November 2025

Digital Marketing and Consumer Surveillance – What You Need to Know to Avoid and Defend Consumer Class Actions

David White, Partner
AlixPartners LLP

Jacqueline Cooney, Partner,
Arnall Golden Gregory LLP

Speakers

David White

Partner & Managing Director
AlixPartners LLP

Jacqueline Cooney

Partner
Arnall Golden Gregory LLP

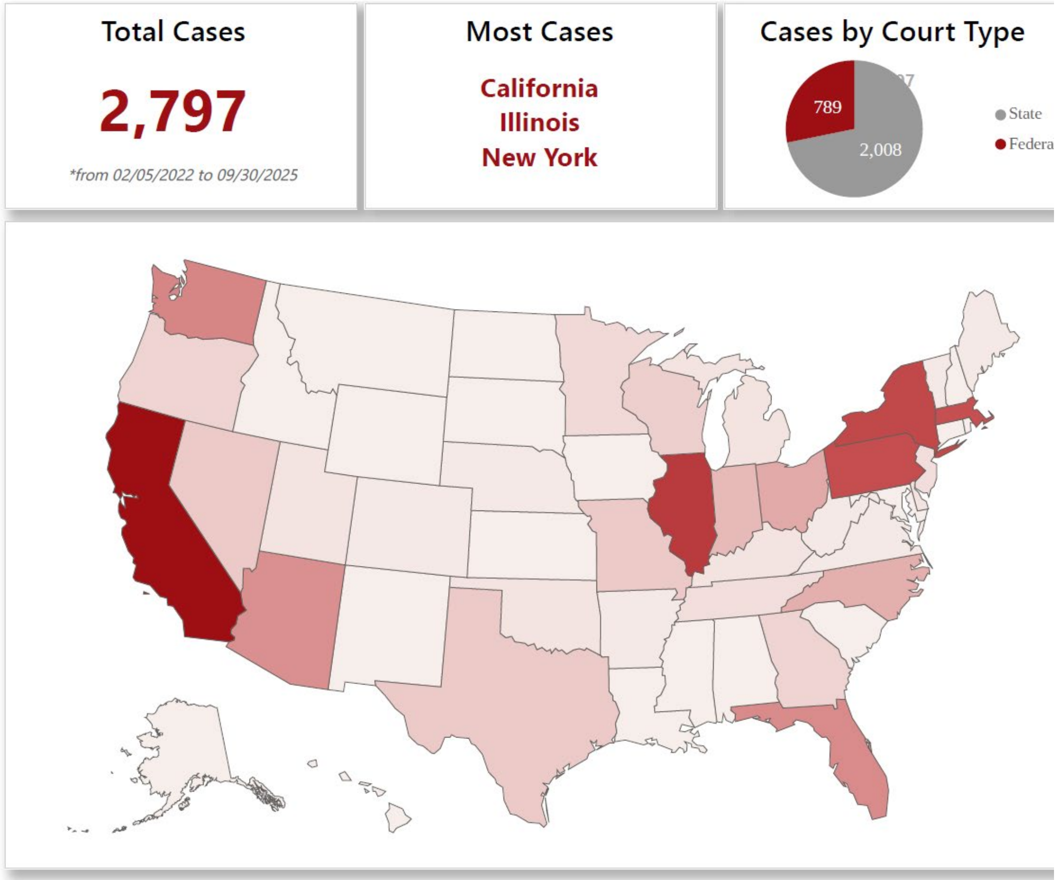
Recent Case Law

Privacy+
Security
Forum

Why this matters now

Nearly 3000 wiretapping privacy cases filed since the Ninth Circuit issued its ruling in *Javier v. Assurance IQ, LLC et al. on May 31, 2022*

1. Plaintiffs are weaponizing wiretap statutes, VPPA, unfair-practice laws, and privacy misrepresentation claims
2. Regulator heat: FTC actions, HHS/OCR guidance (health data + pixels), and AG inquiries are reshaping risk
3. Damages stack fast (e.g., VPPA $2,500 per violation; class sizes = site visitors)



