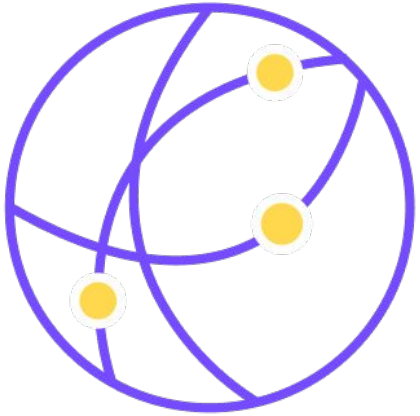
PrivadoAI

Frankfurt Kurnit Klein + Selz PC

Beyond the Website

How CIPA Applies to Mobile Apps and How to Reduce Your Exposure



July 2026

Matt Pearson
Partner, Litigation Group
Frankfurt Kurnit
mpearson@fkks.com

Romit Raj
Founding product manager
Privado AI
https://www.privado.ai/

Frankfurt Kurnit Klein + Selz PC

PrivadoAI

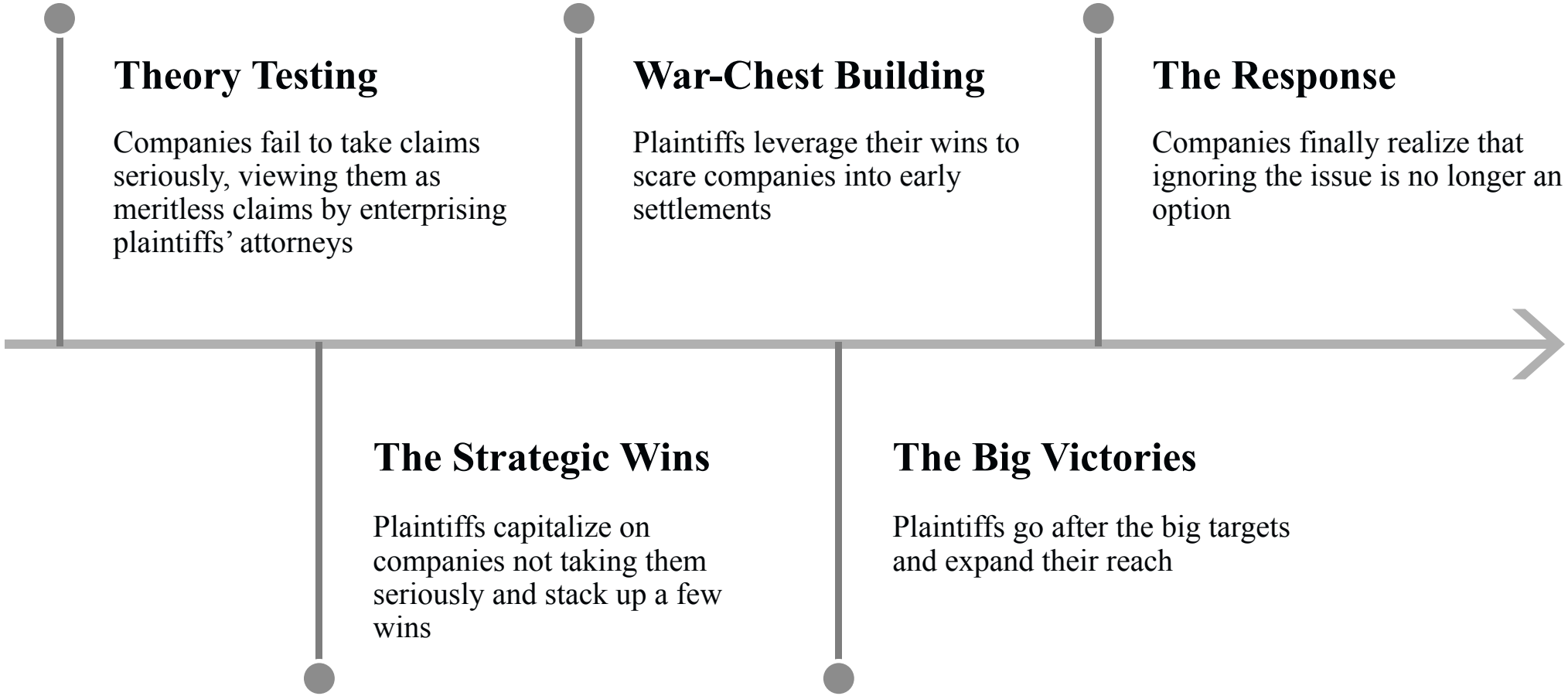
Agenda

1. Online Collection Claims
2. Web vs. App
3. Preparation

Online Collection Claims

Frankfurt Kurnit Klein + Selz PC

The Life Cycle of Privacy Claims



Frankfurt Kurnit Klein + Selz PC

Plaintiffs' Theory

- The "surreptitious" collection by third parties of information "about" website or app visitors

