The Ad Tech Ecosystem:
Demystify the Jungle and the Pitfalls

James Koenig
Partner
Troutman Pepper

Dan Frechtling
CEO
Boltive

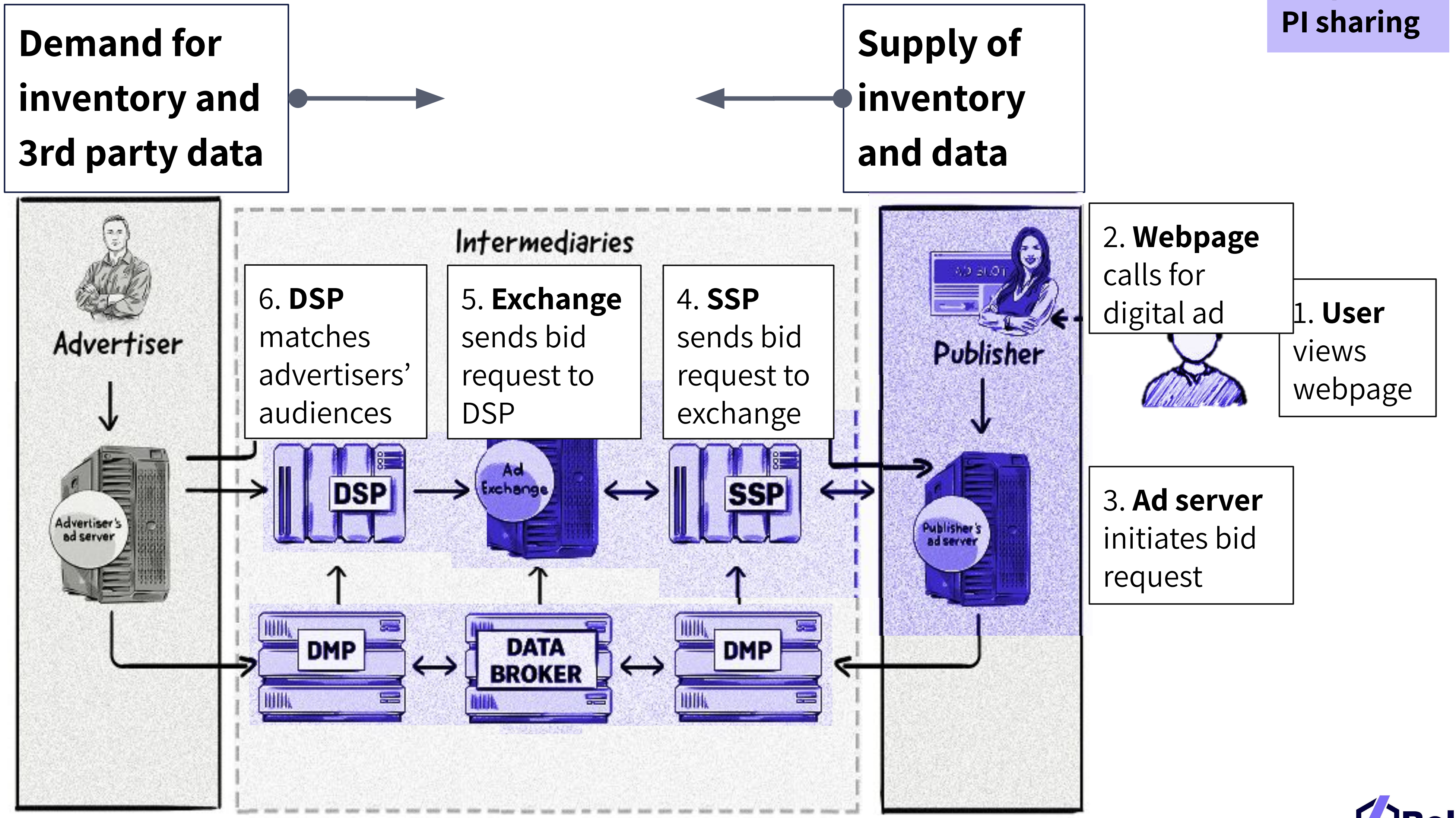
Joel Lutz
Counsel
Troutman Pepper

Demystify the Jungle and the Pitfalls

- Legal risks issues with pixels and cookies
- Risk mitigations
- Getting more familiar with pixels and cookies
- Pixels and cookies on web pages
- Pixels and cookies in ads
- How ad ecosystem sells/shares data (+ Facebook demo)

How Does The Ad Ecosystem Sell/Share Data?