Total Cases

2,797

*from 02/05/2022 to 09/30/2025

Most Cases

California
Illinois
New York

Cases by Court Type

Source: https://www.fisherphillips.com/

Common causes of action & elements

Common Causes of Action and Elements

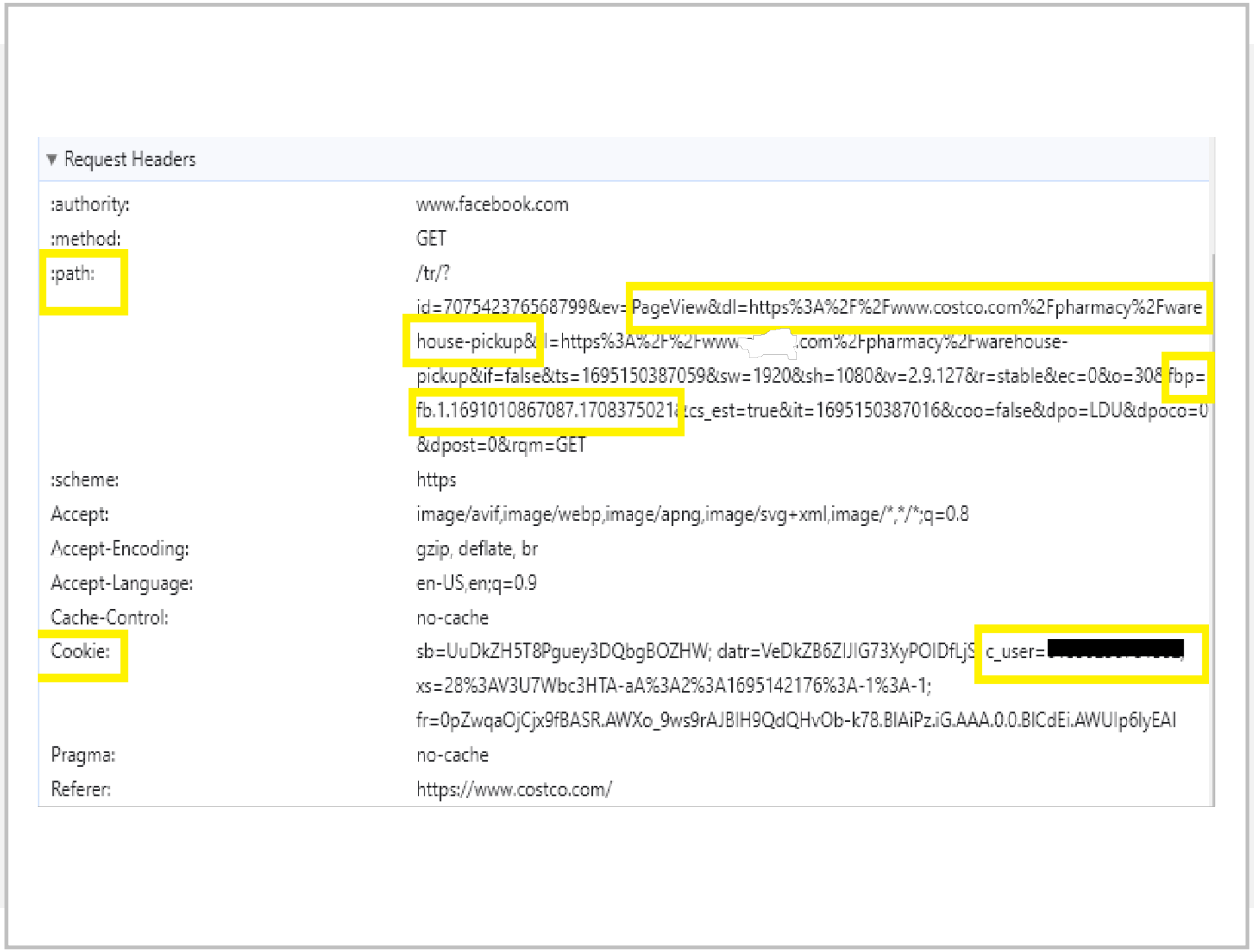
- Federal/State wiretap: ‘interception’ of a communication without consent, content-in-transit, third-party participation theories
- HIPAA: health data, covered entities, and health like data
- VPPA: who’s a ‘subscriber’, what’s ‘personally identifiable’, video pages beyond media sites
- Common Law -UDA(P) / deception: privacy-notice mismatch vs. actual tracking/sharing

