IAPP **Privacy. Security. Risk. 2025**

Training 28-29 October

Workshops 29 October

Conference 30-31 October

SAN DIEGO

#PSR25

Cookie Deep Dive

Maximizing Value While Minimizing Risk

Welcome and Introductions

Amber Mednick

Managing Corporate Counsel, Privacy

T-Mobile

David Cox

Assistant General Counsel – Privacy, Data Governance & E-Discovery

Volkswagen of America

Elliot Golding

Partner

McDermott Will & Schulte

Mark Sauchelli

SVP | Senior Associate General Counsel – Marketing

U.S. Bank

Agenda Outline

I. Welcome and Introductions

II. Why Should We Care: Risks & Opportunities

III. Tracking Technology Overview

IV. Legal/Enforcement Update

V. How to Operationalize, Test, and Maximize Data/Minimize Risk

VI. Questions and Answers

Why Should We Care? (The "Stick")

- **Active enforcement with investigations and fines**
  - **US UDAP (FTC + States)**: Focus on "unfairness" (*e.g.*, collecting/sharing sensitive data without consent) and "deception" (e.g., misrepresenting data is "anonymous")
  - US State Privacy: Focus on transparency and choice
- **Significant litigation risks**
  - Wiretapping (CIPA)
  - UDAP
  - Breaches
- **Self-regulatory** (DAA, NAI, IAB, etc.)

All easily triggered by simple review of public website using freely available tools

Why Should We Care? (The "Carrot")

KEY CONSIDERATIONS

- What data is being used? First-party / third-party / both?
- Is data being made available to third parties, shared by joint controllers (Europe), or kept in-house?

EXAMPLES

- ***Publisher*:** Creating segments with first-party data and allowing third parties to target ads within various company apps and websites
- ***Data Mart*:** Creating segments and making them available for activation (without disclosing the underlying first-party data)
  - Using first-party data only or enhancing with third-party data
- ***Market Research*:** Providing insights to third parties using first-party data
- ***Other Data Monetization*:** Enhancing third-party data for a fee; linking online and offline data (identity graph)

Tracking Technology Overview

Common Tracking Technologies

"Tracking technologies" refer to a broad range of code/scripts, images, or files that collect, transmit, tag, or store information about a user, device, or online activity via website, mobile app, email, and other online interactions.

- **Cookies** are files saved locally on a user's device/browser.
- **Pixel/beacon** is a tiny graphic image or script/code placed on a webpage/in an email that collects/shares data or takes other actions.
- **Session replay tools** record a user's activities (*e.g.*, mouse movements, clicks, typing) when using a webpage or app.
- **Fingerprinting** uses a browser's and/or device's unique configurations and settings to track user activity.
- **Software Development Kits ("SDK")** are essentially the mobile app equivalent of above web-based tracker example (typically 3rd party).

