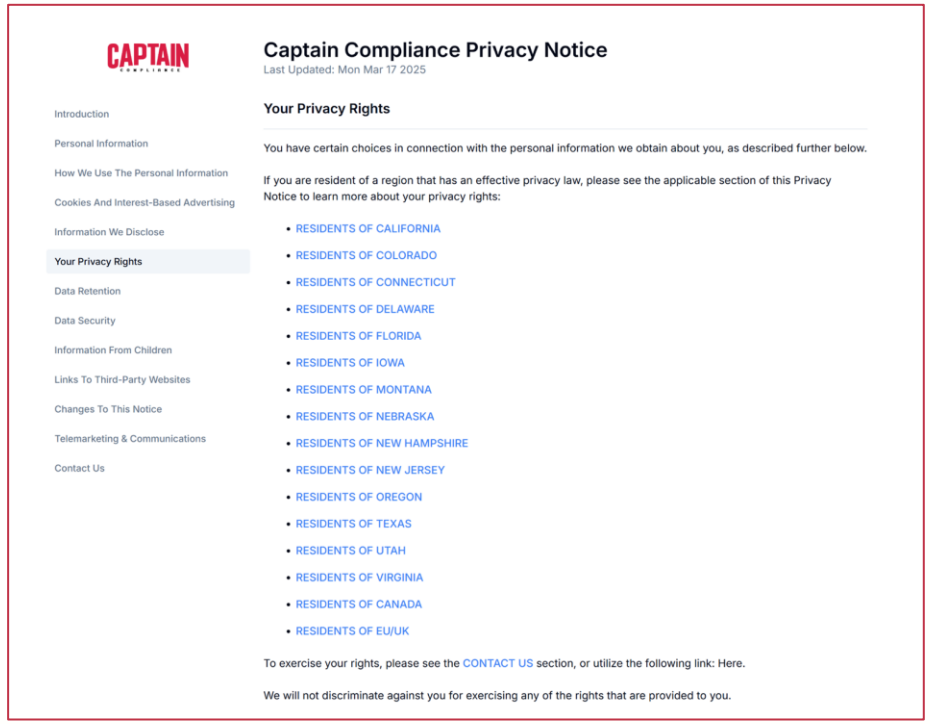
| Option | Potential Upside | Potential Downside |
|---|---|---|
| **Contest** | Motion practice has beaten these claims repeatedly, since standing and pleading defects run through the campaign's record. A win can end the matter outright and deter the next letter. | Defense spend is front-loaded and rarely recovered even in victory, so contesting costs real money before it saves any. An early loss can also raise the settlement price. |
| **Remediate & Respond** | A firm counsel-drafted response paired with prompt remediation can end the matter without payment, since challenged claims in this campaign have usually been dropped. It also closes the exposure that invited the letter in the first place. | Remediation does not undo the alleged past capture, so the claim technically survives and could still be pursued. Any fixes should come only after the technical record is preserved. |
| **Negotiate & Settle** | Settling early is usually the cheapest and fastest exit, since terms tend to stay confidential and the number is known up front. Management trades an open-ended fight for certainty. | Every settlement funds the next wave of letters, and paying offers no protection from copycats. A quiet payment can also mark the organization as a willing payer. |
| **Arbitrate** *(If Invoked)* | Arbitration keeps the dispute in a private forum with no public docket, and the vexatious litigant findings remain fully citable there. Outcomes there also stay confidential. | Consumer-arbitration fees often land on the business regardless of merit, so even a win carries a price tag. |
| **Tender to Insurance** | Cyber and E&O policies may cover defense and resolution, and tendering early preserves every other option while shifting the spend. Notice costs nothing to give. | Coverage varies by policy wording, and notice deadlines are strict, so a late tender can forfeit coverage entirely. A claim can also affect future premiums. |
| **Ignore** | Doing nothing costs nothing, and the numbers may favor it, since thousands of letters have produced only dozens of proceedings. Most ignored letters appear to simply expire. | There is no way to know in advance which letters escalate, and non-response has triggered compelled arbitration in this campaign. Blind silence also skips the internal evaluation that would reveal your actual risk. |

*References: Shah v. Talentbridge (C.D. Cal. 2026); LegalClarity; Jeffer Mangels (Apr. 1, 2026)*

# Privacy Notices and Tracking Disclosures

- A **privacy notice** is a publicly-available statement that explains how an organization processes and protects personal data. It should also inform individuals about their rights and how they can execute them.
- One major concern is **deceptive or misleading privacy practices**. If your privacy notice says one thing, but your company actually does something different, you risk legal action.
- Comprehensive privacy laws in the U.S. generally require businesses to provide accessible, clear, and meaningful privacy notices with specific content.
- Privacy notices also play a critical role in reducing litigation risk, as **inconsistent or unclear disclosures are often at the center of privacy lawsuits**.