Key Cases Under the California Invasion of Privacy Act (CIPA)

- Greenley v. Kochava Inc.
- Licea v. Hickory Farms LLC
- Levings v. Choice Hotels Intern., Inc.
- Calhoun v. Google LLC
- *Doe v. Eating Recovery Center*

Motion-to-dismiss trends

- **Standing:** concrete injury via unauthorized disclosure vs. purely technical violations
- **Definitions:** statutory definitions of wiretaps interpreted differently
- **Consent:** banner quality, scope, and whether it covers third-party advertising uses
- **Content vs. non-content:** what the script actually captured (form fields, URLs, video titles)
- **Communications vs Non-Communications**
- Read while **in transit**



```
▼ Request Headers
:authority:          www.facebook.com
:method:             GET
:path:               /tr/?
                     id=707542376568799&ev=PageView&dl=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fware
                     house-pickup& l=https%3A%2F%2Fwww.      .com%2Fpharmacy%2Fwarehouse-
                     pickup&if=false&ts=1695150387059&sw=1920&sh=1080&v=2.9.127&r=stable&ec=0&o=308 fbp=
                     fb.1.1691010867087.1708375021 cs_est=true&it=1695150387016&coo=false&dpo=LDU&dpoco=0
                     &dpost=0&rqm=GET
:scheme:             https
Accept:              image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:     gzip, deflate, br
Accept-Language:     en-US,en;q=0.9
Cache-Control:       no-cache
Cookie:              sb=UuDkZH5T8Pguey3DQbgBOZHW; datr=VeDkZB6ZIJIG73XyPOIDfLjS c_user=[redacted]
                     xs=28%3AV3U7Wbc3HTA-aA%3A2%3A1695142176%3A-1%3A-1;
                     fr=0pZwqaOjCjx9fBASR.AWXo_9ws9rAJBIH9QdQHvOb-k78.BlAiPz.iG.AAA.0.0.BlCdEi.AWUIp6lyEAI
Pragma:              no-cache
Referer:             https://www.costco.com/
```

Class certification & damages

Privacy+ Security Forum

Considerations for Courts Certifying a Class and Determining Damages

Predominance/ Commonality fights: user-by-user consent and varying site versions/configurations

Damages models: per-capita statutory vs. aggregate unjust enrichment

Identifiable Consumers/ Purchasers vs web site visitors

Injunctive relief: code/config changes, programmatic audits, vendor restrictions

VPPA Revival Specifics

Broadened Definitions

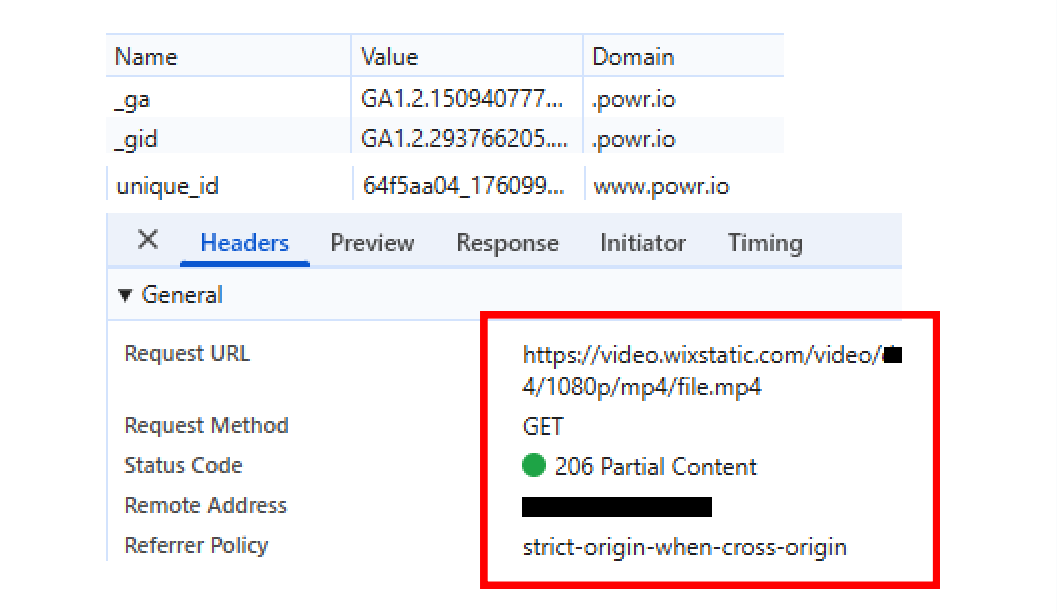
Definitions of ‘Video Tape Service Provider’, ‘Consumers’, and ‘Subscribers’, have broadened to include modern technologies

