Digital Advertising 101: Navigating the Ever-Evolving Online Advertising Landscape

PRESENTED BY:

Meredith Halama | Partner | Perkins Coie

Katie Cramer | Associate | Perkins Coie

Zoe Sharp | General Counsel | Optoro

Who We Are

MEREDITH HALAMA

Perkins Coie, Partner & Co-Chair, Privacy & Security

Washington, DC

KATHRINE CRAMER

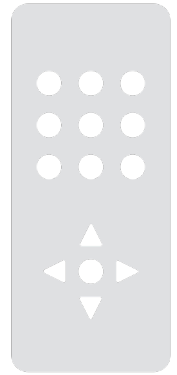
Perkins Coie, Associate, Privacy

Denver, CO

ZOE SHARP

Optoro, General Counsel

Washington, DC



What We'll Cover

- Overview of the Digital Advertising Ecosystem
- How State Consumer Privacy Laws Impact Ad Tech
- Q&A

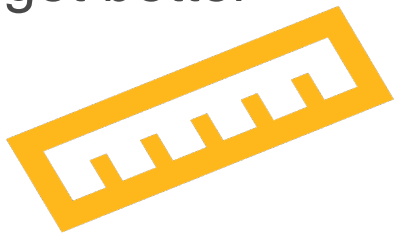
OVERVIEW OF THE DIGITAL ADVERTISING ECOSYSTEM

What is Ad Tech For?

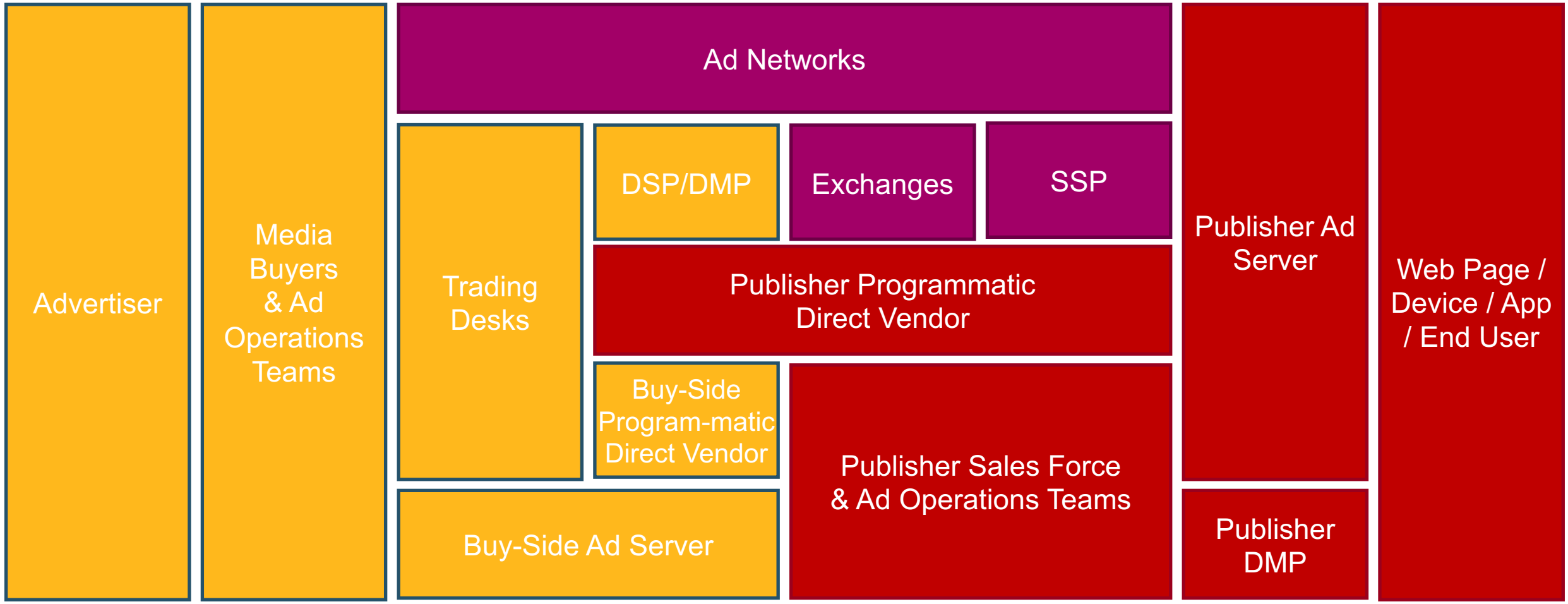
Q: WHAT ARE THE TWO MAIN GOALS OF AD TECH?