Common Purposes and Data Processed

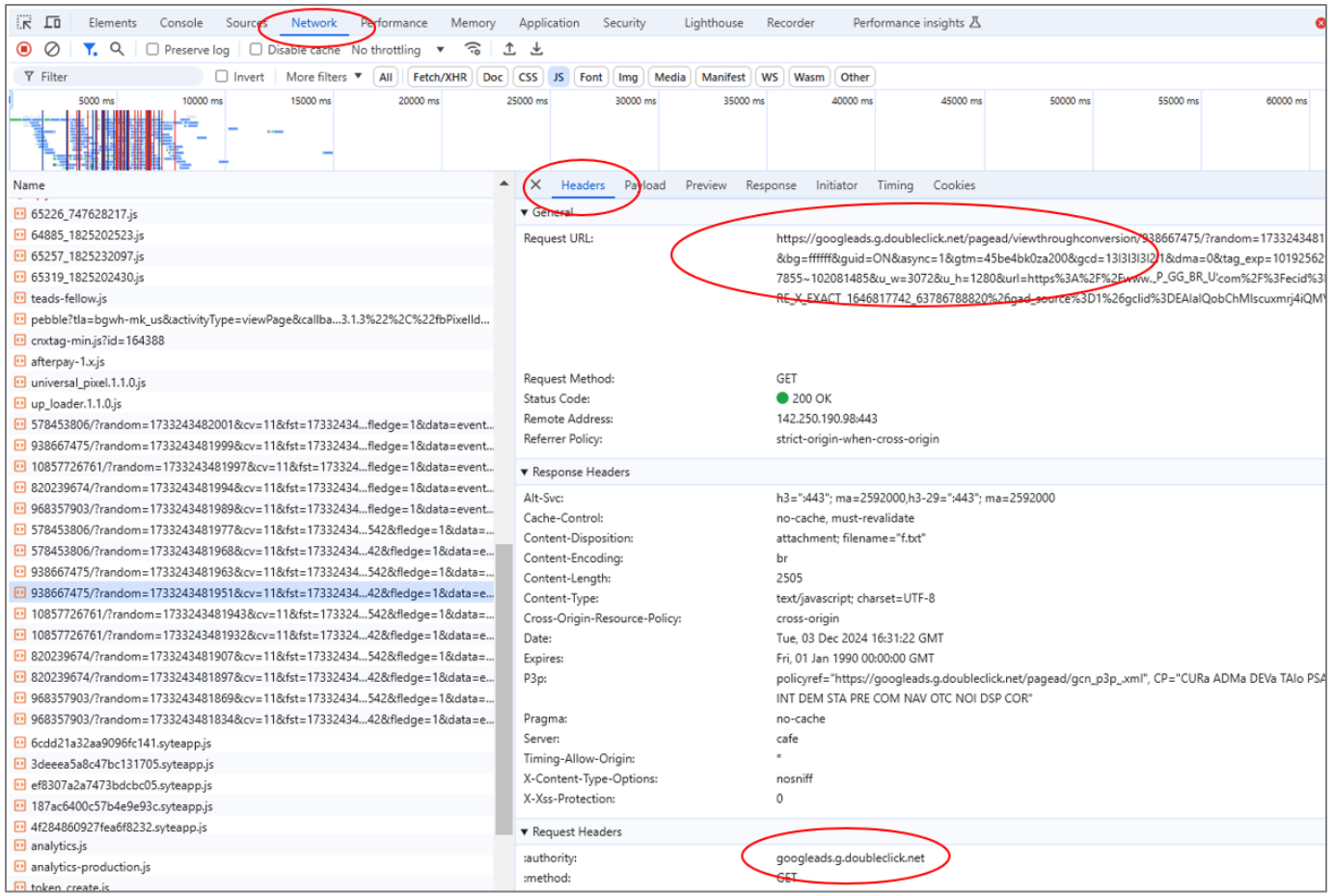
Purposes

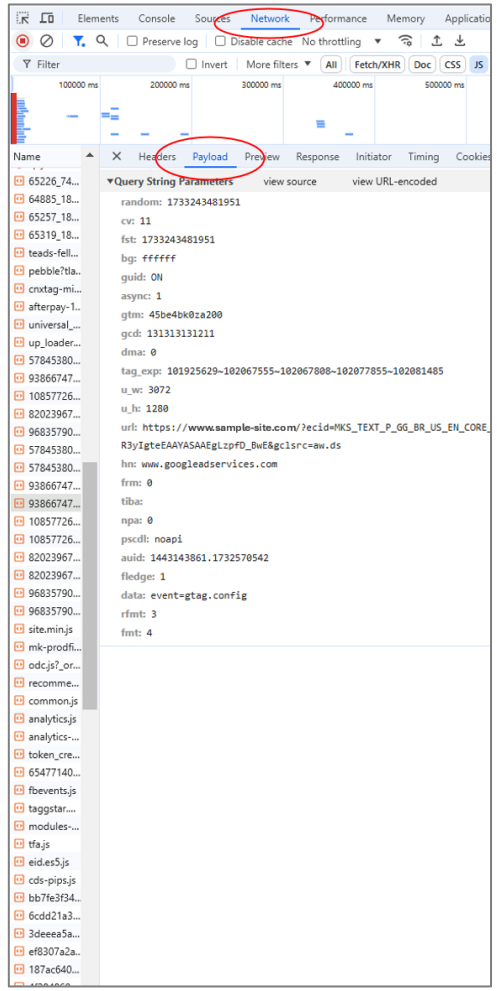
- Advertising
  - Interest-based advertising and retargeting
  - Audience-matched advertising (AKA “custom audiences” and “lookalike audiences”)
  - Location-based
  - Conversion tracking
- Analytics
- Functional
- Essential
- Performance
- Other Variations

Data Elements

- Unique identifiers (e.g., Device ID, MAID, domain-specific IDs, etc.)
- IP address
- URL visited
- Event ID
- Campaign info
- Keystrokes and behavior
- Content entered (e.g., webform)
- Search terms