**Privacy Notice Example (Partial)**



CAPTAIN COMPLIANCE

Captain Compliance Privacy Notice

Last Updated: Mon Mar 17 2025

Introduction
Personal Information
How We Use The Personal Information
Cookies And Interest-Based Advertising
Information We Disclose
Your Privacy Rights
Data Retention
Data Security
Information From Children
Links To Third-Party Websites
Changes To This Notice
Telemarketing & Communications
Contact Us

**Your Privacy Rights**

You have certain choices in connection with the personal information we obtain about you, as described further below.

If you are resident of a region that has an effective privacy law, please see the applicable section of this Privacy Notice to learn more about your privacy rights:

- RESIDENTS OF CALIFORNIA
- RESIDENTS OF COLORADO
- RESIDENTS OF CONNECTICUT
- RESIDENTS OF DELAWARE
- RESIDENTS OF FLORIDA
- RESIDENTS OF IOWA
- RESIDENTS OF MONTANA
- RESIDENTS OF NEBRASKA
- RESIDENTS OF NEW HAMPSHIRE
- RESIDENTS OF NEW JERSEY
- RESIDENTS OF OREGON
- RESIDENTS OF TEXAS
- RESIDENTS OF UTAH
- RESIDENTS OF VIRGINIA
- RESIDENTS OF CANADA
- RESIDENTS OF EU/UK

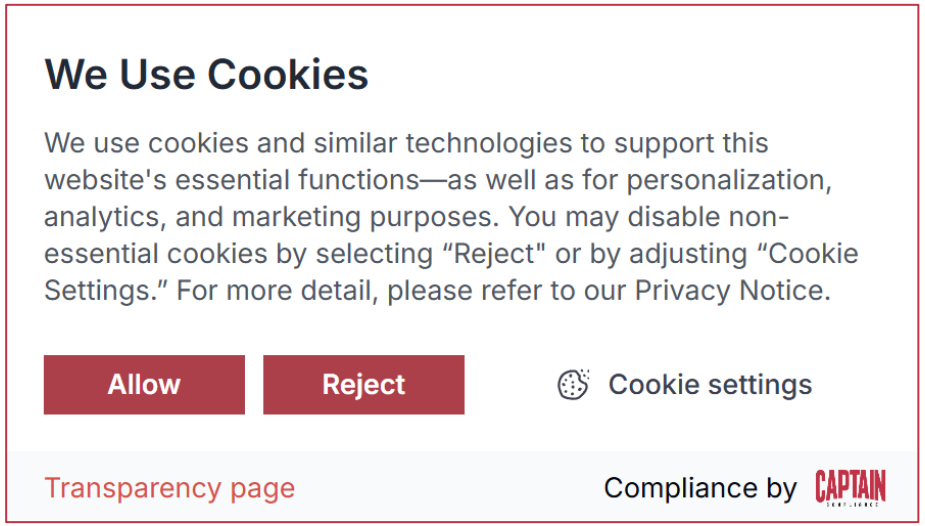
To exercise your rights, please see the CONTACT US section, or utilize the following link: Here.

We will not discriminate against you for exercising any of the rights that are provided to you.