Purple = PI sharing



Demand for inventory and 3rd party data

Supply of inventory and data

1. **User** views webpage

2. **Webpage** calls for digital ad

3. **Ad server** initiates bid request

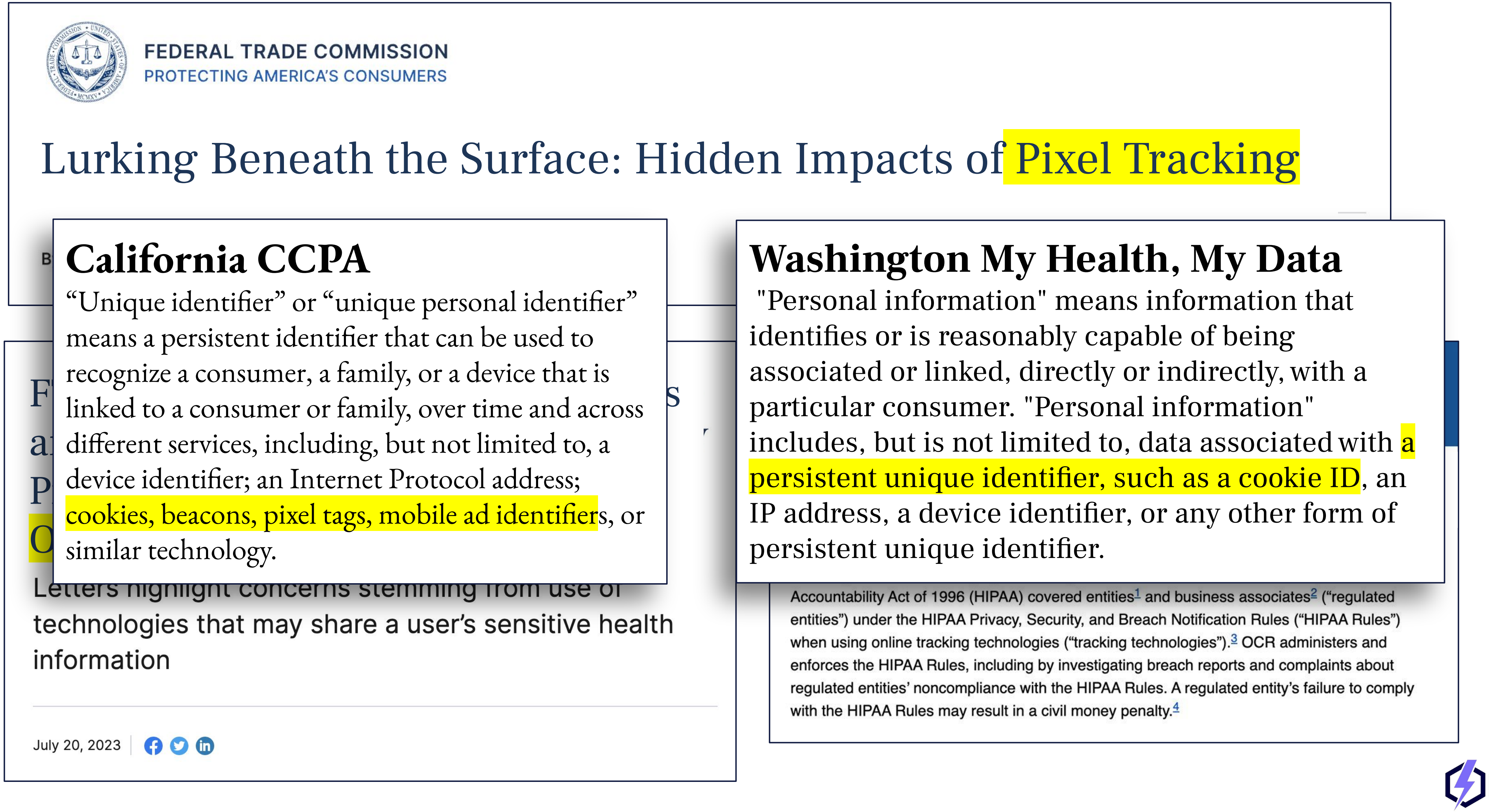
4. **SSP** sends bid request to exchange

5. **Exchange** sends bid request to DSP

6. **DSP** matches advertisers' audiences

Adapted from https://adtechbook.clearcode.cc/adtech-platforms-and-intermediaries/

Pixels, Cookies, And Trackers Appear In Regulations And Enforcement



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking

B

California CCPA

"Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology.

Washington My Health, My Data

"Personal information" means information that identifies or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer. "Personal information" includes, but is not limited to, data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier.

