Sheppard

ACC Association of Corporate Counsel SAN DIEGO

Emerging Trends in Privacy & Data-Breach Litigation

Presented by Wynter Deagle,
Chris Zohlen, and Ceci Fuentes

February 27, 2026

Panelists

Wynter Deagle

Partner | Sheppard
88.720.8947
wdeagle@sheppard.com

Ceci Fuentes

Privacy Program Manager | Torrid
CFuentes@torrid.com

Chris Zohlen

Manager Director | FTI Consulting
415.307.4956
Chris.zohlen@fticonsulting.com

Overview of Discussion

- Current Litigation landscape: consumer class actions, AG enforcement, federal regulator priorities
- How cookie related claims, pixel tracking, and analytics tool data flows are driving new exposure
- Recent cases shaping risk (e.g., wiretap claims, session replay cases, biometric privacy disputes)
- Increasing emphasis on “technical specificity” allegations and forensic detail in complaints

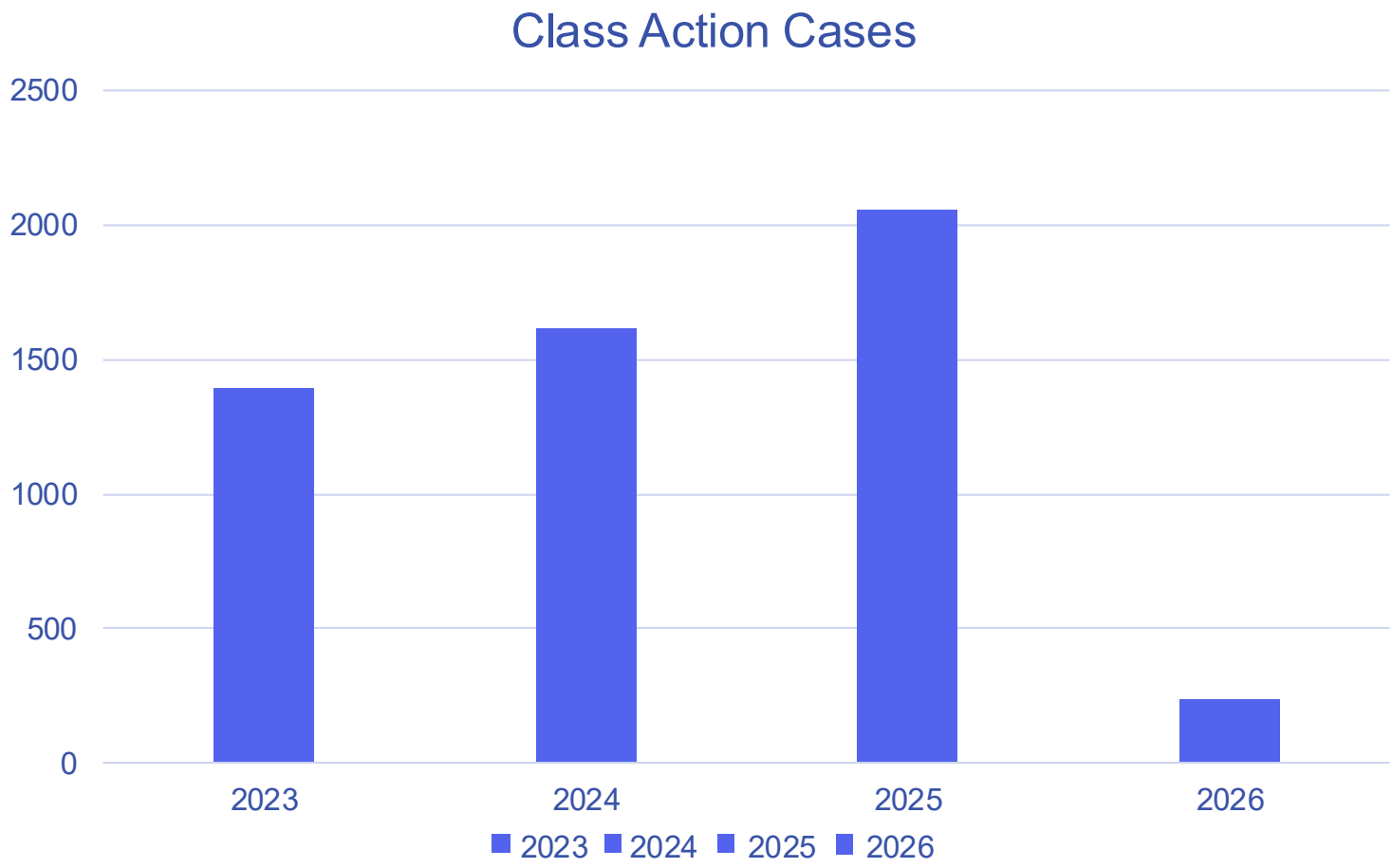
Sheppard

ACC Association of Corporate Counsel
SAN DIEGO

Current Litigation Landscape

Consumer Class Actions

- There has been a gradual and sustained increase in consumer class actions within privacy litigation over recent years.
- 2025 marked a significant spike, with class actions accounting for 32% of all litigation matters filed that year.
- As of February 2026, 236 class actions have already been filed, signaling continued momentum into the new year.
- Data Breaches: still one of the fastest growing areas.



AG Enforcement

- Landscape has shifted from compliance expectations to active, aggressive enforcements.
- Key Enforcement Themes
  - Failure to honor Global Privacy Control (GPC) opt-out signals.
  - Excessive data collection to process consumer privacy requests.
  - Inadequate vendor contracts lacking required privacy terms.
  - Children's data privacy violations.
  - Data broker registration failures.
  - Data breach notification failures and inadequate security safeguards.

AG Enforcement: Settlements