Plaintiffs have argued that device IDs, social media IDs, or replayed data can constitute PII

The ordinary person standard adopted by the Second Circuit in Solomon v. Flipps Media and affirmed in Hughes v. NFL now requires courts to assess if an ordinary person could use the data received to link video viewing to an individual

Typical Evidence

Data streams containing both behaviors and unique identifiers. When coupled with a unique video names could then be used to create a profile



Name	Value	Domain
_ga	GA1.2.150940777...	.powr.io
_gid	GA1.2.293766205....	.powr.io
unique_id	64f5aa04_176099...	www.powr.io

▼ General

Request URL: https://video.wixstatic.com/video/[redacted]4/1080p/mp4/file.mp4

Request Method: GET

Status Code: ● 206 Partial Content

Remote Address: [redacted]

Referrer Policy: strict-origin-when-cross-origin

Technical & Litigation Challenges

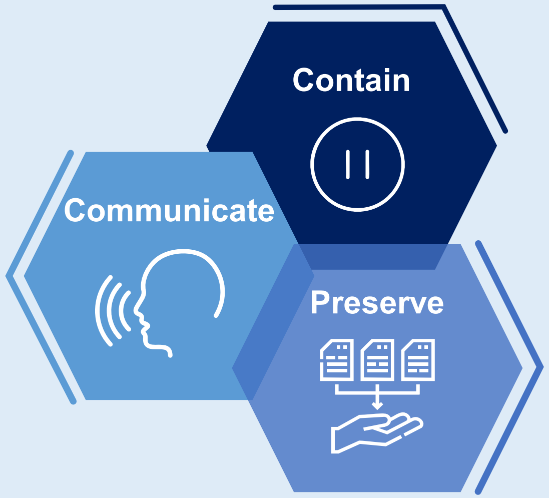
Privacy+
Security
Forum

Preservation vs. Remediation

Day-One Playbook

If a case is filed against you, there are some immediate, organized actions to take that will prioritize containment, preservation, and communication

Pause (not purge) affected containers and tags. Disable compromised accounts, endpoints, or services as needed



Issue litigation holds to all connected 3rd party vendors and platforms

In addition to easily exportable data like logs and version history, collect screen shots of settings and configurations before they can be changed