F

a

P

O

s

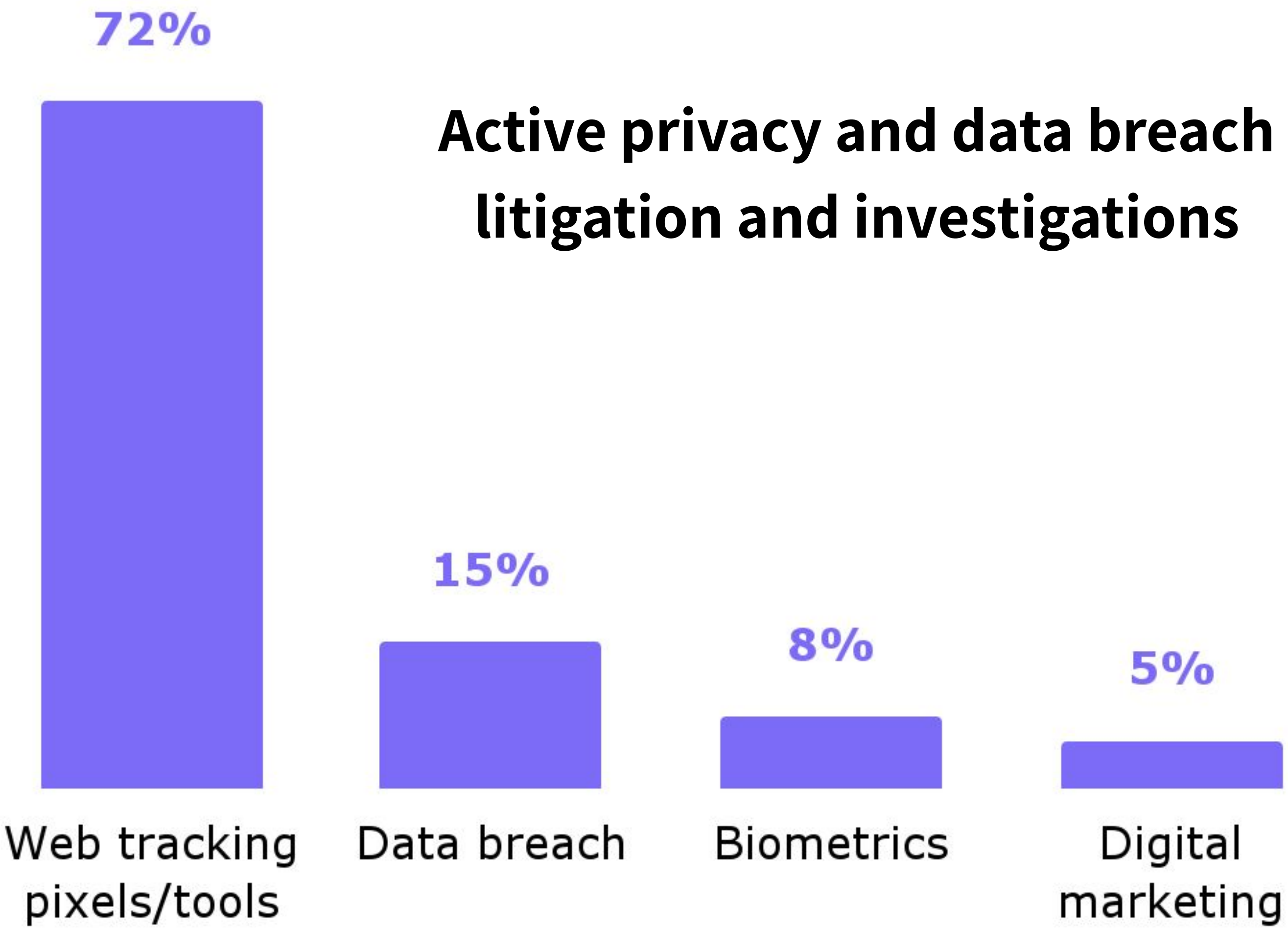
Letters highlight concerns stemming from use of technologies that may share a user's sensitive health information

July 20, 2023

Accountability Act of 1996 (HIPAA) covered entities[1] and business associates[2] ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[3] OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities' noncompliance with the HIPAA Rules. A regulated entity's failure to comply with the HIPAA Rules may result in a civil money penalty.[4]

Boltive

Website Tracking Lawsuits Exceed Other Privacy And Breach Cases



Active privacy and data breach litigation and investigations

Source: Classaction.org

Litigation and Regulatory Issues on the Rise!

Regulatory Issues

- International focus for years – GDPR, ePrivacy, LGPD (Brazil), etc.
- Comprehensive state privacy laws in US — CA, CT, UT, and VA in 2023, many more in 2024
- Industry or data-specific state laws–Health care information is hot topic
- New FTC focus on sensitive data sharing–Health-care information again

Regulatory Issues–Int’l

- ❖ Vary by jurisdiction, so do a case-by-case analysis and use geogating!

- ❖ Examples:
  - ➢ EU requires consent…except for strictly necessary cookies…
  - ➢ Canada doesn’t require express consent, except now in Quebec…
  - ➢ Brazil requires consent for some cookie types like ads and behavioral profiles but not others like analytics and measurement (in some cases!)

