DIDOMI



CIPA Compliance

New Approaches To Tackle Wiretapping Litigation Risk

The California Invasion of Privacy Act (CIPA), a nearly 60-year-old phone-tapping law, is now the most litigated privacy statute in the U.S. Most companies hit with a demand letter thought they were already compliant, because they confuse CIPA with CCPA. This guide breaks down why that mistake happens and how to close the gap.

5,000
per violation, no proof of harm required

1 year
statute of limitations

70-80%
of websites still track client-side

1 · Why your wesbite is exposed

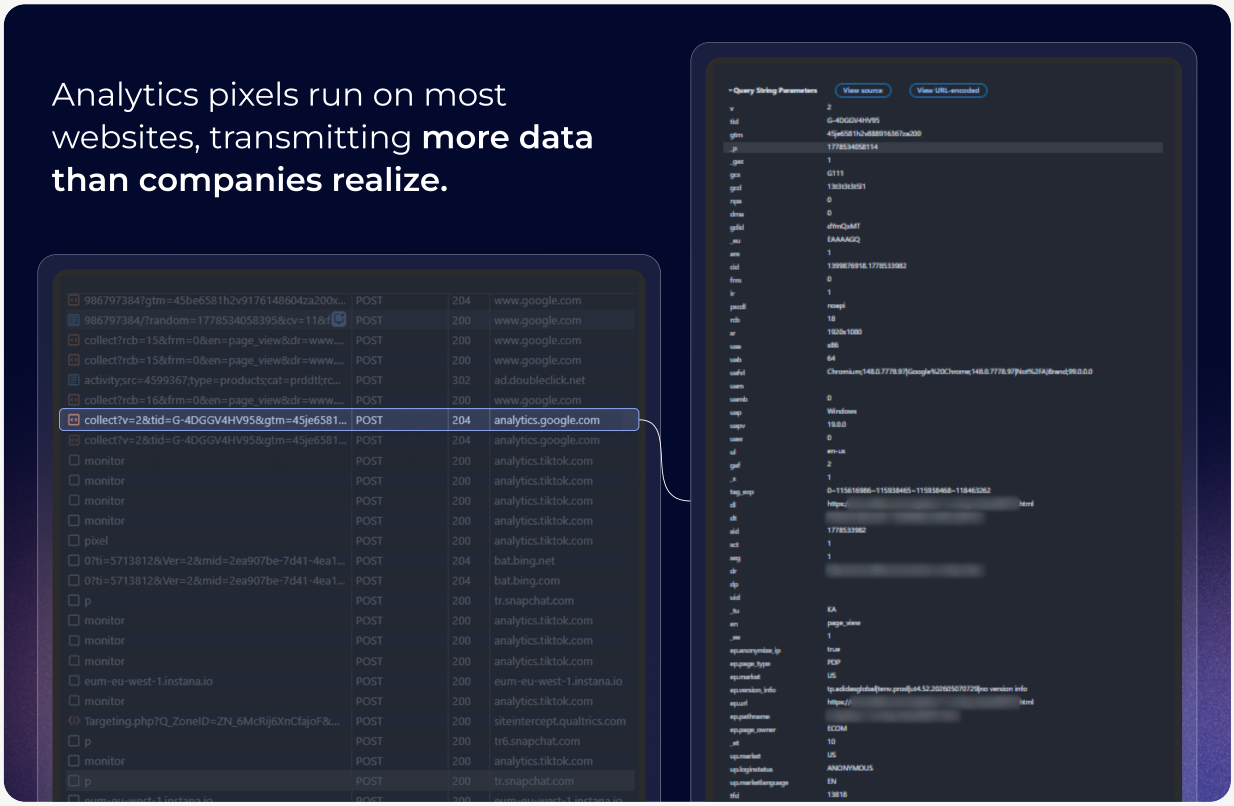
Most claims follow the same pattern: an analytics pixel quietly collects visitor data (IP address, browser, screen size, cookie values, URL) and sends it to a third party. Plaintiff firms find this by inspecting network traffic in a browser. Claims started with chatbots, then session replay tools, then pixels and tags, now mobile SDKs and AI chat features are targets too.

> *"You have to broaden your thought process about what interception is."*



Matthew Pearson,
Partner, Frankfurt Kurnit Klein & Selz

Courts have broadened the legal meaning of "interception" (CIPA Section 631): duplicating a transmission to a third party while a user interacts with your site counts, even without anyone "grabbing it out of the air." Section 632 (recording confidential communications) is increasingly applied to chat widgets.



Analytics pixels run on most websites, transmitting more data than companies realize.

2 · CCPA compliance ≠ CIPA protection

CCPA is an opt-out regime. CIPA, as courts read it, requires consent before tracking fires. A fully compliant CCPA opt-out mechanism will not stop a valid CIPA claim. The two require separate responses.

> *"CCPA, which I call compliance, and CIPA, which is litigation."*



Matthew Pearson,
Partner, Frankfurt Kurnit Klein & Selz

3 · Four enforcement cases: what went wrong

HONDA

Opt-out required more steps than opting back in.

Fix: Make "reject all" as easy as "accept all."

HEALTHLINE MEDIA

Opt-out steps didn't actually disable tracking cookies.

Fix: Mechanisms must work as described.

playon

Only an "Agree" option; opt-out link didn't stop data sales.

Fix: Banners don't replace CCPA opt-out requirements.

sling

Two inconsistent mechanisms confused cookie rejection with a CCPA opt-out.

Fix: Keep tracking and data-sharing choices clearly distinct.