Technologies at Issue

- Pixels / Tags / Beacons
- Analytics & Other SDKs
- Session Replay Tools

State and Federal Statutes

- California
  - Invasion of Privacy Act
    - Section 631
    - Section 632
    - Section 638.51
  - Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code Section 502)
  - Invasion of Privacy/Intrusion upon Seclusion
- Florida
  - Security of Communications Act (Florida Statutes Section 934.03)
- Pennsylvania
  - Wiretapping and Electronic Surveillance Control Act
- Federal
  - Electronic Communications Privacy Act
  - Video Privacy Protection Act

Exposure

1. CIPA: $5,000 per violation
2. ECPA: $100/day or $10,000
3. CDAFA: Actual damages + attorneys' fees
4. VPPA: $2,500 per violation

Unique California Visitors Per Day	Number of Trackers	Total Exposure
100	1	$182,500,000
500	2	$1,825,000,000
1,000	3	$5,475,000,000
5,000	4	$36,500,000,000
7,500	5	$68,437,500,000

Web vs. App

The Claims Are the Same

- Greenley v. Kochava, Inc. (S.D. Cal.)
  - Allegations:
    - Defendant "provides a software developer kit ('SDK') to software application ('app') developers to assist them in developing their apps."
    - App developers "allow Defendant to surreptitiously intercept location data from an app user…via its SDK."
    - Via its SDK, Defendant "collected "geolocation data[] and communications from [plaintiff's] cellular telephone," "advertisement clicks; specific communications from [ ] SDK-installed apps such as consumer's usernames, customer emails and customer IDs on their Apple or Android cellular telephone devices; search terms used by a device user; and "activities within an app after it has been installed."
- Frasco v. Flo Health (N.D. Cal.)
  - Allegations:
    - "Flo Health incorporated…SDK[s] [into its app] so that it could use [third-party] analytics tools to identify which of its users would be prime targets for advertisements keyed off the data they entered into the App."
    - "Flo Health transmitted intimate health data entered into the Flo App," as well as unique identifiers like:
      - Apple Devices (ID for Advertisers ("IDFA") and ID for Vendors ("IDFV"))
      - Android Devices (Advertising ID ("AAID") and Android ID ("ID"))
- Caldwell v. InMobi Pte Ltd. (N.D. Cal.)
  - Allegations:
    - Defendant's SDK operates as a "pen register" because it collects "dialing, routing, addressing or signaling information, including . . . .timestamped geolocation data, mobile advertising IDs, IP addresses, and other device fingerprinting details transmitted in outgoing electronic communications by their devices."

But the Evidence is Different…

Website

- Most websites require no log-in (i.e., no identification)
- IP Address
- Cookie values (first and third party)

App

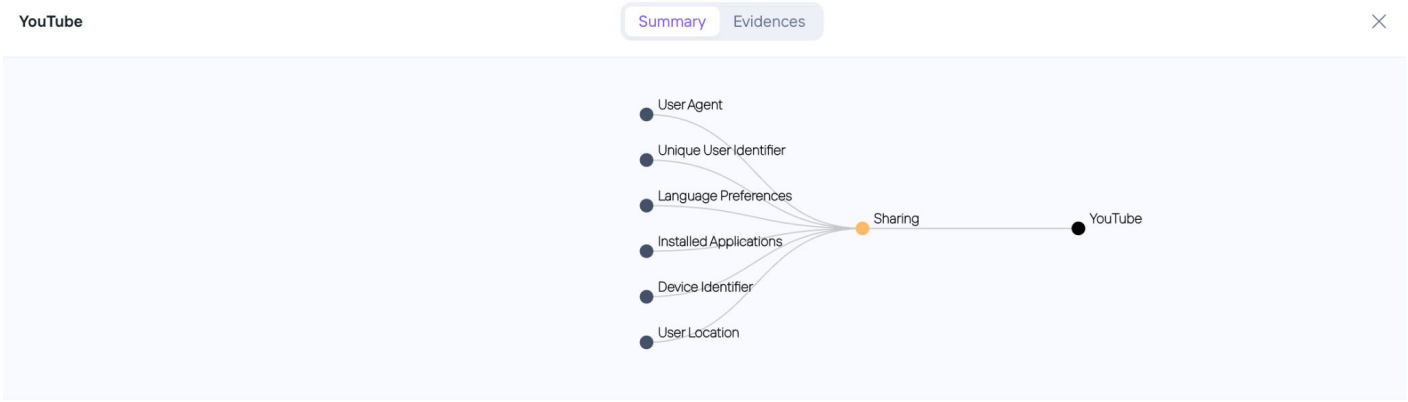
- Most apps require account creation and log in
- IP Address
- Device IDs
  - Apple Devices:
    - IDFA: same across all apps on the device (if consent provided)
    - IDFV: same only for apps from the same developer
  - Google Devices:
    - GAID: same across all apps by default