Regulatory Issues–US States

California (2019)—Opt out of "sale" or "sharing for cross-contextual advertising"

–Cross Contextual Advertising defined as targeting of ads to a consumer based on consumer's personal information obtained from the consumer's activities across businesses, distinctly-branded websites, apps, or services, other than the one with which the consumer is intentionally interacting.

Other states—(CO, CT UT, and VA in 2023 with others to follow in 2024 and beyond FL, OR, TX, MT, DE, IA,TN, and IN):

-Opt out of "Targeted Advertising" or automatic decision making/profiling in furtherance of decisions that produce legal or similarly significant effects.

–Targeted Advertising usually defined as: displaying ads to consumer where ad selection is based on personal data obtained or inferred from that consumer's activities over time and across non-affiliated websites or aps to predict such consumers preferences or interests. Usually exceptions for contextual ads or ads on company's own properties.

Global Privacy Control and "Sales" also at issue

–Most states also require opt-outs for "sale" of personal information, which can be narrowly defined as exchange for monetary consideration or broad to include any consideration or value. Will some sharing in the ad-ecosystem qualify as a "sale?"

–CA and other states, including CO, require that company's honor Global Privacy Controls Global Privacy Control — Take Control Of Your Privacy

Regulatory Issues –Industry/Data Specific

- Washington’s My Health My Data Act– “sale” of consumer personal health data requires an onerous authorization. Data includes past, present, or future physical or mental health of a consumer.

- HIPAA–OCR 2022 Bulletin focusing on online tracking technologies

- COPPA–can’t use personal information collected from child under 13 without parental consent (difficult to use pixels and trackers with parental consent)

Regulatory Issues–FTC and Regulatory Focus

- CCPA–Sephora Enforcement in CA
- FTC–GoodRx, BetterHelp, and Kochava actions
- EU–Criteo, Grindr, Apple, Microsoft, TikTok, Google, Meta