Create and document a timeline from initial discovery to final remediation

Build a Response Team

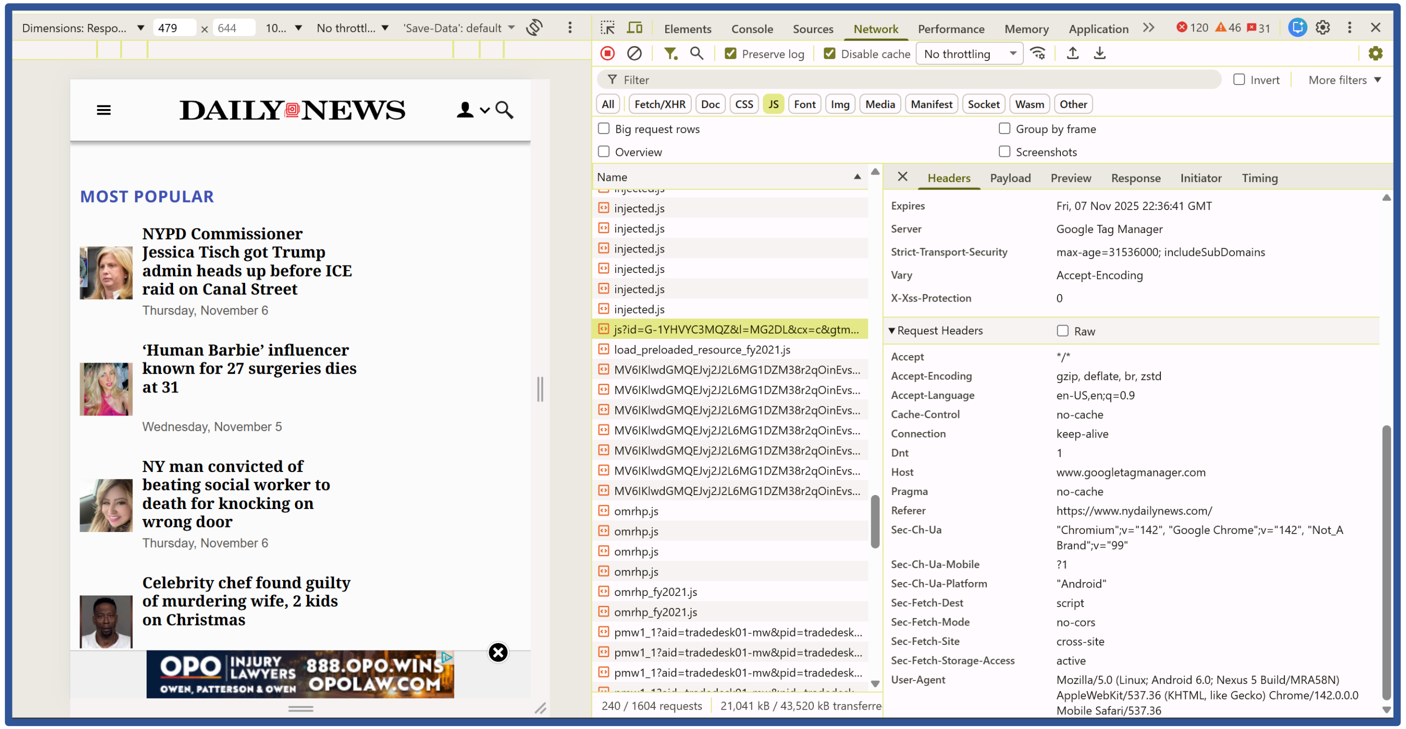
Activate your cross-functional incident response team:

- Litigation coordinators: Define scope, issue holds, establish privilege
- Web forensics experts: Collect and analyze traffic, build defensible data flows
- Tag manager experts: Analyze affected tags, triggers, and API connections
- Network/web engineers: Identify and isolate compromised systems, trace potential attack vectors
- Privacy counsel: Triage sensitive data, map user data to corresponding privacy policy

What to Collect

Data Types to Collect When You Get a Claim

- Data points should be explicitly tied to elements of the claims
- Record user journeys to replicate the scenario claimed to create the alleged exposure
- Collect code snapshots, java scripts, tag manager exports & settings, and privacy policy changes
- In addition to a live snapshot, collect historic configuration changes to pinpoint when the offending change was implemented
- Collect 3rd party contracts, SDK docs, and API interactions to isolate potential outside liability


Dimensions: Respo... ▼ 479 x 644 10... ▼ No throttl... ▼ 'Save-Data': default ▼
Elements Console Sources Network Performance Memory Application >> ⊗ 120 ⚠ 46 31
☑ Preserve log ☑ Disable cache No throttling
Filter □ Invert More filters ▼
All Fetch/XHR Doc CSS JS Font Img Media Manifest Socket Wasm Other
□ Big request rows □ Group by frame
□ Overview □ Screenshots
Headers Payload Preview Response Initiator Timing

DAILY NEWS

MOST POPULAR

NYPD Commissioner Jessica Tisch got Trump admin heads up before ICE raid on Canal Street
Thursday, November 6