# Consent Management Platforms (CMPs)

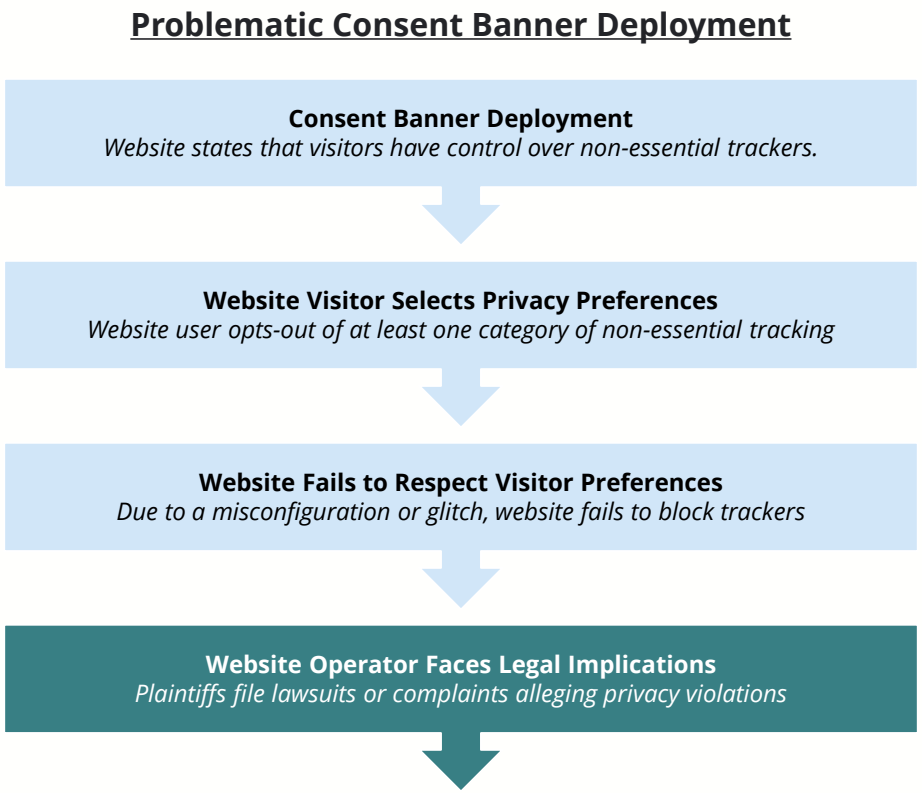
- Cookies are **small text files** that are stored on your device by websites that you visit. They are used for a variety of purposes - both essential and non-essential.
- Cookies have major privacy implications as they are often used to facilitate targeted advertising and can also involve data-sharing with third-party providers.
- Not all web tracking uses cookies, so consent obligations are not exclusive to cookie-based tracking.
- In contrast with the GDPR and some international privacy laws, the existing U.S. state laws *generally allow* for an "opt-out" consent model, so long as clear notice is provided along with relevant opt-out mechanisms.
- **There is a major "grey area" in the U.S. as it relates to wiretapping case law**! (See Javier v. Assurance IQ!)

**Consent Management / Cookie Banner Example**



# Common Issue: Broken & Faulty CMPs

- When a consent banner **fails to block** non-essential cookies or other trackers in response to website visitor opt-outs, it misleads users about their privacy.
- Lawsuits across the country are targeting various industries over these banner failures, alleging misrepresentation of data-collection practices.
- Plaintiffs are pursuing faulty consent banner litigation under various statutes and claims - relating to invasion of privacy, intrusion upon seclusion, wiretapping, misrepresentation, etc.
- Regular testing and monitoring of consent banners is crucial to prevent unnoticed malfunctions and avoid costly litigation - this is especially important after initial deployment, as websites frequently update their design, content, and practices over time.



# Cookie Blocking v. Script Blocking

- There are two primary technical layers through which commercial CMPs operate: **cookie auto-blocking** and **script-level blocking**.
- **Cookie auto-blocking** refers to a CMP's ability to delete, expire, or nullify client-side browser storage.
- **Script blocking** refers to a CMP's ability to "wrap" or conditionally load scripts based on consent logic, including trackers that do not rely on cookies.
- Script blocking is more proactive because it prevents tracking technologies from loading in the first place, (including scripts that do not rely on cookies), while cookie auto-blocking is simpler yet more reactive and cannot address tracking beyond browser storage.
- Mature, defensible deployments typically rely on **both layers** to reduce litigation and regulatory exposure.

**Cookie Auto-Blocking v. Script Blocking**

| Blocking Layer | Cookie Auto-Blocking | Script Blocking |
|---|---|---|
| **General Concept** | Cookies Are Deleted/Nullified When Certain Tracking is Off/Rejected | Scripts/Tags Do Not Load When Certain Tracking is Off/Rejected |
| **General Nature** | More Reactive | More Proactive |
| **Configuration Complexity** | Lower | Higher *(Script Integration)* |
| **Ideal Consent Model** | Opt-Out Model | Either Opt-Out Model OR Opt-In Model |
| **Cookieless Tracking** | Unable to Address | Scripts Can be Wrapped |
| **Overall Defensibility** | **Moderate** | **Very High** |