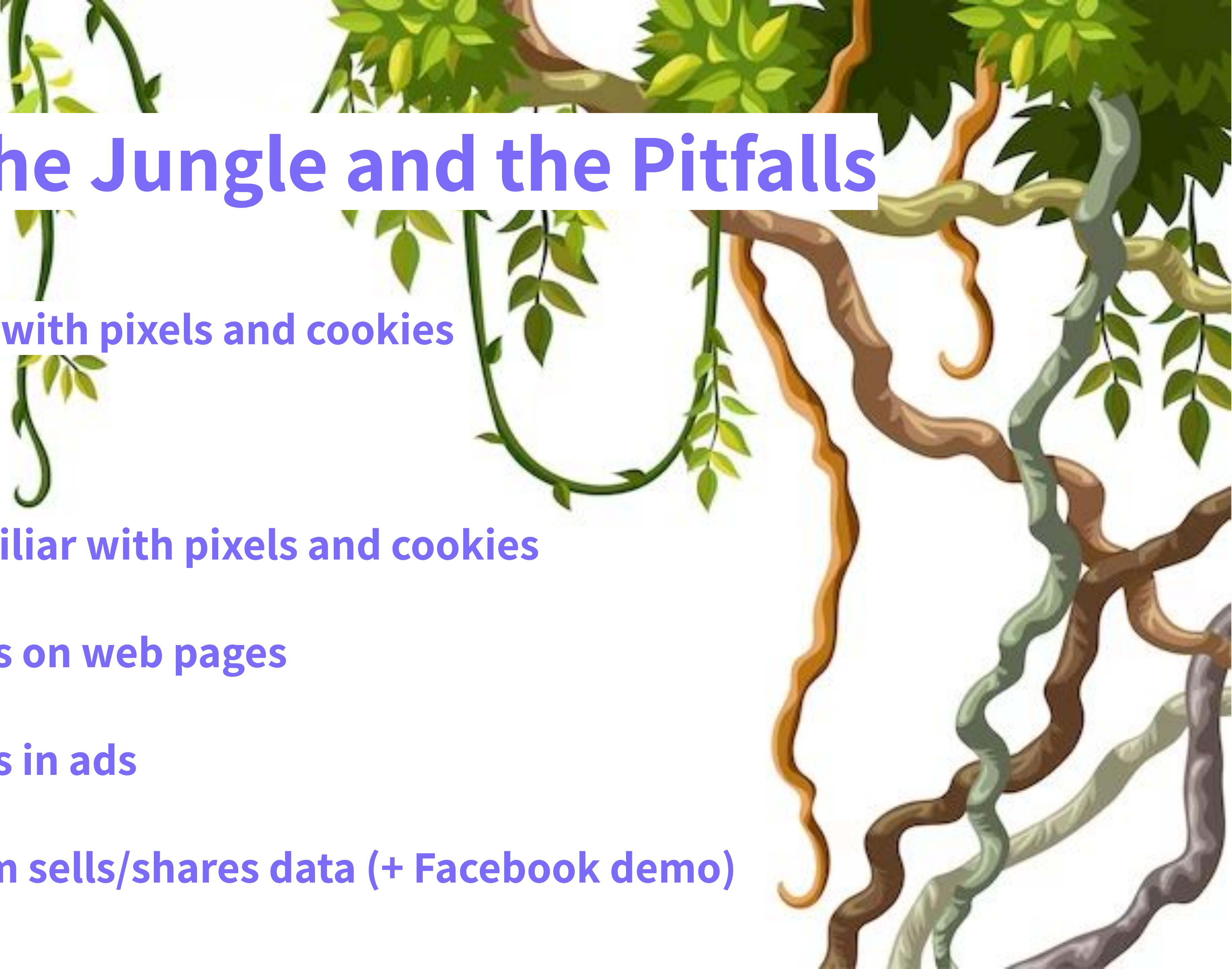
Litigation Issues

Recent cases involving pixels and cookies raise potential class actions related to:

- Confidential Medical Information Protection
- Wiretapping/Surveillance (e.g. California Information Privacy Act and PA wiretapping)
- Invasion of Privacy
- Confidential Medical Information Protections
- Video Privacy Protection Act (Unique rules on sharing video titles)

Demystify the Jungle and the Pitfalls

- Legal risks issues with pixels and cookies
- Risk mitigations
- Getting more familiar with pixels and cookies
- Pixels and cookies on web pages
- Pixels and cookies in ads
- How ad ecosystem sells/shares data (+ Facebook demo)



Tracking Technologies 7 Tips for Risk Reduction

Seven Tips to Address Potential Tracking Technology Issues

1. **Prevent:** Internal controls (e.g. SDLC for web/app) checkpoints limiting who can can change code

2. **Prevent:** Add a checkpoint in your vendor contracting and PIA processes

3. **Detect:** Prepare an inventory of cookies and trackers

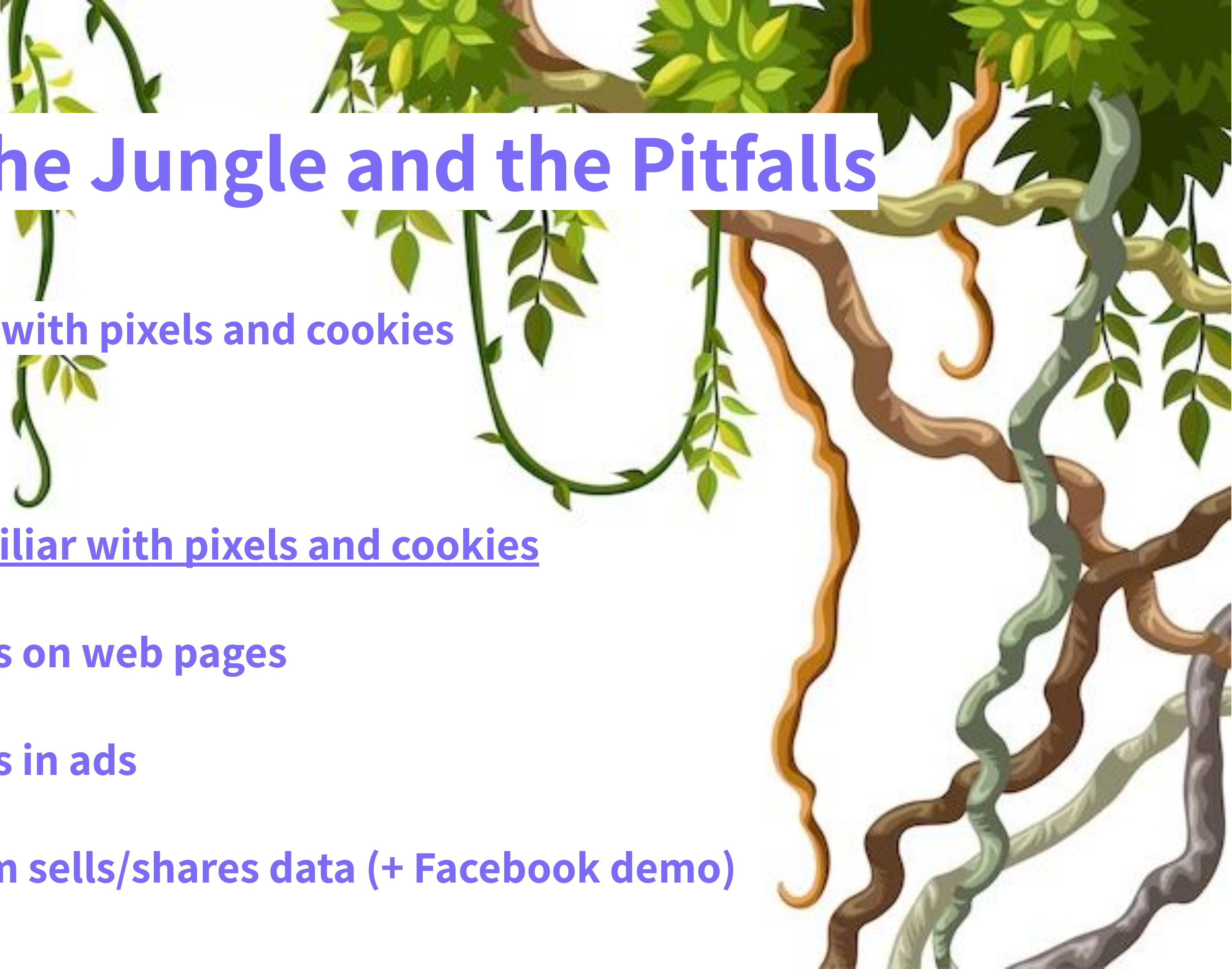
4. **Detect:** Determine what they’re sharing and with whom