- California
  - 1.55M settlement with health website - for failing to honor opt-out requests (including Global Privacy Control signals), sharing sensitive health data with ad partners, and having a broken cookie consent banner.
  - $530,000 settlement with streaming service: for an insufficient opt-out mechanism, excessive data collection from logged-in users, no opt-out option within the app, and sharing data of known under-16 users without required consent.
- Connecticut
  - $85,000 settlement with online ticket marketplace- first monetary penalty under the CTDPA- after the company repeatedly misrepresented to the AG's office that it had corrected deficiencies flagged in a 2023 cure notice.
- Multistate Coalition
  - $5.1M settlement with education technology company- for a data breach exposing millions of students' data.

Federal Regulator Priorities

- Children's and Teen's Online Privacy
  - Amendments to COPAA: Expanded requirements for online operators collecting data from children under 13, including a written security program and enhanced parental control over use and sharing.
  - FTC has brought multiple enforcement actions under COPPA:
    - Media company agreed to pay $10 million civil penalty and designate each video it posts as "Not Made for Kids" or "Made for Kids."
    - $20M settlement with a gaming company; the company also agreed to block children under 16 from making in-game purchases without parental consent.
- Data Security
- FTC continues to prioritize data security, deception, and fraud enforcements.
  - Example: FTC acted against motor vehicle company for sharing geolocation data and driving behavior data without consent.
- Artificial Intelligence
- Focus on false claims about a company's AI offerings.
  - Pursued under Section 5 of the FTC ACT.
  - Example: brought action against AI company for misrepresenting the accuracy of its AI content detection products.

