(11.02.2026)

Advisory on California "Pen Register / Trap-and-Trace" claims under CIPA (§ 638.50–638.55)

Introduction

The California's Invasion of Privacy Act **("CIPA")** includes a set of provisions regulating **"pen registers"** and **"trap and trace devices."** These were originally designed for law enforcement style call-routing surveillance, but the statutory definitions were written broadly enough that plaintiffs now argue they apply to certain web and app tracking tools. CIPA defines the following terms for devices as:

Pen register § 638.50 (b)**:** A "pen register" is defined as a device or process that records/decodes dialling, routing, addressing, or signalling (**"DRAS"**) information transmitted by a wire/electronic communication, but not the contents of the communication.

Trap and Trace device § 638.50 (c)**:** A "trap and trace device" is similarly a device or process that captures the incoming DRAS information reasonably likely to identify the source of a wire/electronic communication, but not the contents.

Rule, Exceptions and Consent

CIPA makes it unlawful to install or use a pen register or trap-and-trace device without first obtaining a court order under §638.52 or §638.53, unless an exception applies.

§638.51 allows a provider of electronic or wire communication service to use these tools for certain purposes (operate/maintain/test service; protect rights/property; protect users; prevent fraud/abuse; or if the consent of the user has been obtained).

Most commercial website operators will not (and typically cannot) obtain the law enforcement-style court orders contemplated by §638.52-638.53. That's why disputes center on whether a website fits within the statutory exceptions or whether consent was obtained from the user/visitor.

Fines and Penalties

Criminal (statutory): A violation of § 638.51 is punishable by **a fine up to $2,500**, and/or **up to one year in county jail**, as per Penal Code § 1170(h).

Civil Damages: § 637.2 CIPA provides a civil action for an injured person to recover the greater of **$5,000 per violation or three times** actual damages and allows injunctive relief without requiring actual damages as a prerequisite.

Why this is being applied to modern tech and websites?

These CIPA §638.51 "pen register/ trap-and-trace" claims are being applied to modern websites because the statute defines a pen register and trap-and-trace device very broadly as any "device or process" that records/decodes or captures (DRAS) information for an electronic communication (i.e., communications "metadata," not content). In recent cases plaintiffs argue that common web technologies like **pixels, analytics tags, session-replay scripts, SDKs** function as a software "process" that causes a visitor's browser/app to transmit DRAS-like identifiers (often alleged to include **IP address, unique identifiers/cookies, URL/referrer paths, and device/browser signals**) to the website and frequently onward to third parties, which they characterize as "installing or using" a pen-register like process without the court order under §638.51 (unless an exception applies). This theory gained momentum after **Greenley v. Kochava** *(Case No. 22-cv-01327-BAS-AHG)*, where the court emphasized that the statute is not limited to physical devices and that a "process" can include software, with the focus on what the process does (collect/correlate signalling information), and the legal landscape remains unsettled because courts have split on key questions like whether IP address 'only' allegations are enough and whether consent / statutory exceptions defeat liability, leading to inconsistent rulings as this wave of cases continues.

Key caveats for business:

- **Courts are inconsistent on** whether **§ 638.51** extends to routine website and app tracking, with post Greenley decisions going both ways in cases involving common tracking tools and identifiers. For eg: in **Licea v. Hickory Farms LLC** *(23STCV26148, 2024 WL 1698147)* court rejected a theory that collecting IP addresses via website tech violates § 638.51.
- Consent is the main battleground, and **courts do not uniformly accept implied consent** from mere site use, so a weak banner flow or pre consent tag firing can drive exposure and be detrimental to the company.
- Statutory damages exposure and the rule that actual damages are not required create settlement pressure because § 637.2 authorizes $5,000 per violation or three times the actual damages and states that **suffering or threat of actual damages is not a prerequisite to suit.**
- Plaintiffs frame these cases as capture of dialling routing addressing signalling metadata rather than contents, so **not recording message contents may not defeat a claim** if DRAS style data is alleged, For eg: **Shah v. Fandom** *(Case No. 24-cv-01062-RFL).*
- Proposed reforms, such as SB 690, have been discussed. As drafted, the bill would carve out certain tools used for a defined commercial business purpose and would apply the change retroactively to cases pending as of January 1, 2026. However, the reforms have not created a stable compliance endpoint, so **companies should not plan on a near term legislative fix eliminating risk.**

What are the common pitfalls for businesses which attract trap and trace cases?