The resulting checklist

1. Consent and opt-out mechanisms must work together
2. Disclosures must reflect actual data practices
3. Tracking must not fire until the user consents
4. Choice must be symmetrical (equally easy to accept or reject)
5. Test the mechanism regularly to confirm it actually works

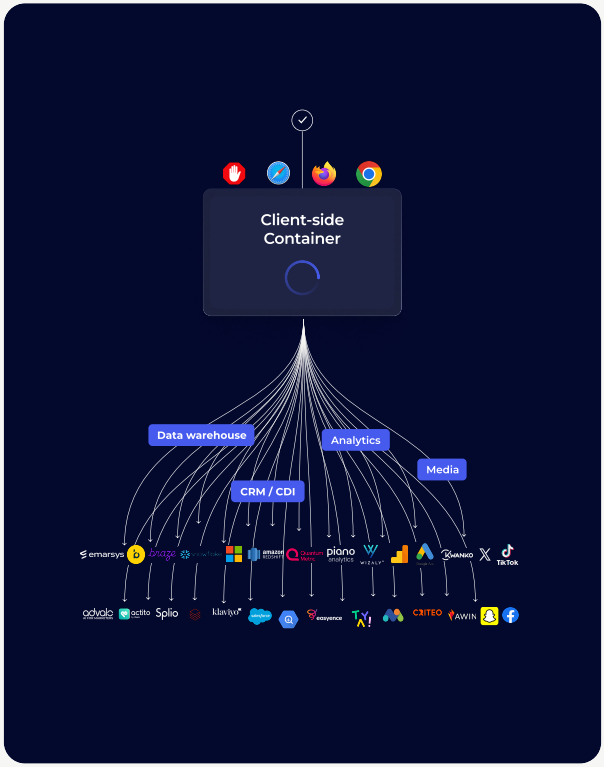
4 · The risk matrix

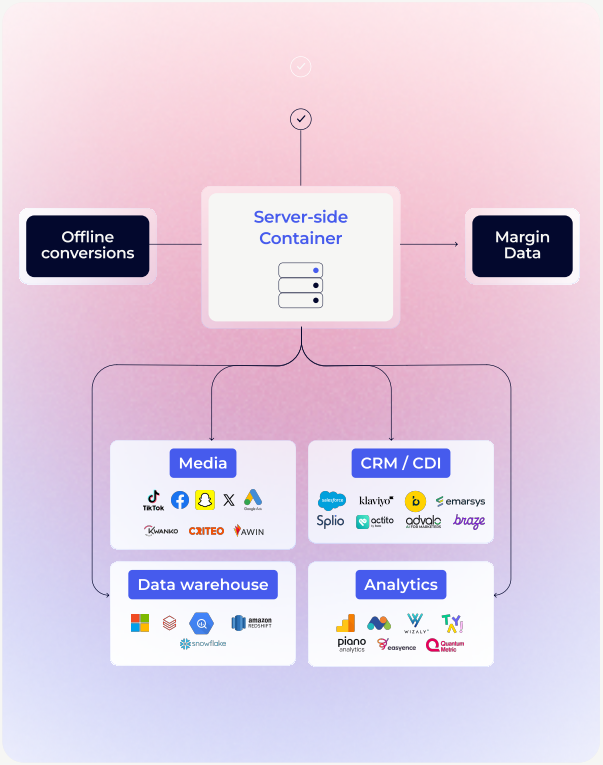
Exposure moves along two axes: how sensitive the site's content is (retail/news is lower risk than healthcare/finance), and whether tracking is client-side or server-side. Regardless of sensitivity, moving from client-side to server-side reduces exposure — because server-side removes the "interception" that plaintiff firms look for.



5 · Server-side tracking as structural mitigation

With client-side tracking (still 70–80% of websites), the browser sends data directly and simultaneously to every third party — exactly what plaintiff firms find when inspecting network traffic. Server-side tracking routes data through a server the website owns first; that server decides what to forward, and to whom, based on consent signals. From the outside, only traffic to the site's own domain is visible.





> *“99.9999% of lawsuits filed thus far are all client-side tags. And the one where they focused on server-side said it's no CIPA violation.”*



Matthew Pearson,
Partner, Frankfurt Kurnit Klein & Selz

Server-side tracking doesn't hide data. It gives the website owner more visibility: every request is logged, every consent signal recorded, every forwarding decision documented. It also bypasses ad blockers and browser restrictions like Safari's ITP, improving conversion attribution and campaign data quality.

NOT A TRADE-OFF

Server-side tracking isn't about choosing performance over privacy. It gives you both: cleaner marketing signals, and an audit log you can hand to a regulator or your DPO.

6 · Closing the loop: consent + server-side monitoring

Didomi's Consent Management Platform and Addingwell's server-side infrastructure connect consent state directly to tag firing. With Event Consent Monitoring, every event logs whether consent was given, which tags fired, what was sent to which partner, and whether it was compliant, surfacing misconfigurations in real time instead of through a demand letter.

WITHOUT EVENT CONSENT MONITORING

Server-side tagging blackbox



- Requires access to raw server logs.
- Misconfigurations go undetected.
- Regulators still asking for proof.

WITH EVENT CONSENT MONITORING

Continuous, automated view of consent compliance



- End-to-end, per-tag, per-vendor consent visibility.
- Misconfigurations surfaced automatically.
- Auditable record you can share with your DPO.

> *I can't tell you how many times I get a lawsuit and I get on the phone with a client and they're like, 'We know we're running it, but I'm not entirely sure what's going on, and when it was going.'*



Matthew Pearson,
Partner, Frankfurt Kurnit Klein & Selz

Bottom line

CCPA compliance and CIPA litigation risk are two different problems. Server-side tracking removes the technical basis for most CIPA claims; consent built around the lessons from these enforcement cases closes the remaining gap. Getting both right is the objective.



Any questions?
Get in touch with our team!

Contact us ›