Target ads to the right people, in the right places, at the right time

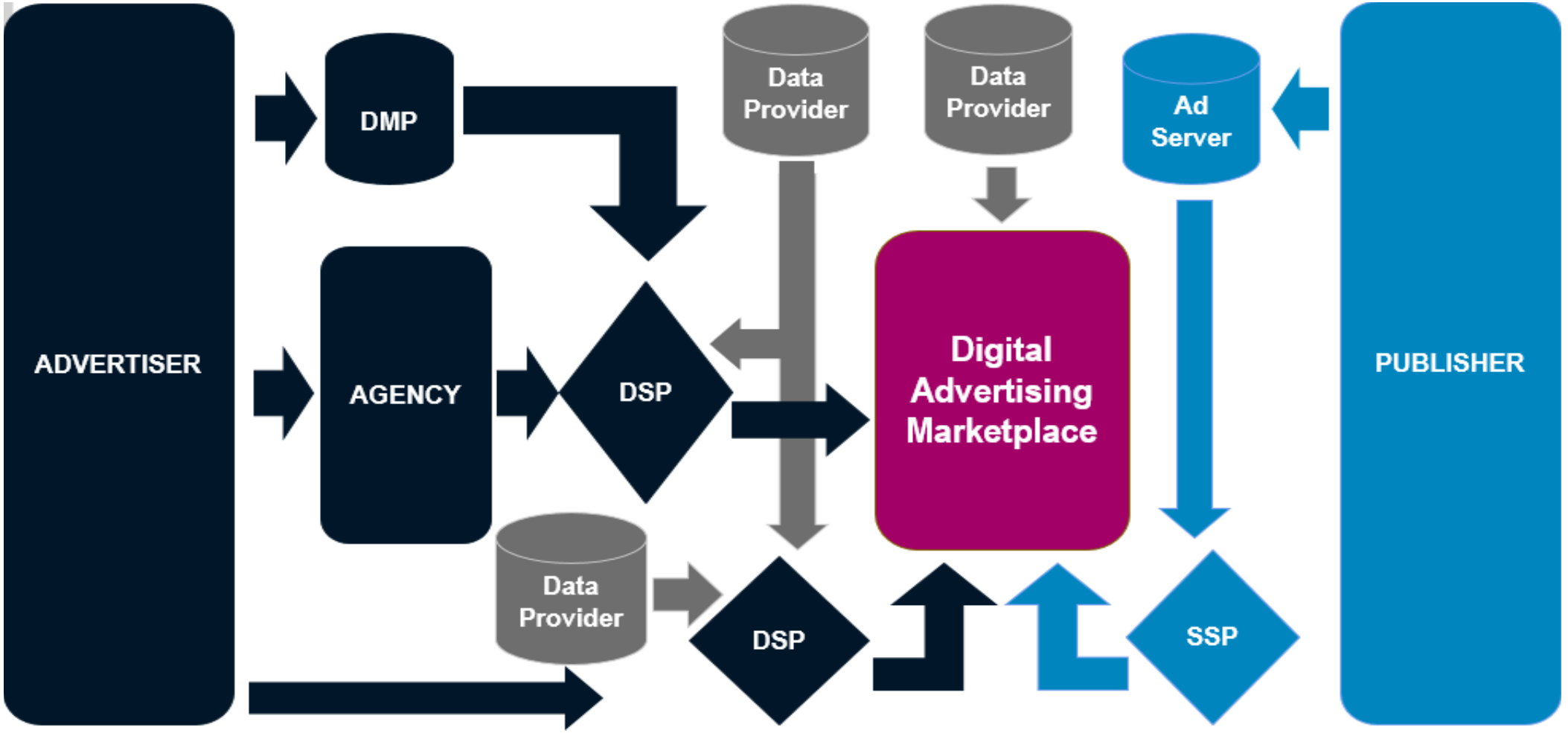
Measure performance so you can target better