# A Key Decision: Opt-Out v. Opt-In

- In some regions, CMP configuration decisions tend to be straightforward. For example, the EU requires an **opt-in consent model** for non-essential tracking.
- In the United States, businesses must make a **risk-based business decision** about whether to fire non-essential tracking technologies by default
- The opt-in model is the most effective at reducing litigation and regulatory risk, but it carries a significant business impact. Because an estimated **95–98% of users do not interact with consent banners**, the (more restrictive) default setting is usually retained.
- As a result, many organizations adopt an **opt-out model** in the U.S., accepting residual exposure in relation to the more extreme CIPA case law "…retroactive consent is invalid…"

**Opt-Out Model v. Opt-In Model**

| Consent Model | Opt-Out Model | Opt-In Model |
|---|---|---|
| **European Union** | Not Permissible | Required |
| **United States** | **Generally Permissible (Modern Laws)** | **Potentially Required (SOME CIPA Case Law)** |
| **Default Behavior (Initial Website Load)** | Only Essential Trackers Fire | All Trackers Fire |
| **What Happens if the Visitor Does Not Interact with CMP?** | Default Behavior Remains In-Place | Default Behavior Remains In-Place |
| **Impact to Analytics Data Collection & Online Marketing** | Very Low *(Often 1%-2% Impact)* | Very High *(Often 98-99% Impact)* |
| **Overall Litigation Risk Reduction** | **Moderate** | **Very High** |

# Do You Know What Your Search Bar is Doing?

When a visitor types something in your website's search bar, do you know the technical mechanics of where that search term goes?

**A.** Yes, the search data stays on our servers

**B.** Yes, the search data goes to analytics/ad vendors

**C.** I have no idea, I've never investigated it

**D.** We don't have a search bar

# Network & Search Bar Litigation Risks

- Plaintiffs increasingly allege that **search terms** and related network requests shared with third parties constitute unauthorized interception and form the basis for privacy claims.
- Some courts have held that search terms entered a website search bar can qualify as "contents of a communication" under statutes such as CIPA.
- Search bar data exposed in outbound network traffic or embedded in URLs can trigger demand letters or litigation, even where no cookies are involved.
- Core issues include search terms passed in URL query strings or referrer headers that are observable by third parties, uncontrolled or inline third-party scripts that execute without consent, and a lack of clear disclosure regarding the collection or sharing of search data.

**Search Bar Litigation Risk Remediation Options**

1. Process search inputs server side where feasible so search terms are not exposed in client-side traffic.
2. Remove search terms from URL query strings and referrer headers so they are not externally visible.
3. Restrict analytics and replay tools from running during search interactions without consent.
4. Ensure privacy notices clearly explain how search data is used and shared with third parties.

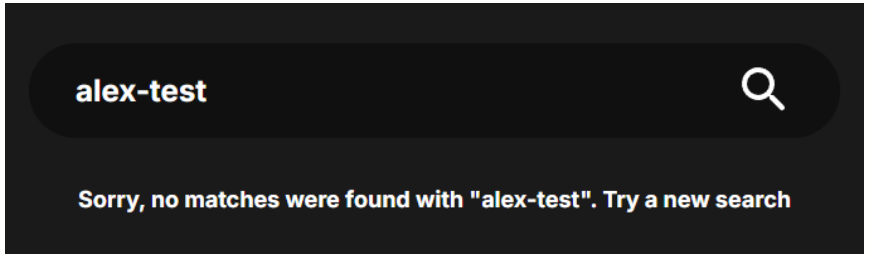
# How to Assess Your Search Bar Risk

1

Use your CMP to **opt-out of non-essential tracking**. Although you may want to restrict search-bar data sharing entirely, the riskiest scenario is one in which you share URL query strings with third parties **after** an opt-out.

