# Auditzo - CIPA Audit Checklist

**Purpose:** Operational checklist for website reviews under California Penal Code §638.51, focused on potential trap-and-trace / pen-register style risk indicators such as addressing information, pixels, identifiers, and third-party request behavior.

**Disclaimer:** Operational and technical review aid only; not legal advice or a determination of liability.

| Control ID | Compliance Area | Audit Control | Relevant Requirement | Evidence to Collect | Test Method | Risk Level | Status | Notes |
|---|---|---|---|---|---|---|---|---|
| CIPA-01 | Scope | Confirm whether the website or service is accessible to California users and whether California traffic or plaintiffs are | Program scope / California nexus | Traffic reports, state targeting docs | Review markets, ad targeting, and user base | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | foreseeable. | | | | | | |
| CIPA-02 | Statutory Framing | Map the review to Penal Code §§638.50–638.51, focusing on dialing, routing, addressing, or signaling information rather than contents. | Core statute framing | Legal memo, control matrix | Review statute definitions and align controls | High | | |
| CIPA-03 | Definitions | Assess whether any website software, script, pixel, SDK, or process could plausibl | Pen register / trap and trace definitions | Script inventory, network logs | Inventory all tracking technologies and their data capture | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | y function as a 'device or process' under §638.50 definitions. | | | | | | |
| CIPA-04 | Addressing Information | Identify whether scripts collect IP address, routing data, device/browser identifiers, request metadata, or other signaling information. | Addressing / signaling review | HAR, request headers, payload samples | Inspect requests and client-side collectors | High | | |
| CIPA-05 | Non-Content Limitation | Separate signaling /addressing data | Content vs non-content distinction | Evidence notes, screenshots | Label findings as content vs | Medium | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | from message contents in the audit record and findings. | | | non-content | | | |
| CIPA-06 | Technology Inventory | Build a complete inventory of pixels, analytics tags, session replay, SDKs, CDPs, fraud tools, and embedded third-party scripts. | Tracking technology inventory | Tag list, script map | Review source, tag manager, and network waterfall | High | | |
| CIPA-07 | Meta / Ad Pixels | Check whether Meta Pixel or compara | Pixel risk review | Network logs, script config | Test first visit, pageview, conversion pages | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ble ad-tech captures IP, fingerprinting-style, browser, or device signals from website visits. | | | | | | |
| CIPA-08 | Fingerprinting Signals | Assess whether software gathers browser, device, or environmental data that can be correlated to identify a visitor. | Fingerprinting exposure | Payloads, SDK docs, request samples | Inspect scripts and captured parameters | High | | |
| CIPA-09 | Session Replay / Analytics | Review whether analytics /session | Analytics / replay risk | Network logs, replay config | Inspect requests and replay | Medium | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | replay tooling captures identifying routing or signaling data alongside page interactions. | | | initializers | | | |
| CIPA-10 | Incoming vs Outgoing Flows | Document whether captured data concerns outbound request metadata, inbound source indicators, or both. | Pen register vs trap-and-trace mapping | Request/response traces | Map data directionality in findings | Medium | | |
| CIPA-11 | Consent Mechanism | Document whether any | Consent / user authorization | Banner screenshots, | Review pre-click and post-click | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | consent mechanism exists and what exactly it discloses regarding tracking or addressing information capture. | | policy text | disclosures | | | |
| CIPA-12 | Consent Quality | Assess whether any alleged consent is specific enough to tracking/signaling capture, rather than generic | Consent sufficiency | Banner, policy, terms text | Compare disclosures against actual technical behavior | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | website use language. | | | | | | |
| CIPA-13 | Provider Exception Review | Test whether any claimed reliance on provider-operation, maintenance, fraud prevention, abuse prevention, or property-rights exceptions is supportable. | §638.51(b) exceptions | Internal technical rationale, SOPs | Review purposes against statutory exceptions | High | | |
| CIPA-14 | Commercial Purpose Tension | Note any litigation-sensitive argument that | Litigation/ defense monitoring | Legal note | Flag unresolved defense posture separately | Medium | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | normal commercial website tracking may be characterized as business-purpose activity, but do not treat it as settled law for compliance sign-off. | | | | | | |