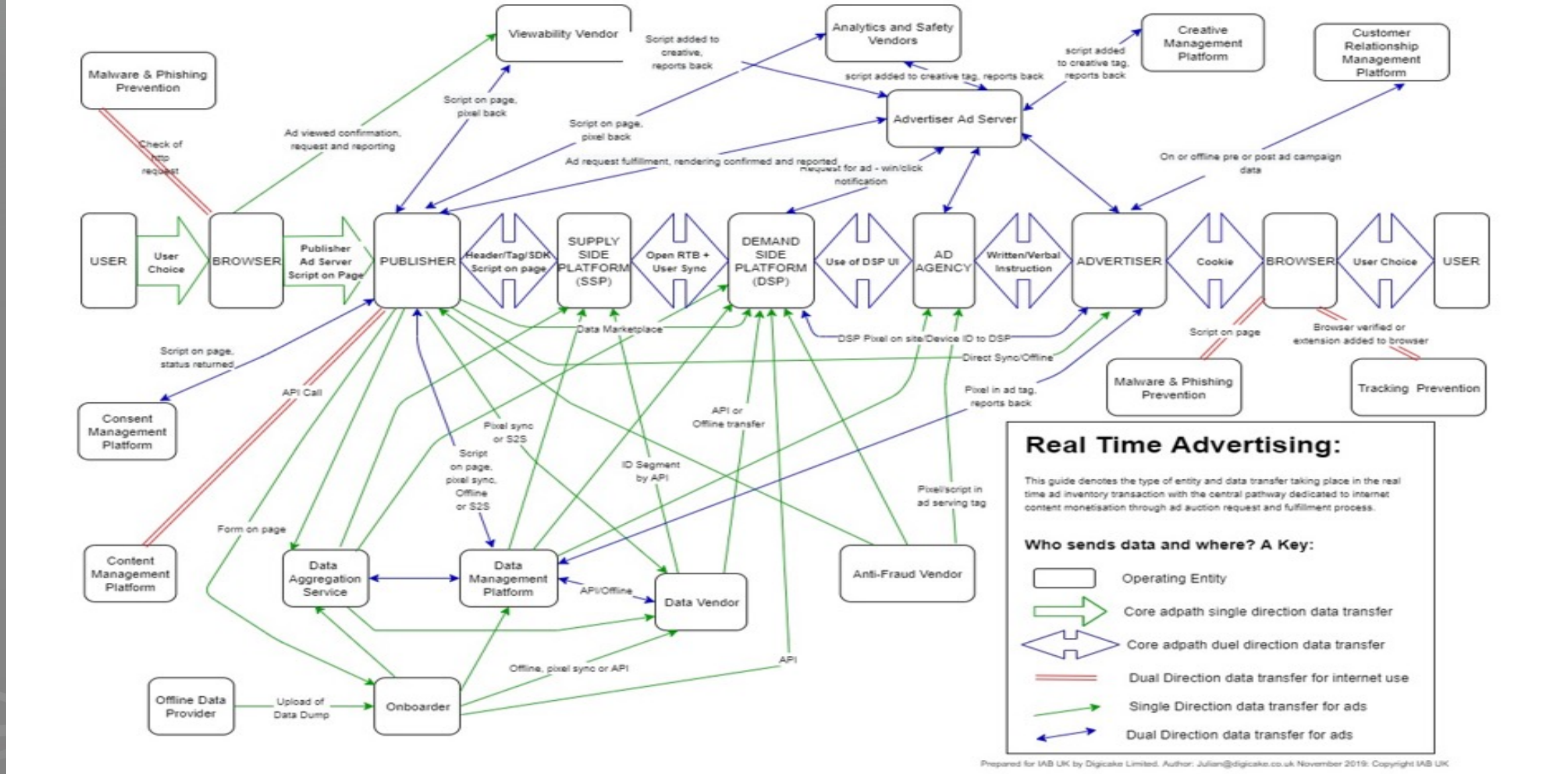
Overview of the Digital Advertising Players



Digital Ad Ecosystem



Q: WHAT DO THE DATA FLOWS LOOK LIKE IN THIS ECOSYSTEM?



Q: WHAT ARE SOME COMMON AD TECH PRACTICES?