1. <u>'Always on' deployment of trackers</u>

Claims: Plaintiff's claim that continuous sitewide deployment of trackers is framed as the company "installing/using" a "device or process" that records/decodes 'DRAS' information from "wire or electronic communication. **Dino Moody v. C2 Educational Systems Inc. et al.** *(case no- 2:24-cv-04249-RGK-SK)*

Points of failure:

When there is overbroad deployment of trackers (running across all site pages, including low-utility pages like content/help pages) this shows the courts that the collection is not limited to what is necessary and rather resembles systematic monitoring.

2. <u>Pre-consent firing (pixels load before user makes a choice)</u>

Claims: When tracker deployed by the businesses is alleged to execute without consent, because it loads at page initialization (or before the consent state is applied), rendering the installation/use "unauthorized" under the statute. **Dino Moody v. C2 Educational Systems Inc. et al.** *(case no- 2:24-cv-04249-RGK-SK)*

Points for failure:

- Trackers deployed by the businesses often trigger before a consent is registered. Thereby capturing information before the user has consented to it.
- Along with this, businesses have lack of evidentiary record of consent. Businesses often have failed to demonstrate consent of the user wherein it has a record of who consented, when they have consented and for what categories they have consented.

3. <u>Third-Party tracker (vendor operated, but deployed by the site/business)</u>

Claims: Even when a third party operates the tracking service, plaintiffs allege that the site operator (the business) is responsible because it caused the tracking code to run in visitors/users' browsers and disclose identifiers to third parties. **Shah v. Fandom** *(Case No. 24-cv-01062-RFL)*

Points of failure

Weak third-party governance: Lack of visibility into who controls a vendor tag and how it operates is a key risk. Once the business deploys the tag on its site, plaintiffs can frame the business as having caused the tracking to occur (and thus having installed/used the alleged trap-and-trace process), even if the vendor operates the service.

What Proactive steps should a business take?

1. Audit every tracking component and remove what you don't truly need

Create a complete inventory of all website and app technologies that can collect or transmit identifiers and browsing or interaction data, such as analytics, advertising pixels, tag managers, chat widgets, session replay, A/B testing tools, Customer data platforms, and mobile SDKs. Eliminate duplicate tags, disable features you do not need, and remove any vendor you cannot clearly justify from a business and privacy perspective, since CIPA "trap-and-trace" claims often focus on these common, standard tracking tools.

2. Put non-essential tools behind affirmative consent (and record proof)

Tracking software should not be deployed until there is an affirmative action by the user like clicking the ‘Accept’ button on the consent banner. Avoid ‘implied consent’ language like “by using this website you agree to cookies,” and instead use an opt-in approach for non-essential tracking. To do this reliably, implement a consent management platform that:

- Blocks non-essential scripts/SDKs until the user opts in
- Stores time-stamped consent logs tied to the user/session
- Allows easy withdrawal/changes via a preference center or similar section on your website.

3. **Minimize what third-party tracking and engagement technologies tools collect (business must configure these tools on their websites, mere disclosure might not be enough)**
   Tune these tools so they don’t capture data that is more than necessary, businesses should try to:

- Mask/disable collection of form fields, search terms, chat text, keystrokes, and anything a user types.
- Configure tools to exclude sensitive content
- Avoid persistent “fingerprinting” style identifiers where possible
- Limit sharing of full URLs/query strings if they can include user-entered data

4. **Add “just-in-time” notices where tracking happens (not only in the privacy policy)**

Along with keeping your privacy policy and terms updated, place short, contextual disclosures right where the user is about to interact with features that trigger tracking, such as a chat widget, checkout, account signup, or embedded third-party content. The notice should clearly explain what tracking is being used, why it is used, and give the user an easy way to manage preferences or opt in where required, because timely, obvious notice and meaningful choice are generally more defensible than disclosures buried in a policy.

5. **Contractually control vendors (and allocate risk clearly)**

Update your contracts with analytics, advertising, session-replay, chat, and SDK vendors (and any marketing agencies) so they are only allowed to process data for your business purposes and on your instructions, are prohibited from reusing or selling the data, are required to limit what they collect and how long they retain it, and must provide prompt notice and cooperation if there is a security issue or a legal claim, with responsibility and liability clearly assigned where you have leverage.

Contact

DPO India
Email: dpo@dpo-india.com
Website: www.dpo-india.com