| CIPA-15 | First Visit Testing | Capture evidence from a first-time visit in a clean browser to see what trackers load before any action. | First-visit evidence | HAR, screenshots, DevTools logs | Use private browser and no prior cookies | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CIPA-16 | Consent-State Testing | Compare behavior before consent, after accept, after reject, and after withdrawal where available. | Behavior state comparison | Multi-state HARs, screenshots | Run scenario matrix across states | High | | |
| CIPA-17 | Page-Type Testing | Test homepage, product pages, blog pages, landing pages, forms, checkout, account areas, and embedded media. | Coverage breadth | Scenario log | Test multiple page types and flows | Medium | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CIPA-18 | Network Evidence | Preserve HAR, DevTools screenshots, request URLs, response headers, cookie tables, and script sources for each finding. | Evidence preservation | HAR, screenshots, exports | Capture reproducible evidence per page | High | | |
| CIPA-19 | Identifier Correlation | Map which identifiers are stable, unique, or correlatable across requests, sessions, or vendors. | Identifier mapping | Cookie table, headers, query params | Create identifier correlation matrix | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CIPA-20 | Third-Party Disclosure | Document third parties receiving potentially relevant addressing or signaling information. | Third-party recipient review | Vendor inventory, network domains | Map third-party recipients by page and event | High | | |
| CIPA-21 | Tag Manager Control | Review whether tag managers or server-side routing inject or proxy tracking in ways that may obscure actual recipients. | Tag management review | Tag manager config, request traces | Inspect tag sequencing and proxied endpoints | Medium | | |
| CIPA-22 | Policy Mismatch | Compare privacy/ cookie | Disclosure consistency | Policies, notices, | Compare written disclosure | High | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | disclosures to observed technical behavior, specifically around trackers and data recipients. | | observed evidence | s to live traces | | | |
| CIPA-23 | User Journey Logging | Maintain a timestamped event log of page loads, clicks, consent actions, and resulting network behavior. | Forensic sequencing | Timeline table | Record precise steps and timestamps | Medium | | |
| CIPA-24 | Geographic Context | Document California-user | California nexus evidence | Geo assumptions, | Record California nexus in | Medium | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | relevance in the evidence package where the claim theory depends on California access. | | business docs | audit notes | | | |
| CIPA-25 | High-Risk Findings | Flag Meta Pixel, fingerprinting-style, or unique identifier capture as high-priority review items. | High-priority signals | Finding summary | Classify severity based on uniqueness and breadth | High | | |
| CIPA-26 | Remediation Planning | Document options such as removing scripts, | Remediation governance | Issue log, owner list | Assign owners and deadlines | Medium | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | changing sequencing, narrowing parameters, updating disclosures, or obtaining stronger user authorization. | | | | | | |
| CIPA-27 | Audit Summary | Prepare a concise summary of observed CIPA risk indicators, evidence captured, unresolved questions, and recomm | Audit closeout | Summary memo | Issue final findings summary | Low | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ended next actions. | | | | | | |

## Sources


**California Penal Code §638.50**

https://www.leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=638.50

Official definitions of pen register and trap and trace device.

**California Penal Code §638.51**

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=638.51.

Official prohibition and provider exceptions.

**Wright v. TrueCare Property Holdings, LLC (S.D. Cal. 2025)**

https://law.justia.com/cases/federal/district-courts/california/casdce/3%3A2025cv00786/809784/34/

Order discussing IP address, Meta Pixel, fingerprinting-style identifiers under §638.51 pleadings.

**Nelson v. Reddit, Inc. (S.D. Cal. 2025)**

https://law.justia.com/cases/federal/district-courts/california/casdce/3%3A2025cv01470/818121/26/

Order noting case law was not favorable to defense on tracker argument.

**Fregosa v. Mashable Inc. (N.D. Cal. 2025)**

https://law.justia.com/cases/federal/district-courts/california/candce/3%3A2025cv01094/443724/53/

Order discussing recent California superior court and federal treatment of CIPA pen register claims.

**SB 690 bill text (2025-2026)**

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB690

Pending bill; included only to flag legal uncertainty, not as enacted law.