Cookie Claims, Pixel Tracking & Analytics Tools: Emerging Legal Exposure

Cookie Claims, Pixel Tracking & Analytics Tools: Overview

- Ongoing surge in cases.
- Online technologies at issue:
  - Chatbots
  - Session Replay: mouse movements, clicks, typing, browsing
  - Cookies/Pixels: MetaPixel, Google Pixel, Google Analytics
  - Trap & Trace or Pen Register claims
  - Privacy of video-viewing behavior: Video Privacy Protection Act (VPPA)
  - Search bar claims
- California courts handling majority of cases.
  - California Invasion of Privacy Act (CIPA), Cal. Penal Code sections 630 –638.55 -used to challenge websites' use of cookies, pixels and similar tracking tools to track and share website visitor data to third parties

Cookie Claims, Pixel Tracking & Analytics Tools: Overview

- Common argument that session-replay and related tools (e.g., tags, pixels, SDKs, and analytics) function as unauthorized “recordings” or “interceptions” of website communications.
- Claims have expanded to include third-party software providers as alleged co-recorders, raising questions about third-party liability and data-sharing practices.
- Courts are increasingly requiring plaintiffs to plead concrete, particularized injury to establish standing
  - *Rodriguez v. Autotrader.com, Inc.,* Case No. 2:24-cv-08735-RGK-JC, C.D. Cal., dismissed CIPA claims with prejudice for lack of standing, finding that a “statutory tester” seeking out privacy violations has no reasonable expectation of privacy.

Recent Cases Shaping Risk

Recent Notable Cases & Developments

- *Frasco v. Flo Health, Inc.,* 3:21-cv-00757, N.D. Cal., jury verdict against Meta
- *Sanchez v. Cars.com, Inc.* and *Aviles v. LiveRamp, Inc.* (CA Superior Courts, Feb. 2025): Both courts rejected the theory that web beacons or pixels tracking IP addresses constitute illegal "pen registers" or "trap and trace" devices under CIPA.
- *Salazar v. Paramount Glob.,* 133 F.4th 642, 650–651 (6th Cir. 2025)., SCOTUS to visit who qualifies as a "consumer" under the Video Privacy Protection Act ("VPPA").
- *Rodriguez v. Google LLC,* case no. 3:20-cv-04688, N.D. Cal., $425MM jury verdict confirmed.
  - Declined to find violation of the California Data Access and Fraud Act.
- *Doe v. Eating Recovery Center LLC*, summary judgment granted in favor of ERC (Meta Pixel case)
  - Applied the rule of lenity and held that any ambiguities in CIPA should be resolved in defendants' favor.
- *Taylor v. Converse Now Technologies,* case no. 25-cv-00990, N.D. Cal.
  - Denied Motion to Dismiss, focused on whether chatbot provider could be treated as a "third party" interceptor.

Increased Emphasis on Technicality in Complaints

Speculative Allegations= Not Enough

- Increased trend of requiring concrete facts of privacy violation in Complaint.
  - *Rodriguez v. ByteDance, Inc.*, No. 23 CV 4953, 2025 WL 2495865 (N.D. Ill. Aug. 29, 2025)
    - Dismissed CIPA and Electronic Communications Privacy Act claims because allegations that company used personal data to train AI systems were overly speculative absent more concrete facts about eavesdropping.
  - *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025)
    - Affirmed lower court's decision, concluding that plaintiff failed to allege a concrete injury related to a website's use of session replay technology.

The Internet – Simplified

When you visit a website, information is exchanged with various parties – in many cases this information is collected to support analytics tracking and targeted advertising.