5. **Detect:** Determine internal/external uses (e.g., marketing, IT, 3Ps)

6. **Remediate:** Implement notices and consents–use a cookie banner

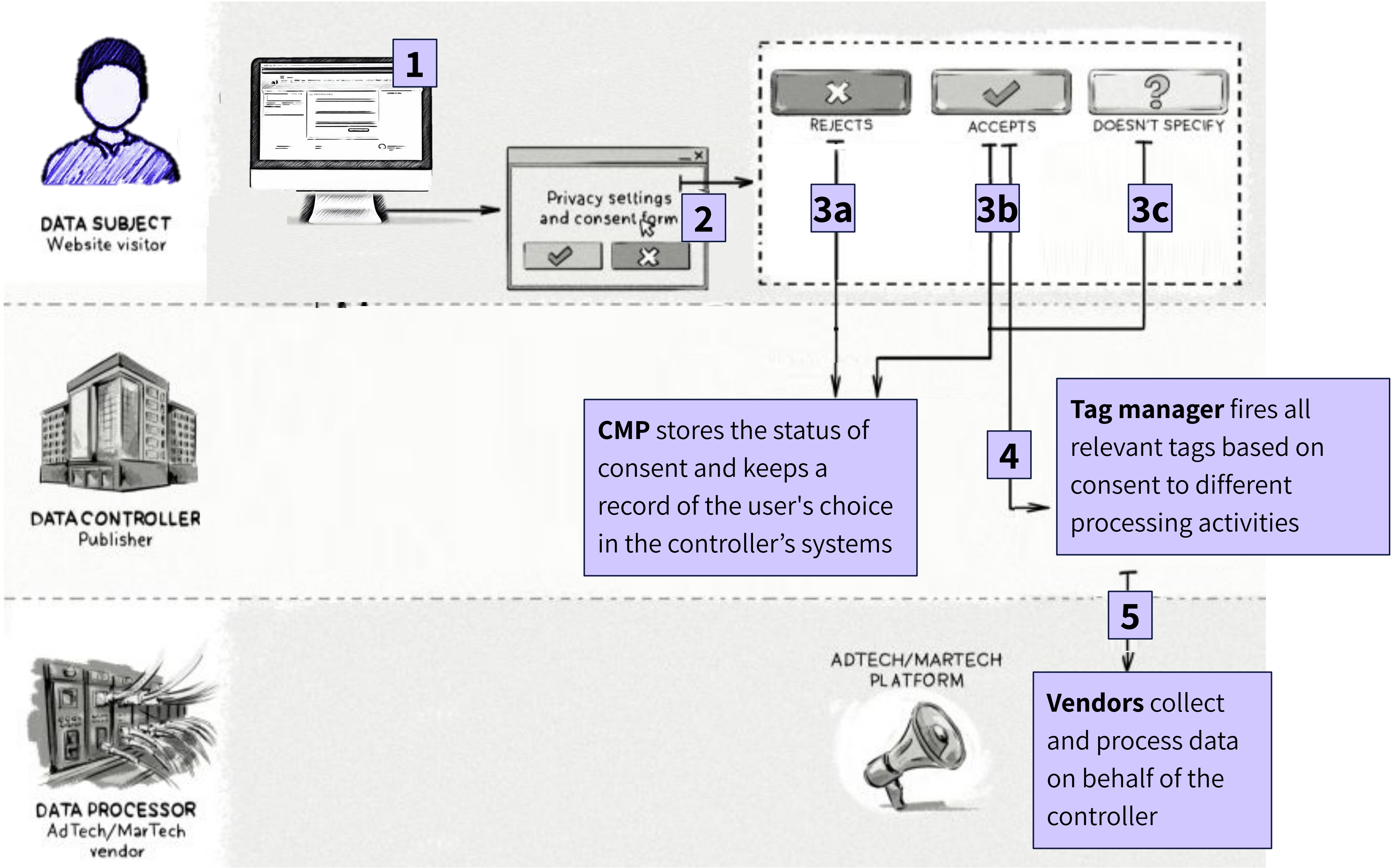
7. **Remediate:** Verify agreements and consents operate as designed