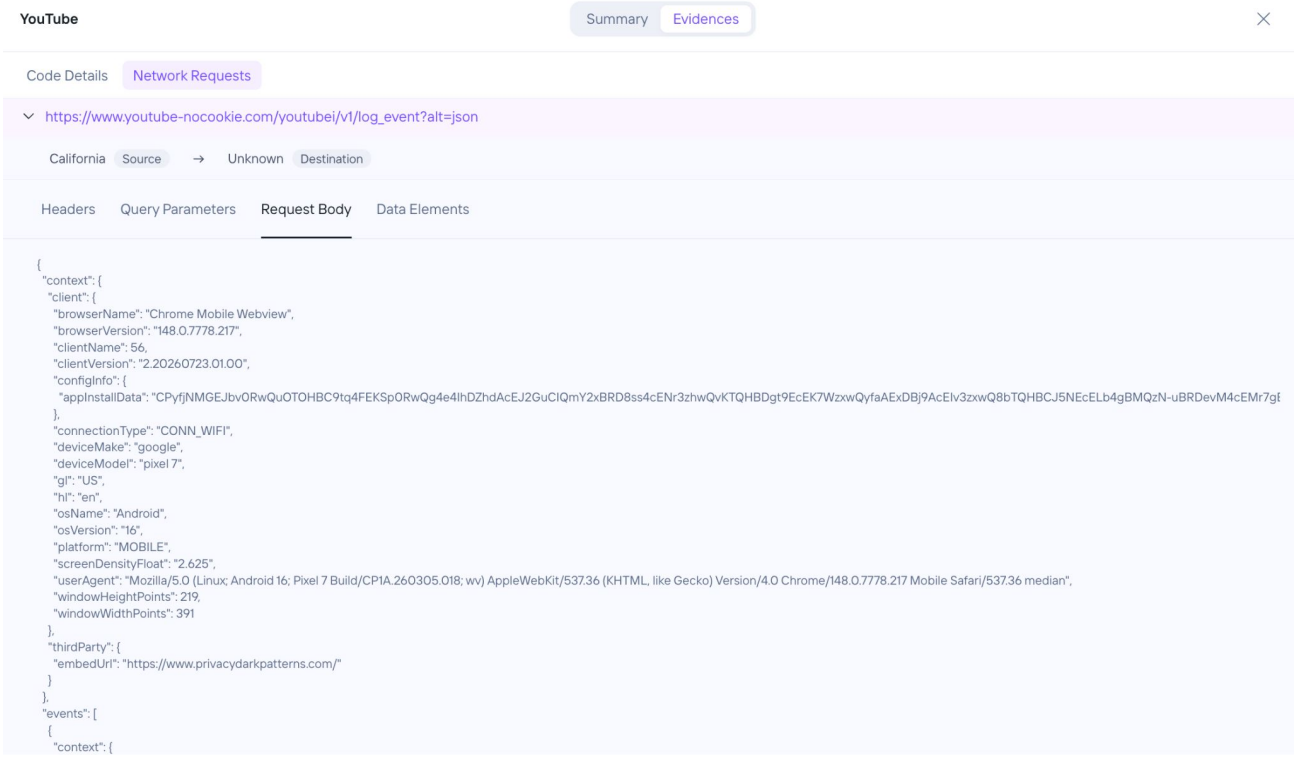
Web Payload

Query String Parameters | View source | View URL-encoded

ti	134596071
Ver	2
mid	b97f568f-1199-4414-9eb5-6a1ad7eda5ef
bo	1
sid	5f3218b0879b11f19042d776867ed5f8
vid	5f327680879b11f1a4485b308fff38ba
vids	1
msclkid	N
uach	pv=19.0.0
pi	918639831
lg	en-US
sw	1664
sh	1110
sc	24
tl	Children's Clothing and Newborn Clothing at [redacted]
p	https://www[redacted]home?lang=en_US
r	https://www.google.com/
lt	2049
mtp	10
evt	pageLoad
sv	2
cdb	AQAQ
rn	2989

App Payload





Frankfurt Kurnit Klein + Selz PC

And This Difference in Evidence Means…

- Class certification is usually easier
  - The class is usually identifiable because app users identify themselves
  - In fact, Google likely could determine, if subpoenaed, the identify of the person associated with specific GAIDs
    - Although they would likely fiercely object to any attempt by a plaintiffs' counsel to obtain this information

Class Certification Decisions

Web-Based Collection

- Unaware of any class certification orders where users did not identify themselves on the site (i.e., log in)
- Class certification denied
  - In re Meta Pixel Tax Filing Cases
  - Ingraham v. Capital One Financial Corp.