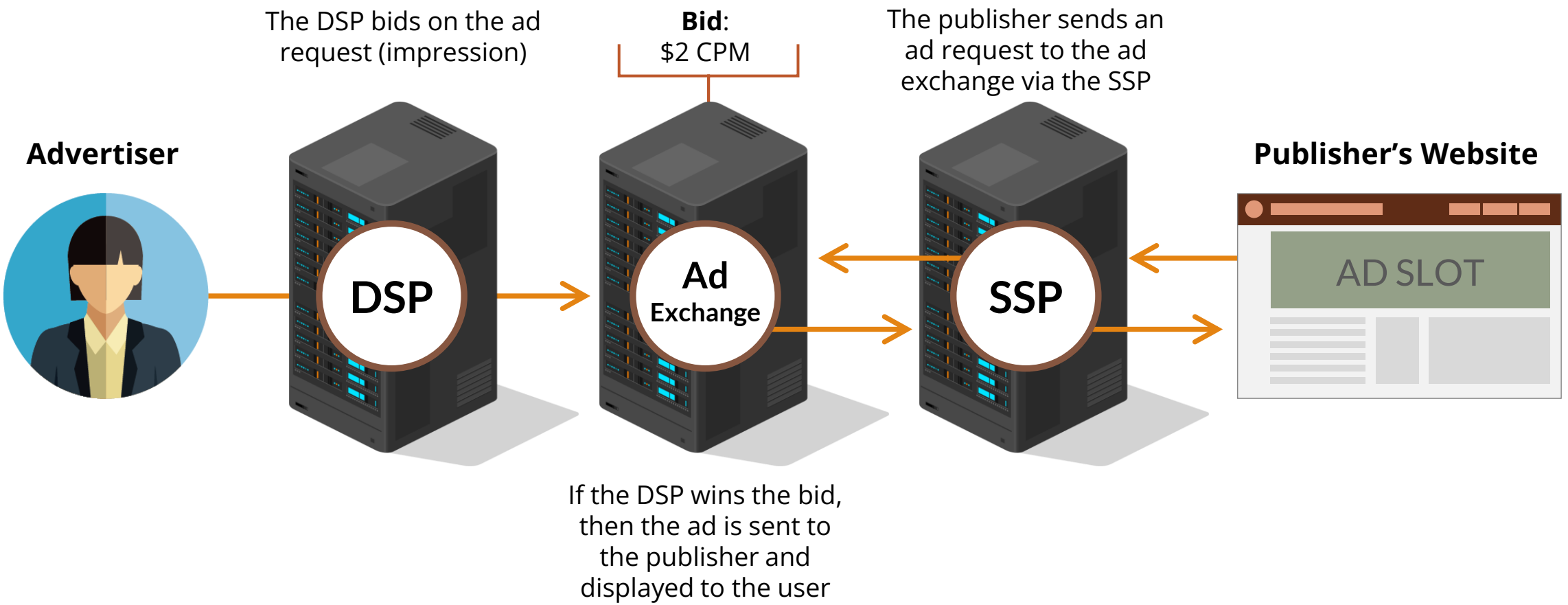
Under the Hood

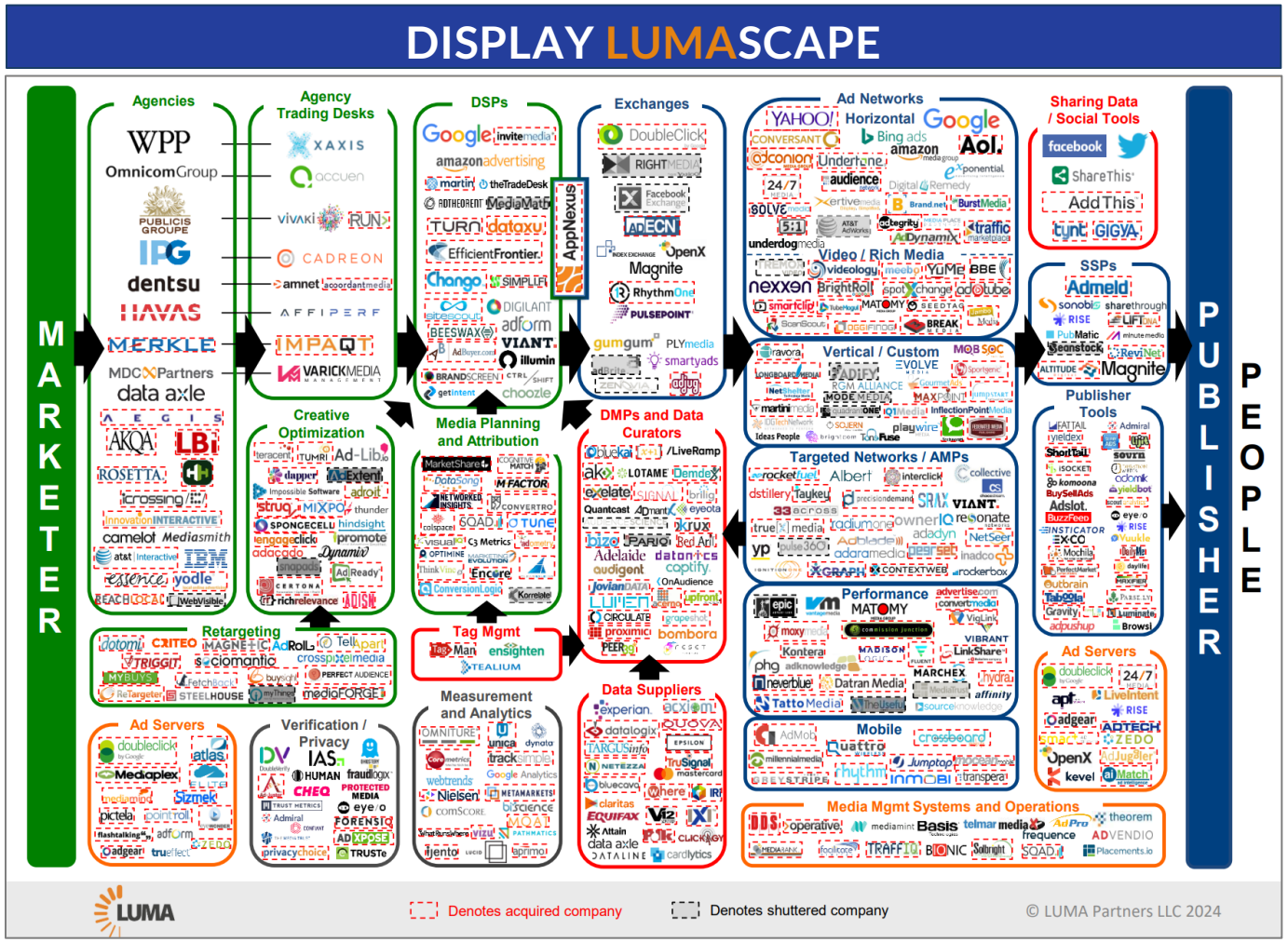




#PSR25

Key Players in the Digital Ad Ecosystem





What It Really Looks Like, Though

LUMA Partners LLC, LUMAscapes: A Visual Guide to the Digital World, https://lumapartners.com/lumascapes/ (accessed Dec. 3, 2024).

Legal/Enforcement Update

US Regulation Is Increasing

U.S. State Laws and Regulation

- State Privacy Laws (new comprehensive + sector-specific (health, financial, etc.))
- Federal Laws (FTC Act, HIPAA, GLBA, DOJ Final Rule on Sensitive Data Transfers, etc.)
- Common law (breach of contract, negligence, etc.)
- Outdated laws applied to new technologies (CIPA/Wiretap laws, Video Privacy Protection Act)

Guidance

- Federal Trade Commission Pixel Guidance (link)
- NY AG Online Tracking Guidance (link)

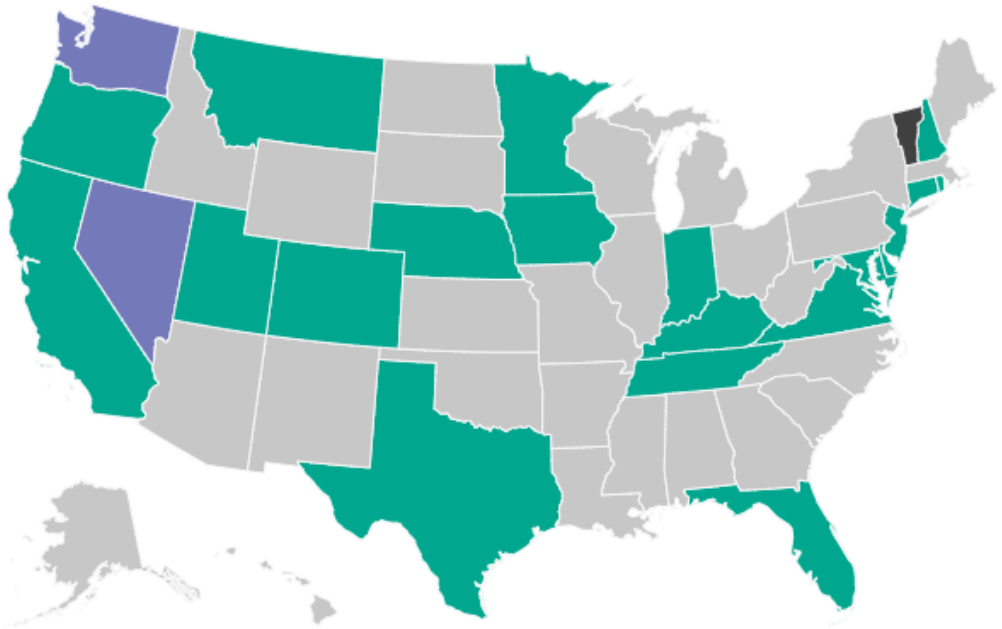
Number of State Laws Is Increasing

20

States have enacted consumer privacy laws

Currently in effect:

- California
- Virginia
- Colorado
- Connecticut
- Utah
- Texas
- Florida
- Oregon
- Minnesota
- Montana
- Iowa
- Delaware
- Nebraska
- New Hampshire
- New Jersey
- Tennessee
- Maryland



Enacted but not yet in effect (by 2026):

- Indiana
- Kentucky
- Rhode Island

https://www.mwe.com/resource/global-privacy-cybersecurity-resource-center/#map

Key Cookie-Related Rights (US)

Opt Out of Selling/ Sharing/Targeted Advertising (Virtually All States)	– CA AG Guidance: Selling occurs when third party collects data directly from website (i.e., not necessary to affirmatively disclose to the third party). – Cases suggest most cookies are likely sales without a DPA (and all marketing cookies are likely sales/sharing regardless of DPA under CA-specific rules).
Opt-In to SPI Processing (Most States)	– Most states require GDPR-style affirmative consent. – WA/NV: Must obtain "written and signed consent" to "sell" health data.
"Affirmative Express Consent" for SPI (FTC)	– Must obtain "opt-in" consent for certain location, health, browsing, and other SPI. – FTC requires companies to disclose: (1) categories of information collected; (2) purpose for collection, use, or sale; (3) identities of entities collecting or receiving information; and (4) a hyperlink for consumers to easily withdraw consent.
Other Rights	– Access, Delete, Correct, etc.