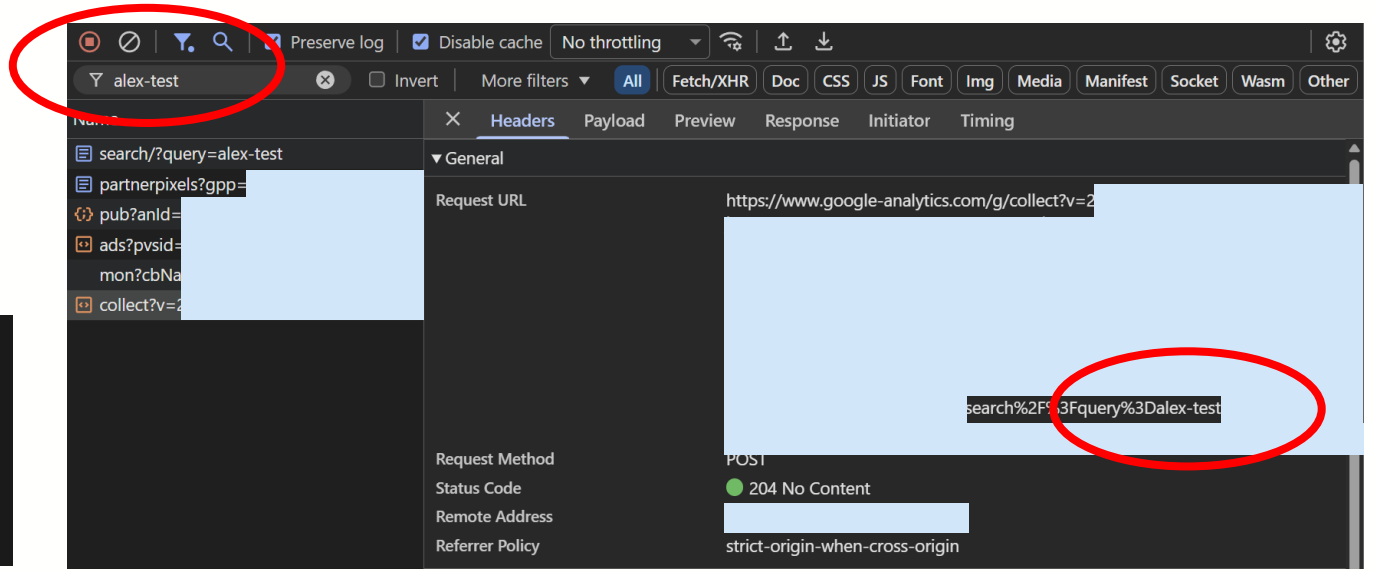

2

Utilize your website's search bar to **conduct a search for a test string**. Usually, plaintiffs will search for their own name to strengthen their claim that any third-party sharing of search queries constitutes a violation.



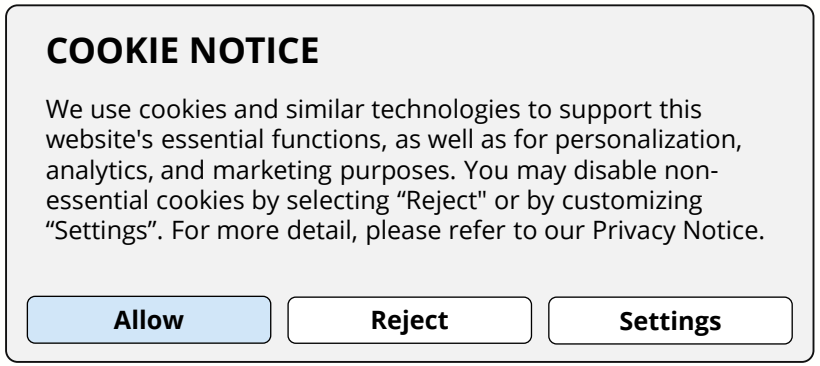

3

While conducting your test search, **add a filter for your search term.** Then, execute your search and observe the traffic that is logged. Review the logged traffic and look for instances in which your search term is being externally-shared. For example, the screenshot below shows a Google Analytics request with the search term embedded into the externally-shared URL. This is a common issue.