'Human Barbie' influencer known for 27 surgeries dies at 31
Wednesday, November 5

NY man convicted of beating social worker to death for knocking on wrong door
Thursday, November 6

Celebrity chef found guilty of murdering wife, 2 kids on Christmas

OPO INJURY LAWYERS OWEN, PATTERSON & OWEN 888.OPO.WINS OPOLAW.COM

Name
injected.js
injected.js
injected.js
injected.js
injected.js
injected.js
js?id=G-1YHVYC3MQZ&l=MG2DL&cx=c&gtm...
load_preloaded_resource_fy2021.js
MV6IKlwdGMQEJvj2J2L6MG1DZM38r2qOinEvs...
MV6IKlwdGMQEJvj2J2L6MG1DZM38r2qOinEvs...
MV6IKlwdGMQEJvj2J2L6MG1DZM38r2qOinEvs...
MV6IKlwdGMQEJvj2J2L6MG1DZM38r2qOinEvs...
MV6IKlwdGMQEJvj2J2L6MG1DZM38r2qOinEvs...
MV6IKlwdGMQEJvj2J2L6MG1DZM38r2qOinEvs...
MV6IKlwdGMQEJvj2J2L6MG1DZM38r2qOinEvs...
omrhp.js
omrhp.js
omrhp.js
omrhp.js
omrhp_fy2021.js
omrhp_fy2021.js
pmw1_1?aid=tradedesk01-mw&pid=tradedesk...
pmw1_1?aid=tradedesk01-mw&pid=tradedesk...
pmw1_1?aid=tradedesk01-mw&pid=tradedesk...

240 / 1604 requests | 21,041 kB / 43,520 kB transferre

Expires	Fri, 07 Nov 2025 22:36:41 GMT
Server	Google Tag Manager
Strict-Transport-Security	max-age=31536000; includeSubDomains
Vary	Accept-Encoding
X-Xss-Protection	0

▼ Request Headers □ Raw

Accept	*/*
Accept-Encoding	gzip, deflate, br, zstd
Accept-Language	en-US,en;q=0.9
Cache-Control	no-cache
Connection	keep-alive
Dnt	1
Host	www.googletagmanager.com
Pragma	no-cache
Referer	https://www.nydailynews.com/
Sec-Ch-Ua	"Chromium";v="142", "Google Chrome";v="142", "Not_A Brand";v="99"
Sec-Ch-Ua-Mobile	?1
Sec-Ch-Ua-Platform	"Android"
Sec-Fetch-Dest	script
Sec-Fetch-Mode	no-cors
Sec-Fetch-Site	cross-site
Sec-Fetch-Storage-Access	active
User-Agent	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Mobile Safari/537.36

- 1 Web Page
- 1604 browser requests
- 240 java scripts
- 384 Cookies

Digital Artifacts Proving or Disproving ‘interception’

First Party vs Third Party

- Develop “Customer Journeys” to show in-transit traffic: Capture HAR/PCAP evidence of field-level data transfers
- Distinguish consumer communications through their browser with the defendant company vs those with third parties
- Identify cookies used for tracking and separate 1st party from 3rd party

Analytics vs Advertising

- Differentiate functional analytics vs. ad targeting; show parameter minimization
- Distinguish company marketing from downstream 3rd party Real Time Bidding
- Attribute responsibility: who configured the event or dropped the cookie and when

Mapping General User Interaction Sequence

1 **User Visit:**
The user's browser sends an HTTP request to the website’s server