Global Privacy Control Is Increasingly Required

Global Privacy Control (GPC):
Browser add-on that transmits a signal to websites in order to trigger opt-out rights under data protection laws

Expressly required under state laws (e.g., CA and CO)

- Effectively required under most other state consumer privacy laws

GPC is completely **distinct** from many existing rules and upcoming changes:

- EU-style cookie banner is insufficient
- Do Not Track (CalOPPA) is different
- Apple ATT requirements are different

US Enforcement Is Increasing

Agency	Fact	Cause of Action	Status
FTC	Antivirus/software provider sold identifiable **browsing data** without notice/consent.	UDAP	Settled for $16.5 million + 20-year CAP
FTC	Data broker sued for selling sensitive data (including **geolocation**).	UDAP	Pending
CA AG	Food delivery company sold data to **marketing cooperatives** without notice under CCPA (notice and DNS) and CalOPPA (notice).	CCPA & CalOPPA	Settled for $375k + CAP
CA AG	Cosmetic retailer failed to (i) **inform** consumers it sold data collected via its website and (ii) **honor opt-out requests.**	CCPA	Settled for $1.2 million + regular compliance reports to the CA AG
FTC	Data broker sold raw location data with sensitive locations and failed to implement reasonable safeguards against downstream use of **precise location data**.	UDAP	Banned from sharing or selling sensitive location data
FTC	Data aggregator failed to fully inform consumers and obtain consent before collecting and using **precise location data** for advertising and marketing.	UDAP	Banned from selling or licensing precise geolocation data
FTC	Online counseling service revealed data to **social media companies** for advertising purposes.	UDAP	Settled for $7.8 million.

Enforcement Issues

Who is Targeted?

- FTC targets the company **"selling" data** (typically acting as "data broker")
- **State AGs** target the **advertiser**

Remedy

- Settlement (FTC: ***20-year*** settlement decrees)
  - Must get affirmative express consent
  - Ban on selling/disclosing
  - Deletion of data AND algorithms/models/software
  - Comprehensive privacy program
  - Reporting to regulators
  - Mandatory third-party assessments every other year
  - Senior officer certification annually
- Monetary settlement
- Disgorgement

Recent Paradigm-Shifting Examples

Agency	Target Company	Key Allegations	Penalties
CA AG	Healthline	• Failed to honor consent choices (by misconfiguring cookie consent tool). • Shared health-related article titles with third parties, which CA AG alleged violated the CCPA's "purpose limitation" because it was an unexpected use of "sensitive personal information" (SPI). • Note: Calls into question the ability to use trackers for health marketing at all. • Failed to offer consumers a right to limit SPI processing. • Failed to include required terms in contracts with advertising companies.	• $1.55 million settlement. • Data disgorgement. • Prohibition of certain data "sales" altogether.
CPPA	Honda	• Required more steps to opt out of sale/sharing than to opt back in. • Requested excessive information to process data subject rights requests. • Required verification for authorized agent requests to opt out of sale/sharing. • Failed to execute required contracts with advertising technology partners.	• $632,500 fine.
CPPA	Todd Snyder	• Failed to properly configure privacy portal and cookie banner and continued to sell personal information via tracking technologies after consumers requested to opt out. • Required consumers to submit more information than necessary to process privacy requests. • Required consumers to verify their identity before they could opt out of the sale or sharing of their personal information.	• $345,178 fine.
CPPA	Tractor Supply	• Failed to: (i) inform consumers about how to opt out of sale/sharing through tracking technologies; (ii) honor browser-based opt-out through webform; and (iii) honor GPC • Failed to execute required contracts with advertising technology partners. • Failed to inform consumers and job applicants of their CCPA rights and how to exercise them; failed to update consumer privacy notice annually.	• $1.35 million fine. • Onerous remedial measures (e.g., quarterly website scans, inventory, updating and distributing notices, etc.). • Annual compliance certification.

Lessons From Enforcement (Public/Non-Public)

Non-Verifiable vs. Verifiable Requests	– Verification – Authorized Agents
Opt-Out Requests	– "Too many steps" ▪ But: Cookie-Based vs. Non-Cookie-Based – Immediate Effect
DSR Responses	– Timeliness – Statistics (Grant vs. Deny) – Particularized Reasons for Denial

US Litigation Is Skyrocketing

- Wiretap laws permit **statutory damages** of up to **$10k per violation (under ECPA; most states are $1k-$5k).**
- **20+ plaintiffs' firms** sending **tons** of demand letters/filing litigation alleging violations of wiretap laws, UDAP, etc.
- Big settlement range (4-5 figures for some firms; others demand high 6-7 figures).
  Most public settlements range from **$2 million – $18 million.**
- **Jury verdicts** are coming out against defendants (including recent case against large social media company).