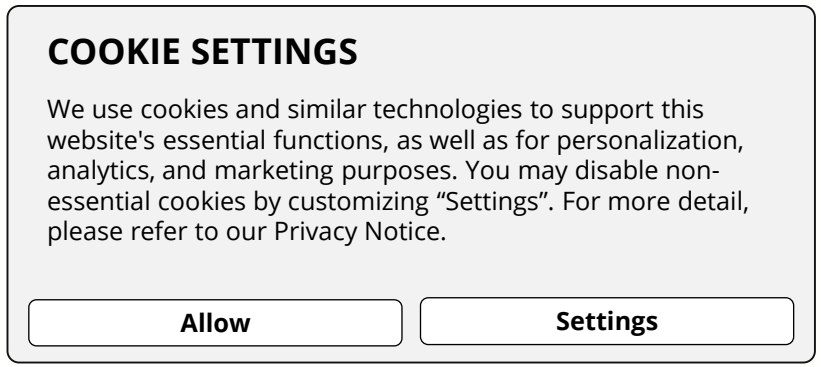


# Which Banners Have Dark Patterns?

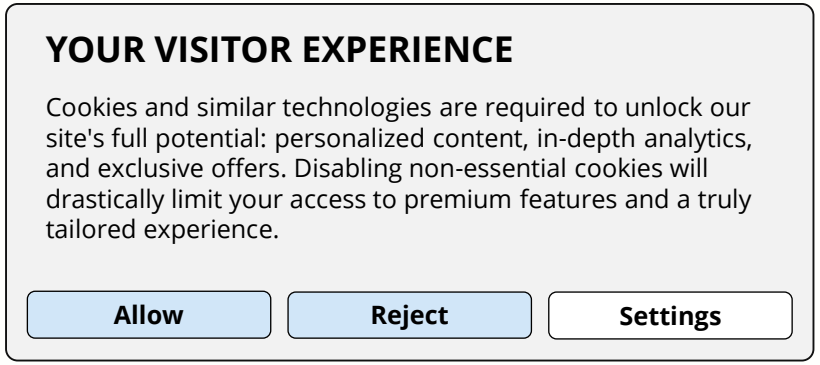
**A**



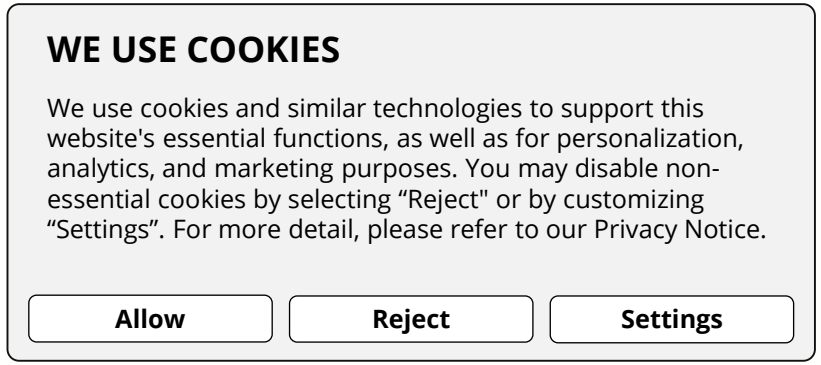

**B**




**C**

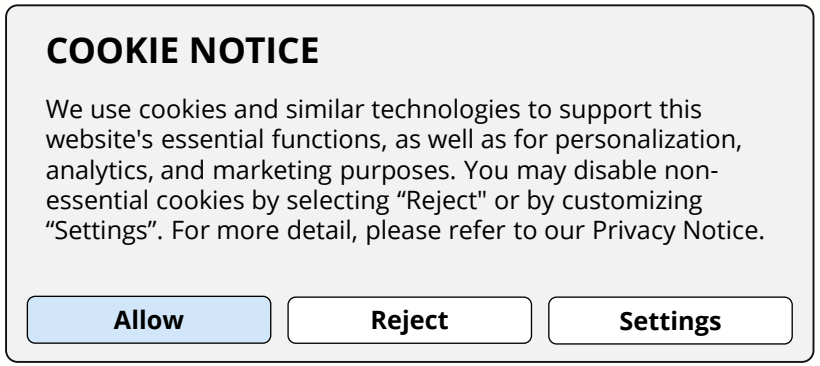



**D**



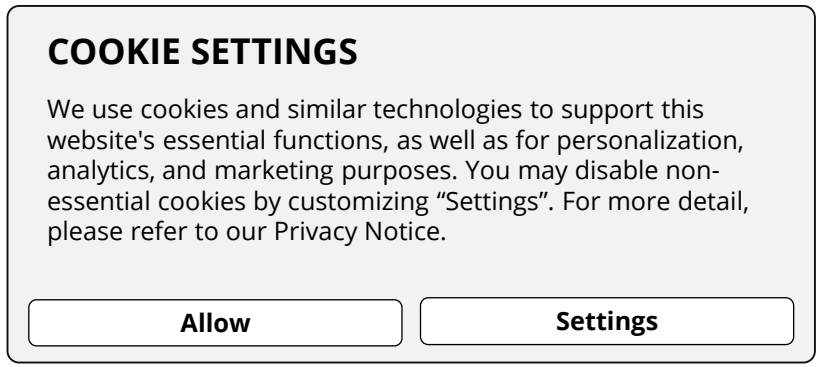
# Which Banners Have Dark Patterns?