Ad Targeting

- **Interest-Based Advertising/Online Behavioral Advertising/Targeted Advertising:** tracking a user across non-affiliate sites for the purposes of serving ads targeted to that browser's interests
- **Cross-App Advertising:** the mobile app equivalent of IBA, tracking a user across non-affiliate apps.
- **Retargeting:** using data collected on one site or app to show an ad to a user on another site or app

Data Onboarding/Data Append

- Adding information to a user's profile
- Typically, via hashed PII match (but can be via device ID)

Ad Delivery and Reporting

- Essentially, everything else: analytics, understanding ad effectiveness, counting uniques, etc.

Q: ARE ALL TYPES OF ONLINE ADVERTISING CONSIDERED TARGETED ADVERTISING?

Targeted Advertising Does NOT Include...

- **Contextual advertising** (based on what the consumer is viewing at that moment)
- "**First party**" advertising – a company using its own information to show an ad to a user
  - Even if such ads are "behavioral" or "targeted" in some respect

Q: WHAT KIND OF TECHNOLOGY POWERS TARGETED ADS?

Common Terms

Cookies: Bit of code that sets on a browser, often identifying the browser/device. Can be session or persistent, first or third party

Pixels (tags): Bit of code that fires to other parties, tells the cookies to drop (if cookies are enabled). Often called ad tags or conversion pixels

SDK: Works like cookies/pixels, but in mobile apps. Bit of software that pulls an Ad ID or other identifier

Advertising ID: A resettable ID provided by Apple and Google to allow companies to identify users on mobile apps

AND MORE…

Common Terms

IP Address: A network identifier, sometimes specific to device and other times not

Hashed Email Address: Can be used in different ways, including: Platform audience tools (e.g. Facebook “Custom Audiences”); Means to onboard offline data (e.g. LiveRamp); Conversion to online identifier (e.g. UID)

Device Fingerprints: IP Address + “special sauce” to attempt to divine uniqueness

Cross Device Mapping: Algorithmically or deterministically associating one device to another device

HOW STATE CONSUMER PRIVACY LAWS IMPACT AD TECH

Q: What Privacy Laws Are We Talking About?

5 state omnibus privacy laws go into effect by the end of 2023 (with many more to come beginning in the second half of 2024)

These laws…

- Codify principles previously addressed by industry self-regulatory organizations.

- Make certain long-held best practices mandatory (e.g., notice and opt-outs for targeted ads).

- Emulate the Europe's privacy laws in some respects.

California, Colorado, Connecticut, Utah, Virginia → 2023

FL, OR, TX, MT → 2024

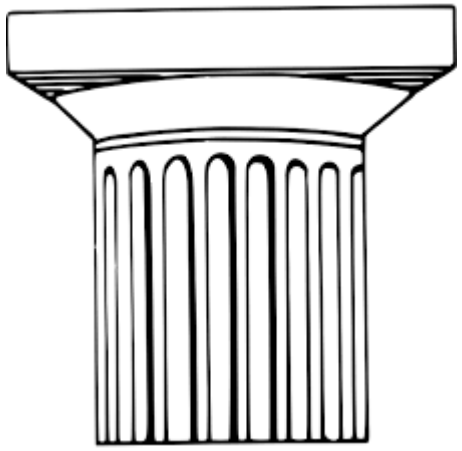
IA, TN, IN,→ 2025-2026

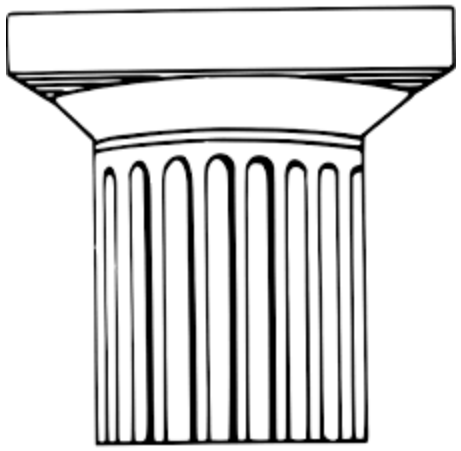
Q: How Do These Laws Impact Ad Tech?