Demystify the Jungle and the Pitfalls



- Legal risks issues with pixels and cookies
- Risk mitigations
- Getting more familiar with pixels and cookies
- Pixels and cookies on web pages
- Pixels and cookies in ads
- How ad ecosystem sells/shares data (+ Facebook demo)

How Is User Consent Captured And Transmitted? (GDPR Terminology)



CMP stores the status of consent and keeps a record of the user's choice in the controller's systems

Tag manager fires all relevant tags based on consent to different processing activities

Vendors collect and process data on behalf of the controller

Adapted from: https://www.linkedin.com/pulse/what-consent-management-platform-cmp-how-does-work-maciej-zawadzinski/

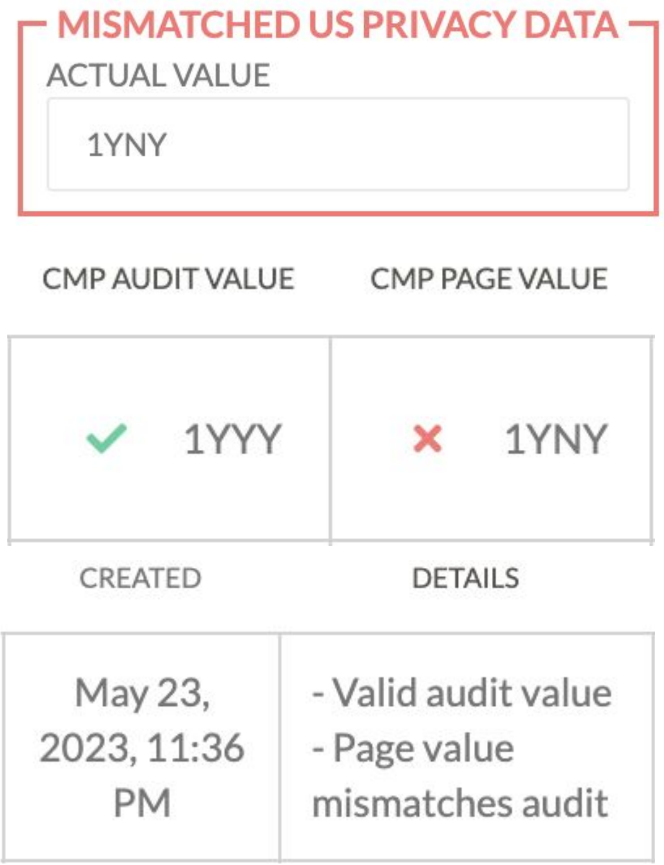
Diagnosing Reason For Loss Of Minors' Opt-Outs

Client: Major Gaming Website

Problem: After new CMP implemented, PI of minors leaked to ad partners despite user opt-out

Solution:

- CMP discovered to be receiving erroneous opt-ins when users intended to opt out
- CMP was re-implemented and QA'd until corrected