**A**



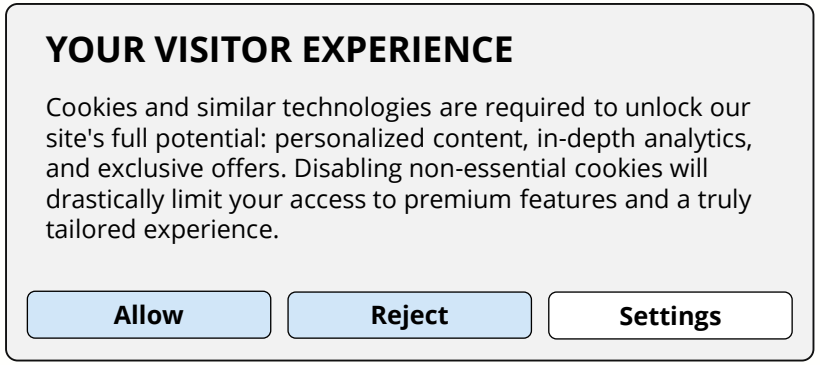

Dark Pattern: “Allow” Button Color

**B**



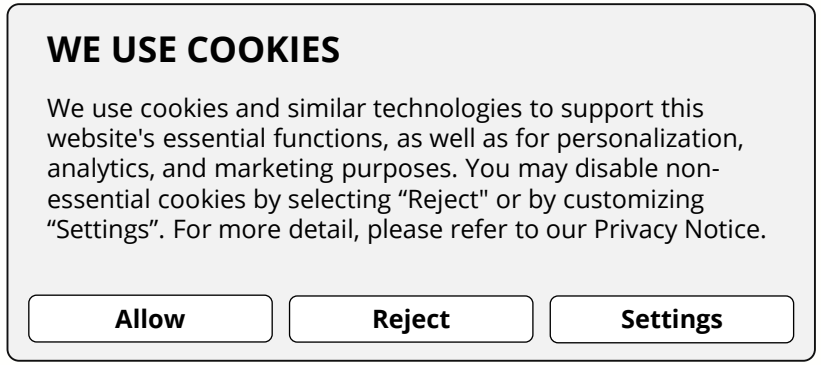

Dark Pattern: Asymmetrical Choices

**C**




Dark Pattern: Persuasive Language

**D**




Dark Pattern: None (Compliant Design)

# Summary: U.S. Litigation Defensibility

| Example | Common Example #1 No CMP | Common Example #2 "Free Plugin" CMP | Common Example #3 Broken (Opt-Out) CMP | Common Example #4 QA'd (Opt-Out) CMP | Common Example #5 QA'd (Opt-In) CMP |
|---|---|---|---|---|---|
| **Privacy Notice** | Published | Published | Published | Published | Published |
| **Top-Level Consent Notice** | Absent | Clear & Visible | Clear & Visible | Clear & Visible | Clear & Visible |
| **Dark Patterns** | N/A | Deceptive UI | None | None | None |
| **Cookie Blocking** | N/A | Not Functional | Partially Functional | Functional | Functional |
| **Script Blocking** | N/A | N/A | Partially Configured | Mostly Configured | Fully Configured |
| **Default Policy (U.S.)** | N/A | Opt-Out Model | Opt-Out Model | Opt-Out Model | Opt-In Model |
| **Global Privacy Control** | N/A | Not Respected | Not Respected | Respected | Respected |
| **External Integrations** | N/A | Not Addressed | Not Addressed | Addressed | Addressed |
| **Residual Risk** | Very High | Very High | High | Medium-Low | Very Low |
| **Litigation Defensibility** | **Very Low** | **Very Low** | **Low** | **Medium-High** | **Very High** |

# Reduce Website Litigation Risk

1. **Understand your technology stack and its data flows.** Audit what fires on your website, what each technology does, and where visitor data goes, including search terms passed to third parties in URLs and network requests. Remove any tracking technology that does not serve a clear purpose.
2. **Make a deliberate decision about default tracking.** Requirements vary by region: some jurisdictions mandate opt-in, while much of the U.S. requires a risk-based decision. Choose opt-in for maximum risk reduction, or adopt opt-out knowingly and accept the residual risk.
3. **Provide meaningful user choice and honor it.** Ensure opt-outs, consent flows, and preference signals (including Global Privacy Control) are technically operational and consistently respected. Avoid dark patterns!
4. **Implement script-level controls where possible.** Wrap tags in consent logic so they cannot execute under blocking conditions, whether via a tag manager or directly in site code. Govern non-cookie technologies as well.
5. **Maintain an accurate and highly visible Privacy Notice.** Your disclosures must reflect your actual data practices, vendors, and tracking technologies, and the notice should be easily accessible to maximize defensibility.
6. **Monitor and audit continuously.** Websites evolve quickly; configuration drift or vendor updates can quietly undermine defensibility. Review controls regularly, including the same browser-level test serial plaintiffs run.
7. **Revisit your website terms with counsel.** Mandatory arbitration clauses drafted to stop class actions can be invoked by serial claimants, so review scope, fee allocation, and mass-filing protections.