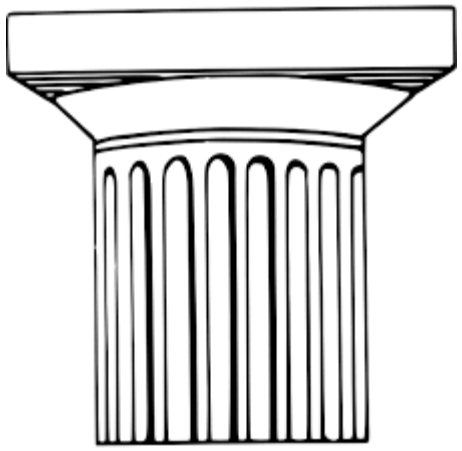
SEVEN KEY CONCEPTS IMPACTING AD TECH:

- Address intent behind each component and what compliance involves.

- Organized through the lens of two broad policy goals: **consumer control** and **harm reduction**







Q: What Do These Broad Policy Goals Aim To Solve For?

CONSUMER CONTROL

Addresses perceived asymmetry of information and power among consumer and companies through:

- **Transparency** (e.g., notices and other disclosures, data access rights); and
- **Choice** (e.g., opt-out rights, consent for sensitive data processing, etc.)

HARM REDUCTION

Focus on reducing risk of harm to consumers from use of their PI, such as by:

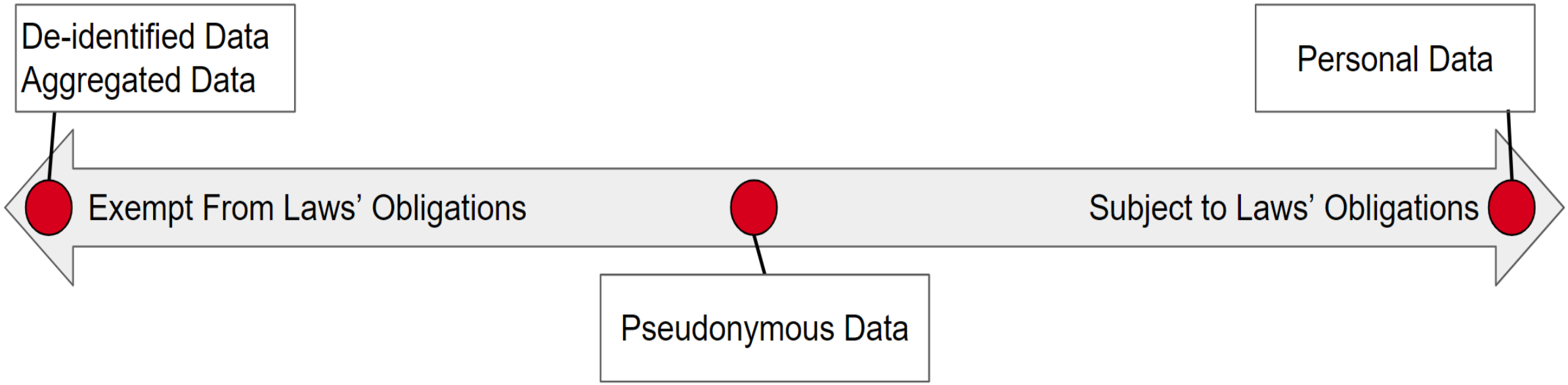
- Codified purpose limitation and data minimization principles;
- Heightened controls and protections for certain categories of data; and
- Contractual requirements governing data sharing relationships.

Q: What Are The Core Requirements

1. Allow Consumers to Opt Out of Targeted Advertising and “Sales”
2. Limit Data Sharing, Including Requirements for Contracts with Service Providers and Third Parties
3. Special protections for “sensitive data” (e.g. precise location information, health data, and race/ethnicity)
4. Grant Consumers the Right to Access, Delete, and Correct Their Data
5. Mandate Responsible Data Practices, Including Purpose Limitation and Data Minimization
6. Expand Privacy Policy and Other Notice Obligations
7. Effective Bar to Targeting Kids



Q: BEFORE DIVING INTO EACH PILLAR, CAN WE TALK A BIT HOW THEY APPLY TO DIFFERENT DATA TYPES?



Q: WHY DO THE STATE LAWS REQUIRE OFFERING OPT-OUTS FOR ADVERTISING SPECIFICALLY?