- **Common states**: CA, PA, FL, MA, etc.
- **Common Targets**: Specific cookies, session replay tools, chatbots, search functionality, etc.
- **Methods**: Litigation, arbitration (depending on website TOS).

To minimize risks, need **adequate notice** and **consent**.

Changing the Game:
Salazar v. National Basketball Association

Video Privacy Protection Act

- "Consumer" means renter, purchaser, or subscriber of goods or services.
- "Goods or services" was historically limited to audiovisual materials.

Salazar v. National Basketball Association

- "Consumer" expanded to mean "a renter, purchaser or subscriber of ***any*** of the provider's goods or services – audiovisual or not."

Salazar v. National Basketball Association, No. 23-1147 (2d Cir. 2024).

Industry Changes

Apple/Google Changes	– Apple ATT (opt-in for “tracking”) – Google Privacy Sandbox (maybe?)
Cookie Alternatives	– Hashed IDs – Data “Clean Rooms” – IAB Server-Side – Fingerprinting – Customer Data Platforms

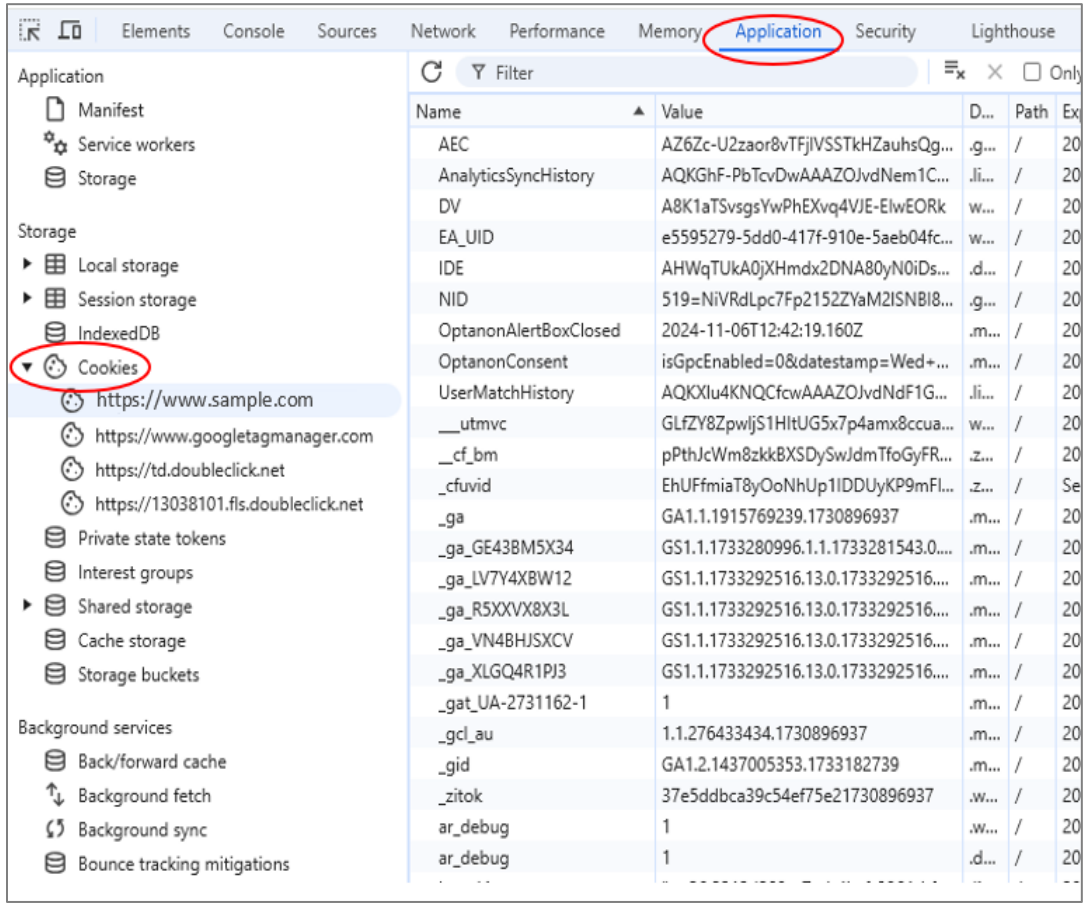
How to Operationalize, Test, and Maximize Data/Minimize Risk