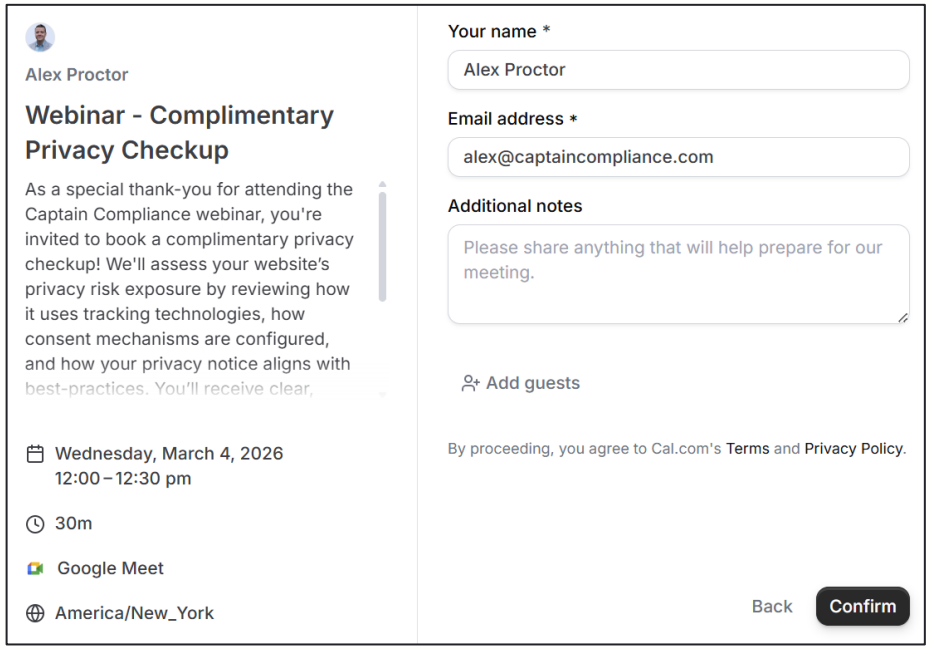
# Complimentary Privacy Checkup!

- As a special thank-you for attending the In-House Connect webinar, you're invited to book a **complimentary privacy checkup**!
- We'll run the same tests serial plaintiffs run, reviewing your tracking technologies, consent configuration, and privacy notice alignment, before a demand letter forces the issue.
- You'll receive clear, actionable guidance on what's working and where improvements may be needed.
- This is a private session. Registration is available through this invite-only link, and spots are limited.

  *Sign-up for the complimentary checkup:*

  **cal.com/alex-captaincompliance/checkup**

**Schedule Your Complimentary Checkup!**



# Captain Compliance Can Help!

- **ComplianceShield** provides qualified customers with legal risk mitigation and defense support in the event of web-tracking litigation, designed for the demand-letter scenarios covered today.
- **Cookie Consent Module** delivers regionally-customizable banners and ensures that websites respect visitor tracking preferences in accordance with global privacy laws.
- **Free Cookie Scanner** analyzes any website and generates a categorized inventory of first-party and third-party cookies while flagging higher-risk trackers.
- **Dynamic Privacy Notice** turns a simple questionnaire into a comprehensive privacy disclosure with dynamic, layered formatting that adjusts based on visitor location.
- **Data Subject Rights (DSR) Portal** provides a customizable and automatable workflow to intake, verify, and fulfill privacy requests from consumers.
- **Privacy-Auditing Browser Extensions** allow businesses, insurers, and similar parties to assess cookie consent functionality, including identifying banner misconfigurations.
- **Cookie Transparency Page** automatically generates a clear, up-to-date web page describing the cookies and tracking technologies used on websites.

# Questions & Answers

Alex Proctor
AIGP, CIPP/E, CIPP/US, CIPM, CIPT, FIP
Chief Trust & Privacy Officer
Captain Compliance

www.captaincompliance.com

# Web Conference
# Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

**Click here:** https://iappwf.questionpro.com/t/AbBPvZ9byc

**Thank you in advance!**

For more information: www.iapp.org

## Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

## Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: livewebconteam@iapp.org