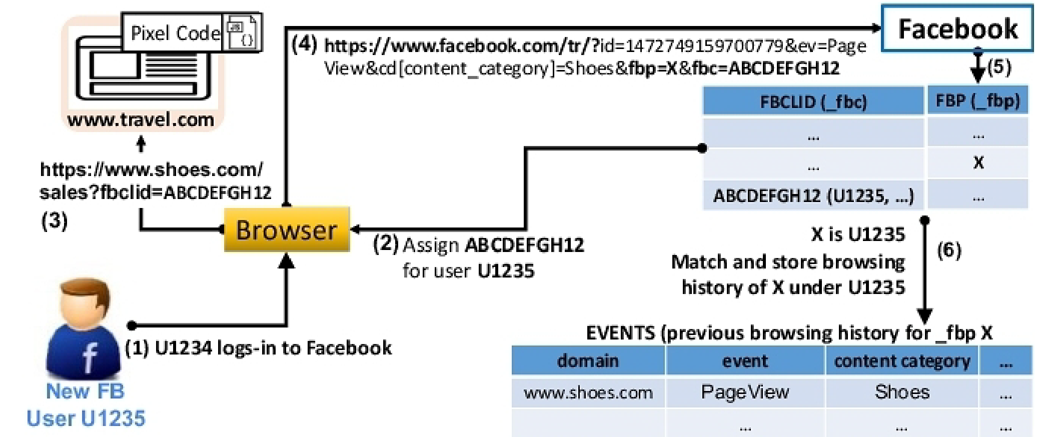
2 **Page Load and Tag Initialization:**
The website loads its core content along with embedded first-party scripts

3 **Consent and Tag Activation:**
If a consent management platform (CMP) exists, it determines which trackers may be activated

4 **First-Party Tracking:**
The website’s own analytics tools record actions such as page views, clicks, and session duration for internal metrics (performance & security)

5 **Third-Party Tracking:**
Tracking pixels are triggered based on user behavior. External scripts loaded and data is sent to the vendor

6 **Ad Delivery or Personalization:**
The aggregated attribution information allows the ad platform to serve tailored ads or content as the user continues browsing across sites


Pixel Code
www.travel.com
https://www.shoes.com/ sales?fbclid=ABCDEFGH12
(3)
Browser
(4) https://www.facebook.com/tr/?id=147274915970077 9&ev=Page View&cd[content_category]=Shoes&fbp=X&fbc=ABCDEFGH12
Facebook
(5)
(2) Assign ABCDEFGH12 for user U1235
X is U1235
Match and store browsing history of X under U1235
(6)
(1) U1234 logs-in to Facebook
New FB User U1235

FBCLID (_fbc)	FBP (_fbp)
...	...
...	X
ABCDEFGH12 (U1235, ...)	...

EVENTS (previous browsing history for _fbp X

domain	event	content category	...
www.shoes.com	PageView	Shoes	...
	...	...	...

Configuration Complexity & Drift

TMP Misconfigurations

- Multiple workspaces, versions, and human error can lead to sprawl that can increase risk.
- Tags that check for consent before executing can still collect data if they are deployed before user consent is set.
- Tags can bootstrap custom scripts that can bypass privacy controls that exist in standard functions.
- Tags can be misconfigured to automatically parse URL parameters, which could contain sensitive information.
- Deploying tags on unintended pages can potentially expose sensitive information to containers not meant to handle stricter privacy controls.

Cookie-less Tracking

- Ad tech is trending away from 3rd party unique identifiers, but it not immune to risk
- Probabilistic tracking uses statistical models and algorithms to infer a user's identity and behavior based on non-personal data points
- Digital fingerprinting creates a unique and persistent identifier for each device based on detailed system attributes that are stored server-side
- Session-replay is a process where a user journey is recorded to create better user analytics and insights
- These methods are more covert as they bypass 3rd party controls and can lead to issues without more robust and transparent privacy language

Organizational/Compliance Challenges

Privacy+
Security
Forum

Contracting & Notice Friction

Potential Issues with Contract and Notices

- Many vendors won’t sign sensitive-data terms (some expressly ban health contexts)
- Notice mismatch (promises vs. practice) = plaintiff Exhibit A
- Cross-border issues: SCCs/DPFs and profiling disclosures

Non-Exhaustive List of Contract Must Haves

- Processor/Controller Roles: Make sure these are defined (if a vendor isn’t designated as a ‘processor’ or “service provider” they might be considered a “third-party” and that affects your notice and consent requirements
- Consents: Your contract should make it clear who is responsible for getting consent from the consumer (and recording it and honoring opt-outs)
- Indemnification: Both parties should always agree to comply with applicable data protection laws and indemnify the other for violations