1. Allow Consumers to Opt Out of Targeted Advertising and "Sales" of Their Personal Data

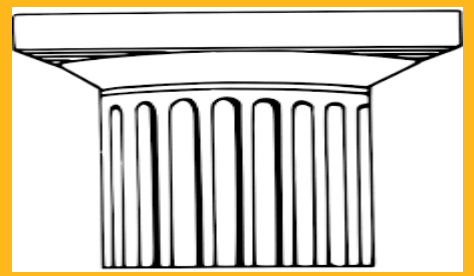
What: must allow consumers to opt out of the "sale" of their personal data and the disclosure or processing of their personal data for purposes of targeted advertising

Why: regulators perceive cross-site advertising as more harmful to consumers than first-party and contextual advertising

Intent: allow consumers to easily opt out of cross-site advertising and certain disclosures of their data to unaffiliated companies (termed "sales")

→ Make opt outs easier to find and use than choices required by self-regulatory groups (e.g., The NAI and DAA)

→ Make these opt outs broader and more durable than cookies-based opt-outs alone (e.g., GPC), also cover email-based targeting



TARGETED ADVERTISING

(All non-CA states' privacy laws)

The **display of advertisements** to a consumer where the advertisement is **selected based on PI obtained from** his or her activities on **other companies' websites**, applications, or services.

*Whether processing for targeted advertising does **not** depend on receiving entity's status as a service provider or third party*

Processing for purposes of targeted advertising can occur irrespective of a transfer

SHARING (CA only)

Transferring, or otherwise communicating a consumer's PI by the business to a third party for **cross-context behavioral advertising [CCBA]**, whether for monetary or other valuable consideration

Sharing requires a transfer of data to a third party; service providers cannot facilitate CCBA

SALES (CA + Other States)

Any transfer of personal information to a third party for "**monetary [or other valuable consideration]**"

Transfers to service providers/processors are not sales.

What counts as "sales" and disclosures for targeted advertising?

What requires an opt-out?

Likely No Opt-out

- Contextual advertising
- Ads based on 1P data*
- Counting ad impressions
- Analytics
- Fraud detection and prevention
- Aggregate service improvement
- Disclose to other processors

Gray Area

- Lookalike modeling
- **Measurement**
- Clean room-type offerings
- DMPs and data onboarding -- e.g. LiveRamp-like solutions

Opt-out Needed

- Use for cross-site advertising at any future time
- Recipient has right to supplement a cross-device or add to a profile to benefit others
- **Retargeting**
- **Custom audience type products**
- Disclosures to non-processors

Factfinding to evaluate your companies sales/sharing/targeted advertising activities

Who should I ask about these activities? What should I ask them?

Who to talk to:

- Marketing team (internal or external agency/consultant)
- IT team
- E-commerce site team

What to ask:

- Do we have third-party pixels on our site?
- Do we have third-party SDKs in our mobile app?
- Do we use custom audiences (Meta product), Customer Match (Google product) or other email-based ad targeting products to reach customers and prospects on third-party sites?
- Do we sell any data?
- Are there other reasons / scenarios that personal data leave our walls except to vendors that use it just to perform services for us (e.g., cloud hosting, email marketing)?

Other tools:

- Ghostery (free browser extension to see pixels on your company's site)
- Review contracts with ads/marketing partners
- Review the policies and contracts you inherit
- Subscribe to your own marketing emails

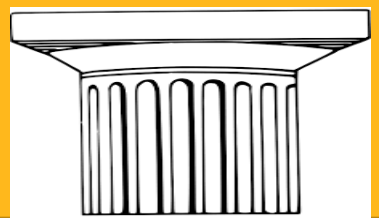
2. Limit Data Sharing, Including Requirements for Contracts with Service Providers and Third Parties

What: The State Laws Add Substantial Contractual Requirements on Ad Tech Relationships

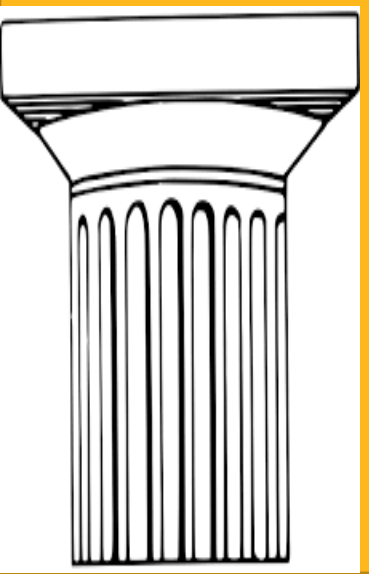
→ **3P Terms:** In California, a business may not process PI sold to it or shared with it by another business without a contract in place that governs the recipient's use of such PI, including by identifying the "limited and specified purpose(s)" for which the PI is made available to it.