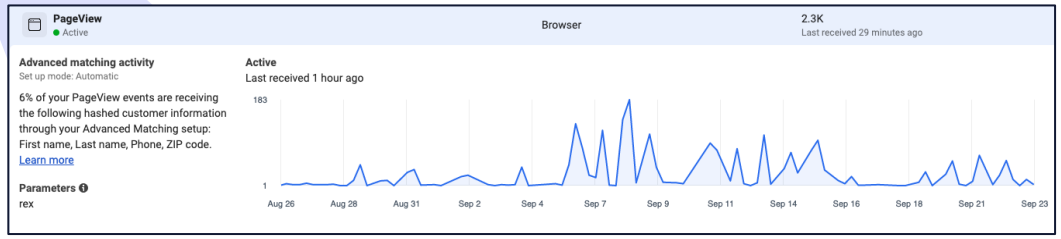
Response / Request

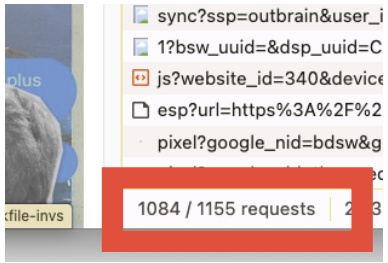
Request / Response

Web Server

Database

Analytics Dashboard
E.g. Meta Pixel Dashboard





F12 in Chrome → Network
Within 10 seconds of loading

AdTech Risks Taxonomy – The Targets

Pixels and Analytics

Send URLs, search terms, titles, referrers, and identifiers to third parties

Drives most CIPA, ECPA, VPPA, and HIPAA-style claims when firing before consent or leaking sensitive page data

Session Replay Tools

Capture clicks, scrolls, and sometimes keystrokes or form inputs

Frequently alleged as “recording” or “interception”

Chat Widgets and Webforms

Load inside i-frames but often fire events on open or message send

Plaintiffs treat chat as a modern phone call, even metadata can appear as “intercepted communications”

Video Players with Attached Tracking

Send video titles or IDs plus device identifiers

Core trigger for VPPA claims when any video content exists on the site

Mobile SDKs