Common Pitfalls

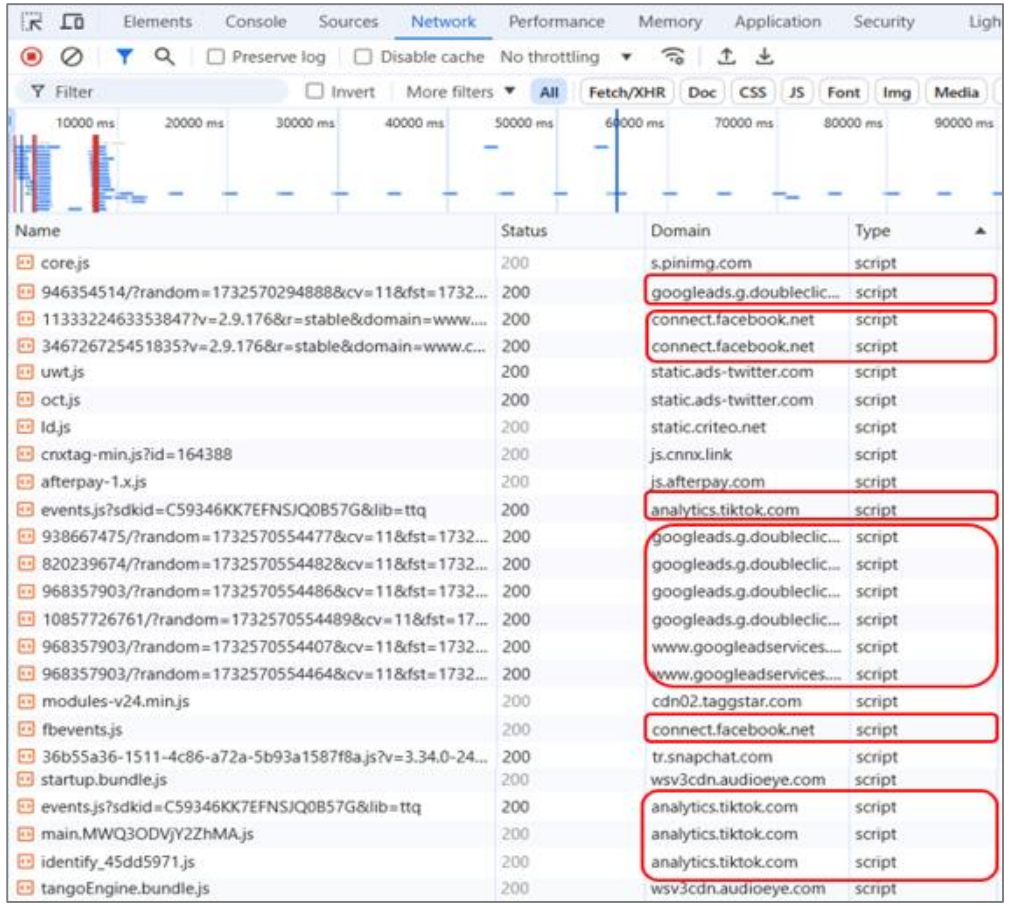
- Banner / Preference Center Language & Functionality
- Categorization
- Choice & Dark Patterns
- Non-Cookie
- Configuration Issues
- Alignment to Privacy/Cookie Notices

How to Test: Chrome Developer Tools

Application Tab



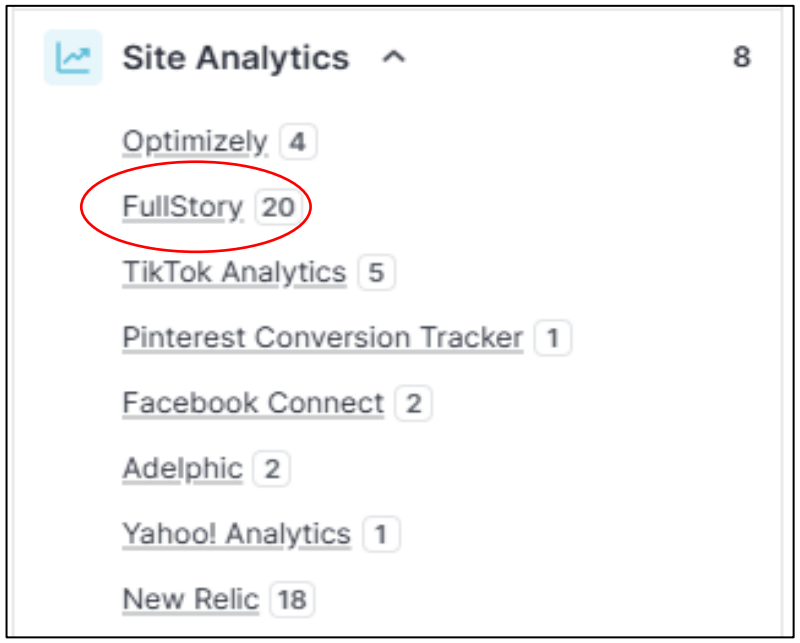
Network Tab



Other Issues: Search, Session Replay, etc.

Claim that website search functionality shares search terms with third parties (often server-to-server, so harder to check)

Claim that session replay shares detailed behavior, keystrokes, etc.