Operating model realities

Common Challenges

1. Marketing, product, IT, and legal own different levers—creates gaps

2. Change control for tags is weak; agencies push updates outside legal review

3. Continuous monitoring needed (tools + process), not one-time audits

4. Data protection laws change and create new regulatory requirements that need to be operationalized

5. Inadequate documentation on purposes/uses of tracking and other tech can create gaps in knowledge over time, for instance when someone with knowledge of the tech leaves

Lawful basis & minimization in practice

Privacy+ Security Forum

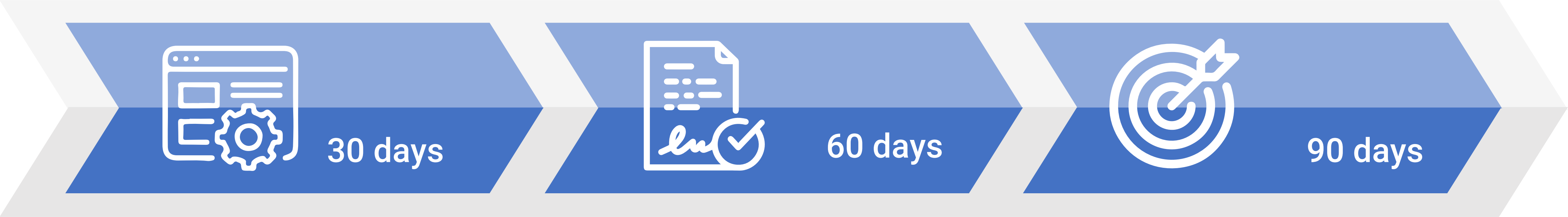
Tips to Ensuring You're Meeting Regulatory Requirements

- Map each event/parameter to a purpose and lawful basis; kill everything else
- Field-level filters & hashing with salt/pepper; IP truncation; defer IDs until consent
- Respect universal opt-out signals and consent scope; suppress IDs until consent
- Short retention windows; aggregate where possible
- De-identify data where possible; it can still be valuable for analytics purposes even if anonymized and/or aggregated

Best-Practice Playbook

Privacy+
Security
Forum

Defense-ready 30-60-90 day technical plan



30 days

Full tag inventory; blocklist sensitive selectors; freeze high-risk pages; fix notices

60 days

Contract addenda (service-provider status, no secondary use, logs access); enable allow-list deploy

90 days

DPIAs on profiling/targeted ads; server-side measurement with parameter minimization; quarterly audits

Goal is near-term risk reduction without killing Marketing Initiatives

Code & config controls that move the needle

Tips for Technical Implementation

Defined no third-party data collection (no-pixel) zones (auth, checkout, health/children pages)

Field-level filters & hashing with salt/pepper; IP truncation; defer IDs until consent

CSP/SRI, deployment allow-lists, and ‘two-person rule’ for tag changes

Pixel Settings: Limited Data Use (LDU), 1st party cookies, advanced matching

Program governance & monitoring

Tips for Creating a Defensible Governance Framework

Central Tag Governance Board (marketing + legal + security)

Change-ticketing with legal sign-off; scheduled synthetic journeys capture

Dashboarding: show delta of tags/vendors quarter-over-quarter

Conduct periodic reviews of all websites – some tags are easily implemented without going through review

Make sure you are aware of any unapproved tech

Regulators want evidence of understanding and control, not slogans

Five take-home truths

1. Plaintiffs win with mismatches (notice vs. reality) and a showing interception
2. Preserve before you fix
3. Contracts and configuration settings are evidence—treat them that way
4. Server-side tagging reduces noise, not liability, unless fields are properly minimized
5. Continuous monitoring + clear ownership beats annual audits

Questions & Contacts

David White
Partner & Managing Director
AlixPartners
909 Third Avenue 30th Floor, New York
NY 10022
dwhite@alixpartners.com

Jacqueline W Cooney
PARTNER, CO-CHAIR, PRIVACY &
CYBERSECURITY PRACTICE
ARNALL GOLDEN GREGORY LLP
2100 Pennsylvania Avenue NW
Suite 350S
Washington, D.C. 20037
jacqueline.cooney@agg.com

Q&A