Collect device IDs, app events, and behavior signals

Creates health, finance, and children’s data exposure

Often bypasses web-style consent controls

What needs to work correctly.. Every time

Orchestration across this ecosystem determines compliance, not any single tool.

DATA FLOW LAYER

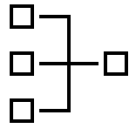
Banner Selection

Global Privacy Control (GPC) Signal

Consumer Rights Request

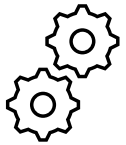
User Interaction

User sends consent/opt-out preferences



Consent Management Platform

Collects consent/ opt-out data



Tag Management System

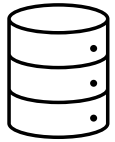
Controls which pixels/tags are deployed

online

offline

Online Tracking

Online trackers suppressed per consent choice and contracts maintained with service providers and third parties



Customer Data Platform / Back End Systems

Ensures downstream sharing is aligned with user choice

Downstream Third Parties

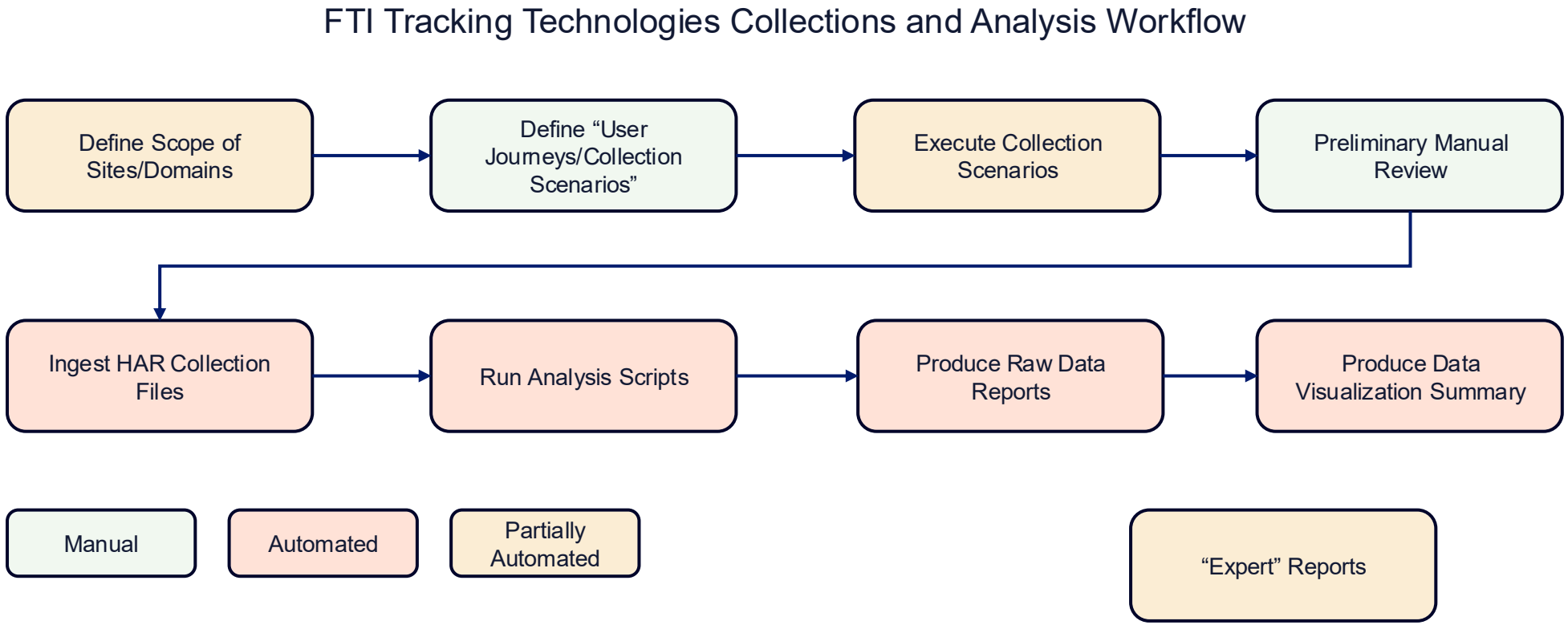
Must respect consent choice and suppression flags