→ **Processor Terms:** In all omnibus laws states, a contract is also is required where a company acts as a processor that limits how the processor may use, retain, and further disclose the PI.

- **For certain non-targeting services, ad tech players will act as a service provider / processor for opted out user data.**



3. Special protections for “sensitive data”



- Definition varies; generally, includes the following as relevant to ad tech:
  - Precise location information
  - Data “revealing” racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation.
  - In CA: “PI collected and analyzed concerning a consumer’s health”
- Under Colorado regulations, inferences about sensitive characteristics are considered to “reveal” such characteristics

CA - Right to opt out other than to the extent used for purpose for which collected/consistent with ordinary consumer’s expectations

CO, VA, CT, MT, IN - Require consent to process

- High bar for consent, especially in CO

UT & IA - Requires clear notice and ability to opt out

Q: WHAT DOES THIS HEIGHTENED FOCUS MEAN FOR AD TECH?

Implications for Ad Tech:

- Pressure to end targeting based on race/ethnicity. Due to discrimination lawsuits and state law requirements more companies are ending or limiting these practices.
- Prohibit any inferences that are SPI categories for individuals unless obtaining consent & offering opt-outs.
- Treat any inferences that are essentially used to reveal or infer sensitive characteristics as SPI
- Interest inferences likely okay so long as do not infer SPI.
- Health segments are higher risk in light of recent FTC enforcement (next presentation).

Q: CAN YOU TELL US MORE ABOUT THE RECENT FTC ENFORCEMENT?

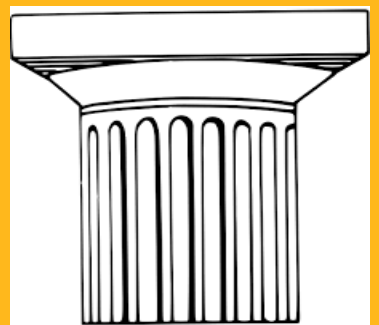
GoodRx

- FTC faulted the companies for sharing health-related data with Meta and other advertising platforms, including for targeted advertising purposes
- Determined companies' statements were deceptive by promising not to share health information with third parties.

betterhelp

- Focus on lack of proper privacy program and training.
- Part of GoodRX that offered Personal Health Records found to be in violation of Health Breach Notification Rule in addition to Section 5.

4. Grant Consumers the Right to Access, Delete, and Correct Their Data



What: The State Laws grant rights to consumers (e.g., access, portability, deletion, correction). Controllers must inform consumers of such rights and how to exercise them in their privacy notices.

Implications:

- ***Accepting & Honoring Requests.*** Must honor requests submitted by consumers (and authorized agents in some states). Processors must comply with passed on requests.
- ***Authentication.*** Must take steps to verify identity of the requestor.
- ***Appeals.*** Some states provide the right to appeal a decision to not act on the request.
- ***Exceptions.*** Consumer rights are not absolute.

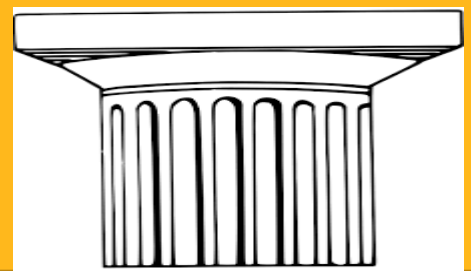
5. Mandate Responsible Data Practices, Including Purpose Limitation and Data Minimization

What: The State Laws codify data governance principles long endorsed by the FTC.

Data Minimization & Purpose Limitation: (i) limit collection of PI to what is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed;" and **(ii)** such purposes must be disclosed to the consumer.

→ To process PI in a manner not "reasonably necessary nor compatible with" the disclosed purposes, a company must obtain opt-in consent.

Data Retention: CA and CO also impose explicit data retention requirements.



Q: WHAT IMPACT DO THESE DATA GOVERNANCE REQUIREMENTS HAVE PRACTICALLY?