App-Based Collection

- Class certification granted
  - Frasco v. Flo Health

Why the Focus on Web-Based Claims?

- There have been thousands of online-tracking lawsuits filed, but the majority have been against website operators
- The reason?
  - It is much easier for plaintiffs' counsel to see web-based network traffic than it is for them to see app-based traffic
  - BUT that is changing…

Preparation

Step 1: Know What Is Running

- The lack of transparency cuts both ways
  - Just as it is harder for plaintiffs' counsel see what is running in an app, it is harder for companies, too
- Don't just assume that because you didn't add it, it's not there

Step 2: Know What You Need

- There is no reason to create exposure without a corresponding return on investment
- Companies should be able to explain the purpose behind every transmission

Step 3: Tailor Your Disclosures

- For litigation purposes, relying on generic or overly broad descriptions of third parties and/or information being collected is not going to work
- Be painfully transparent
- Tell users what is being collected and by whom
  - Which you cannot do unless you know what is happening

Step 4: Leverage Pre-Existing Friction

- Having multiple pop-ups on a website can denigrate the user experience and drive away traffic
- The same is not true with apps.
  - Customers expect some friction (i.e., downloading the app, creating an account, logging in), so take advantage of it
  - Get affirmatively agreement to your Terms and get acknowledgement of your Privacy Policy

Step 4: Monitor Ongoing Developments

- Complaints based on similar SDK's or third parties
- Court decisions
- Legislative response

Court of Appeal Decisions

- *Variety Media, LLC v. Superior Court,* Case No. B350578
  - Issue: Does CIPA 638.51 (pen register / trap and trace) apply to the internet and, if so, does it apply to scripts?
- *Salazar v. Paramount Global*, Case No. 25-459
  - Issue: Does a plaintiff have to purchase "audiovisual goods and services" from the defendant in order to be considered a "consumer" under the VPPA?
- *Goulart v. Cape Cod Healthcare, Inc.*, Case No. 25-1672
  - Issue: Does the crime/tort exception apply when the defendant's "primary motivation" is commercial, not tortious or criminal?

Legislative Response

- SB 690

637.2. (a) ~~A~~ ***Except as provided in subdivision (d), a*** person who has been injured by a violation of this chapter may bring an action against the person who committed the violation for the greater of the following amounts:

(1) Five thousand dollars ($5,000) per violation.

(2) Three times the amount of actual damages, if any, sustained by the plaintiff.

(b) ~~A~~ ***Except as provided in subdivision (d), a*** person may, in accordance with Chapter 3 (commencing with Section 525) of Title 7 of Part 2 of the Code of Civil Procedure, bring an action to enjoin and restrain a violation of this chapter and may, in the same action, seek damages as provided by subdivision (a).

(c) It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.

~~(d) This section does not apply to the processing of personal information for a commercial business purpose.~~

(d) (1) An action against a private actor for a violation of section 638.51 alleged to arise from conduct occurring on an internet website, online application, or mobile application may be brought under this section only by the Attorney General.

(2) The amendments to this section by Senate Bill No. 690 of the 2025-2026 Regular Session apply retroactively to any pending claim in an action commenced within two years before the operative date of that legislation.

How Privado Closes the Gap

- **Automated App Scanning**
  Privado scans iOS and Android apps the same way it scans websites — detecting what data is collected, by whom, and whether consent was properly obtained.

- **Third-Party SDK Detection**
  Identifies every active SDK, ad network, and analytics library — including ones your dev team didn't know were still running.

- **Consent Gap Analysis**
  Surfaces cases where data is leaving the app without a valid consent signal — even when the consent UI appears to be functioning correctly.

What Privado Actually Catches

- **Location Data to Ad Networks**
  Precise location being passed to advertising SDKs — often without explicit user consent or disclosure in the app store listing..

- **Health-Related Values Leaving in Background**
  Sensitive data transmitted silently during background app activity — invisible to the user and to manual review processes.

- **SDKs Firing Despite Consent Denial**
  Third-party libraries transmitting data regardless of the consent signal recorded by the UI — the Tilting Point failure, at scale.

Catch It Before They Do

- **The Question to Ask Your Team**

  Can you name every SDK active in your iOS and Android apps right now? Can you confirm each one has a valid consent signal before it fires?

  If the answer is uncertain, the exposure is real. Privado catches this before your users, a regulator, or Apple does.

Questions?

App Auditor

Detect all mobile app privacy risks with Privado AI

- **Identify all 3rd party activity:** SDKs and data flows
- **Flag all non-compliant data sharing** to 3rd parties
- **Verify consent management platforms adhere** to applicable regulations worldwide