STAKEHOLDERS

Agencies MarTech
Website Developers / IT
Legal / Data Privacy
Outside Counsel
Business Owners

The process to identify what happens

This work can be performed both proactively (compliance and preemptive remediation) and reactively (litigation or regulator request for information)



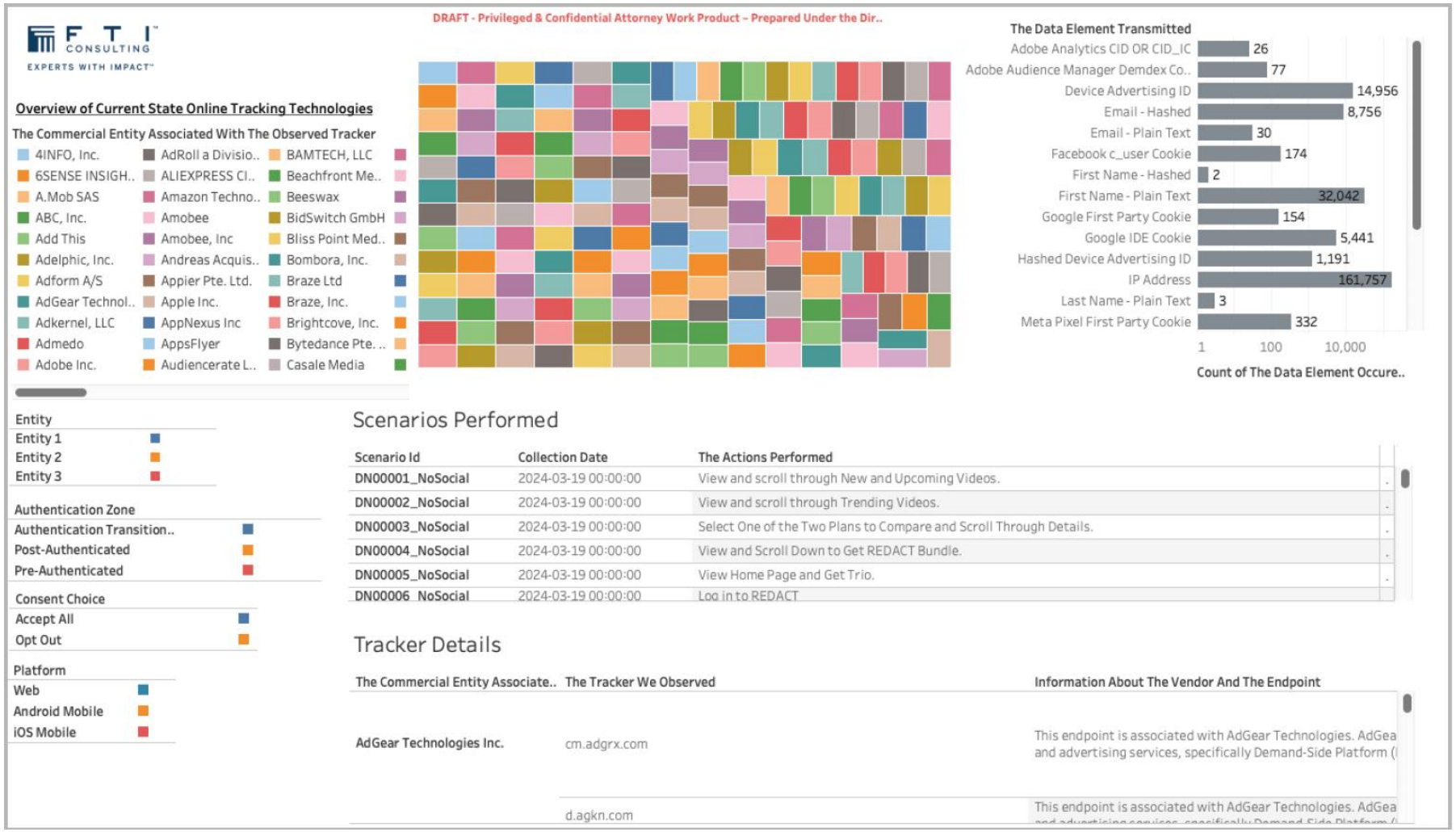
The Evidence

- **Accurate reconstruction** – Independently recreate the user journey and capture what happened.
- **Precise data evidence** – Preserve HAR / Network logs to verify what data was transmitted and what was not from the website or mobile app.
- **Historical analysis** – Analyze Tag Manager versions, script changes, and page configurations at the time of the visit to clarify which tags were active and eliminate false positives. This includes configuration(s) of Adtech ecosystem dashboards (Meta, Google, X, etc.)
- **Consent behavior validation** – Prove whether tracking fired before or after consent or GPC.
- **Payload analysis** – Determine whether any video titles, health terms, or identifiers ever left the site.
- **Expert testimony support** – Provide qualified technical experts who can explain browser behavior, pixel mechanics, and consent logic in court and withstands cross-examination.
- **Defensible chain of custody** – Collect and preserve evidence using forensic standards trusted by courts and regulators.