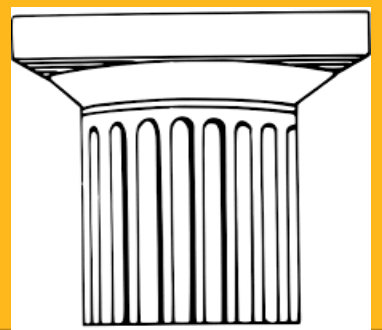
Implications for Ad Tech:

- **Evaluate requirements on data sources and recipient:** Understand role played, notices and choices provided, and obtain appropriate contracts.

- **Confirm notices align with practices:** Review existing privacy notices to ensure they comprehensively describe the purposes for which they will use PI.

- **Implement and honor retention policies:** Review existing data retention policies and ensure they are scoped to cover CA and CO requirements.

6. Expand Privacy Policy and Other Notice Obligations



What: The State Laws mandate presentation and content of privacy notices (also referred to as "privacy policies").

- Plus, CA also mandates **(i)** "notices at collection" to be provided at or before the point at which consumers provide their PI and **(ii)** notices for companies that "sell" or "share" PI or that use SPI for unexpected purposes.

Content: Privacy practices related to collection, use, and disclosure of their customers' PI; Information about sales/sharing of PI (including disclosures for purposes of targeted advertising); information about uses and disclosures about SPI, and information about consumer rights and how to exercise them.

Format: All 5 states impose accessibility obligations on businesses with respect to their privacy notices and other privacy disclosures (i.e., be "reasonably accessible). CA and CO impose more particular mandates.

Q: What kind of ad tech disclosures are necessary?

Updates include:

- Explaining targeted advertising and sensitive personal data in jargon of state laws;
- Explanation of how an opt-out preference signal will be processed and how consumers can use an opt-out preference signal;
- (CA & CO) Granular explanation of which categories of PI are used for which purposes, and which categories of PI are disclosed to which recipients, usually in a chart format; and
- If applicable, a statement that the company does not knowingly sell or share PI of consumers under age 16.

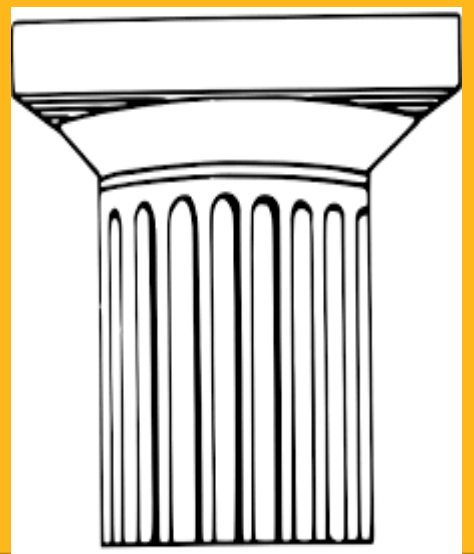
7. Effective Bar to Targeting Kids

What: Prohibition on processing of PI of known children under 13 without parental consent and "sale" or "sharing" of children under **16** in CA (and as old as **18** in some states).

How: Underscoring and in some places purporting to add obligations beyond those already imposed by federal law governing kids' data (the Children's Online Privacy Protection Act, or "COPPA").

→ **CA:** Imposes obligations on "selling" PI or "sharing" PI of children under 16, requiring opt-in consent from a parent for children under 13 years of age and opt-in consent from the minor for children ages 13 - 15.

→ **Most other states:** Classify data from children under 13 as SPI. Thus, any planned processing of data collected from children 13 is considered processing with a heightened risk of harm and requires a data protection impact assessment.



Compliance Steps Summary

BUILDING A PLAN TO COMPLY AD TECH REQUIREMENTS UNDER STATE PRIVACY LAWS

- Determine targeted advertising / sales activities.
- *Deploy an opt-out solution* (could be homegrown, or use a vendor like OneTrust). Test the solution to ensure intended functionality.
- Institute a process to ensure new targeted advertising / sales activities integrate with the opt out.
- Training your people (required by law and practical need)
- Make sure privacy policies adequately describe advertising activities.
- Update agreements with processors and third parties to meet state law requirements.
- Carefully evaluate all uses of sensitive personal data, especially health, and remediate as necessary.

QUESTIONS?

Q: WHAT DO THE DATA FLOWS LOOK LIKE IN THIS ECOSYSTEM?