How to Operationalize

Cookie Management:

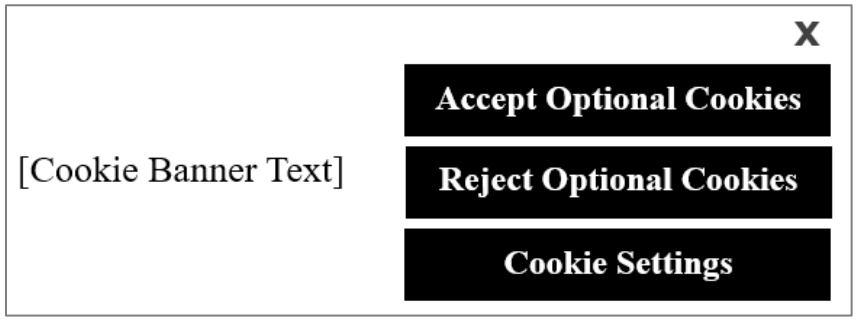
- Identify and categorize cookies
- Confirm legal obligations/ compliance approach
- Select third-party vendor
- Set up a repeatable process to manage any changes to cookies used

How to Operationalize (Cont'd)

Cookie Banner:

- Should you have a cookie banner?
- What is the functionality of the banner?
- How do you describe banner options?
- What buttons should you use?
- Will you implement different banners in different locations?
- Will you honor GPC? If so, where?
- Will you force banner interaction (or allow "X")?
  - Does "X" accept or reject cookies?
- What Cookies go in each category?

Common Approaches	Risk Level
Opt-In (Everywhere)	Low (Most Conservative)
Opt-In (CA only)	Low-Moderate
Opt-Out	Moderate
Notice Only	Moderate-High
No Banner	High

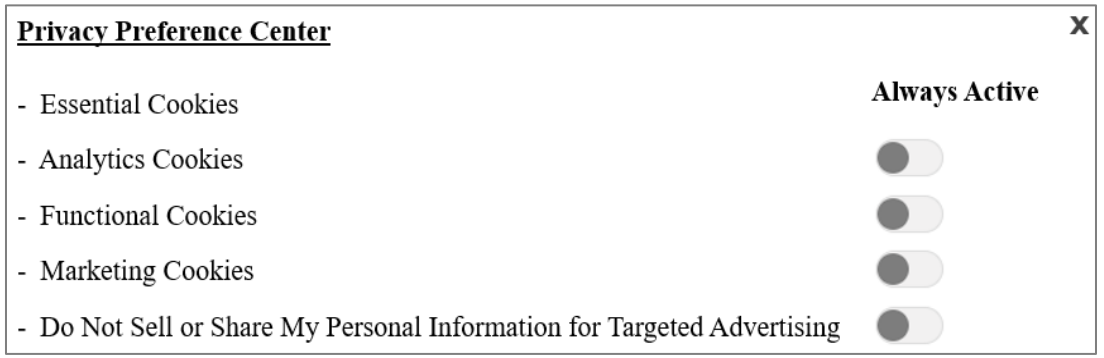


How to Operationalize (Cont'd)

Preference Center:

- Should you have a preference center?
- What should the text say?
- What buttons should you use?
- How is the preference center accessible?
- Will you implement different preference centers in different locations?
- Will you honor GPC? If so, where?
- Will you force interaction (or allow "X")?
  - Does "X" accept or reject cookies?
- What cookies go in each category?

Approach	Description
Granular Choice	Separate toggles for each cookie category
All-or-Nothing Choice	"Do Not Sell or Share My Personal Information for Targeted Advertising" toggle



How to Operationalize (Cont'd)

Data subject requests:

- Which requests will you honor?
- How are requests received?
- How do you process requests internally?
- Do you have template communications?
- What are your recordkeeping processes?
- Can you connect cookie with non-cookie data (e.g., to honor opt-out rights fully)?

Takeaways

- It’s more complicated than you think
- Risk Mitigation requires a combination of legal and technical expertise
- Third Party tools are required to manage cookies effectively (home-grown solutions are cost-prohibitive)
- Must be living program – cannot just set and forget

Action Items

Discovery and Testing	• Conduct audit (testing current state/gaps + regularly test moving forward) • Create inventory + categorize (which cookies, purposes, data elements, type, retention, etc.) • Cross-site, cross-platform, cookie and non-cookie
Banner and Preference Center	• Decide type of banner/preference center (opt-in vs. opt-out vs. notice vs. none) • Language, Buttons, User Experience • Configure: Consent tool, 3P cookie account settings, web/mobile integration, geofencing, GPC
Policies, Procedures, and Governance	• Prepare technical-facing cookie SOP • Prepare business-facing cookie SOP • Update privacy notice + cookie policy • Prepare procedures for documenting/tracking/storing consent • PIA process (*e.g.*, Cookies) • Other (additional guidance for sensitive info (health/location/etc.); data dictionary; deidentification)
Vendor Issues	• Execute DPAs with cookie vendors (mostly C2P, but C2C for marketing and in some jurisdictions) • Restrict third-party processing where possible (*e.g.*, Google RDP and Meta LDU) • Prepare for compliance with DOJ rule on Bulk Sensitive Data Transfers for certain vendor agreements

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Privacy. Security. Risk. 2025**
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!