Sample Output

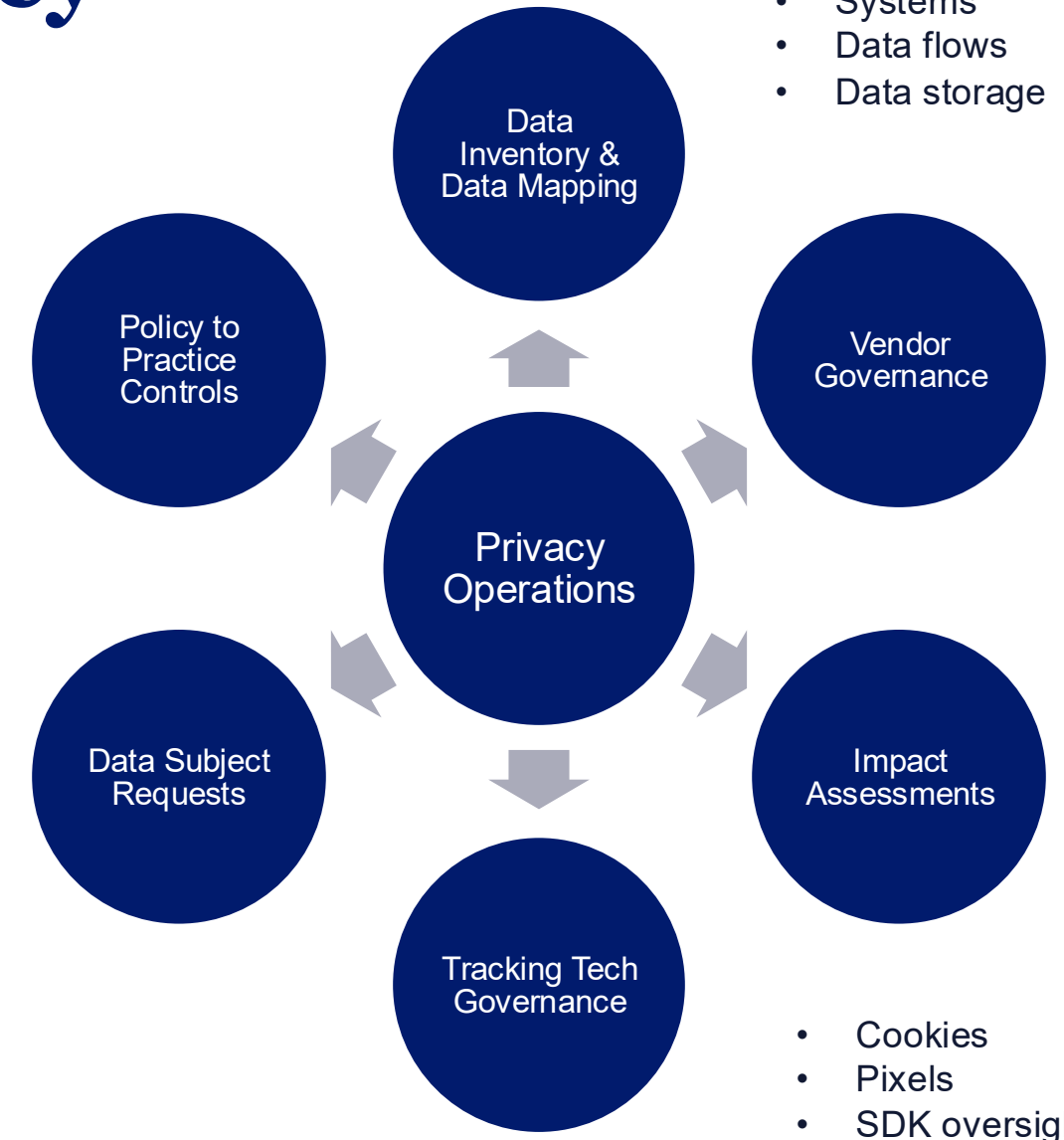
Identify:

- External parties
- Data transmitted
- The domain
- Consent choice
- The platform (web/mobile)
- When it happened



Inside Privacy Operations

- Translating legal requirements
- Implementing stated policy into daily operational workflows
- Defined data retention periods



- Systems
- Data flows
- Data storage

- Onboarding
- DPAs
- Third-Party Risk Assessments

- Intake and verification
- SLA tracking
- Audit logs

- PIA/DPIA
- New projects / systems
- Risk identification and mitigation

- Cookies
- Pixels
- SDK oversight

Operational Challenges & Common Gaps

Where Things Break Down:

- Fragmented communication across Marketing, IT, and Legal
- Limited visibility into new vendors / deployments
- Rush to go-live and limited timing
- Manual processes across multiple systems and lack of system integration
- Competing business priorities

Misalignment creates risk

Coordination & Compliance

What good looks like:

- Early privacy involvement in projects
- Standarized contract intake and approval processes
- Alignment across Legal, IT, and Security
- Clear ownership and escalation paths
- Continuous monitoring and testing

Role in Incident & Litigation Response

Privacy Operations acts as the Fact Engine and we:

- Gather system level facts quickly
- Recontrcust data flows
- Validate disclosures vs. practices
- Provide DSAR and consent logs
- Support defensible legal narratives