MISMATCHED US PRIVACY DATA

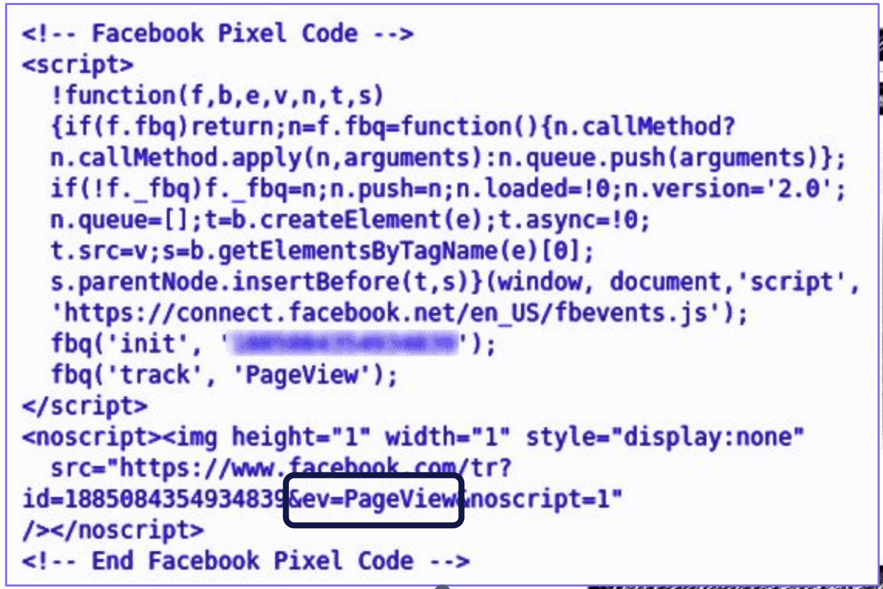
ACTUAL VALUE

1YNY

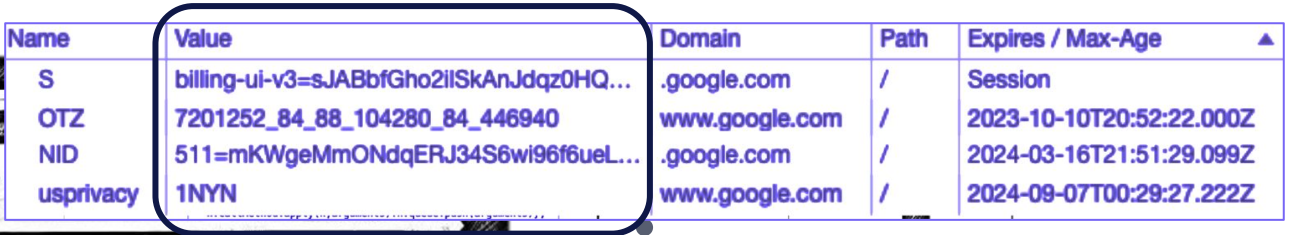
CMP AUDIT VALUE	CMP PAGE VALUE
✓ 1YYY	✗ 1YNY

CREATED	DETAILS
May 23, 2023, 11:36 PM	- Valid audit value - Page value mismatches audit

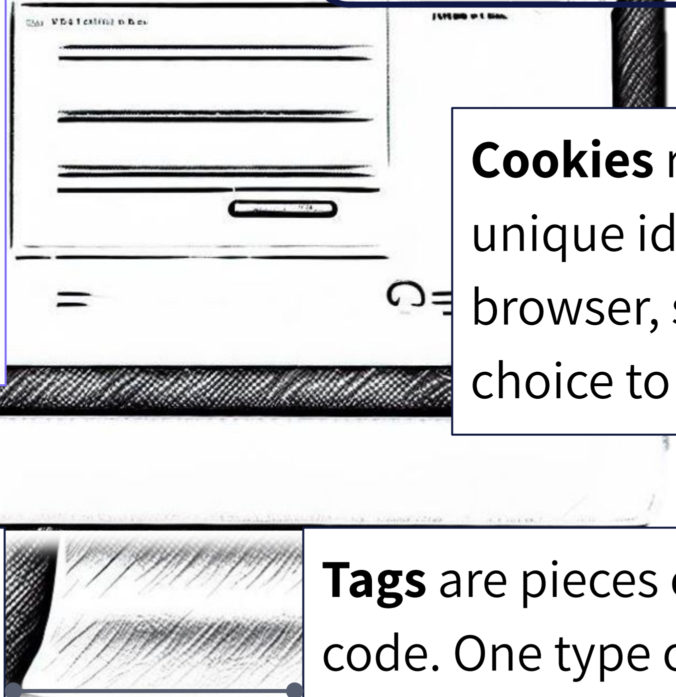
What Are Differences Between Pixels And Cookies?



```
<!-- Facebook Pixel Code -->
<script>
  !function(f,b,e,v,n,t,s)
  {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', '[redacted]');
  fbq('track', 'PageView');
</script>
<noscript><img height="1" width="1" style="display:none"
  src="https://www.facebook.com/tr?
id=1885084354934839&ev=PageView&noscript=1"
/></noscript>
<!-- End Facebook Pixel Code -->
```



Name	Value	Domain	Path	Expires / Max-Age ▲
S	billing-ui-v3=sJABbfGho2ilSkAnJdqz0HQ...	.google.com	/	Session
OTZ	7201252_84_88_104280_84_446940	www.google.com	/	2023-10-10T20:52:22.000Z
NID	511=mKWgeMmONdqERJ34S6wi96f6ueL...	.google.com	/	2024-03-16T21:51:29.099Z
usprivacy	1NYN	www.google.com	/	2024-09-07T00:29:27.222Z



Cookies record user info in a unique identifier text file to a browser, so users have the choice to block or clear them

Pixels are 1X1 or 0X0 images within websites, ads and emails that send user info directly to third party servers. They can't be easily cleared.

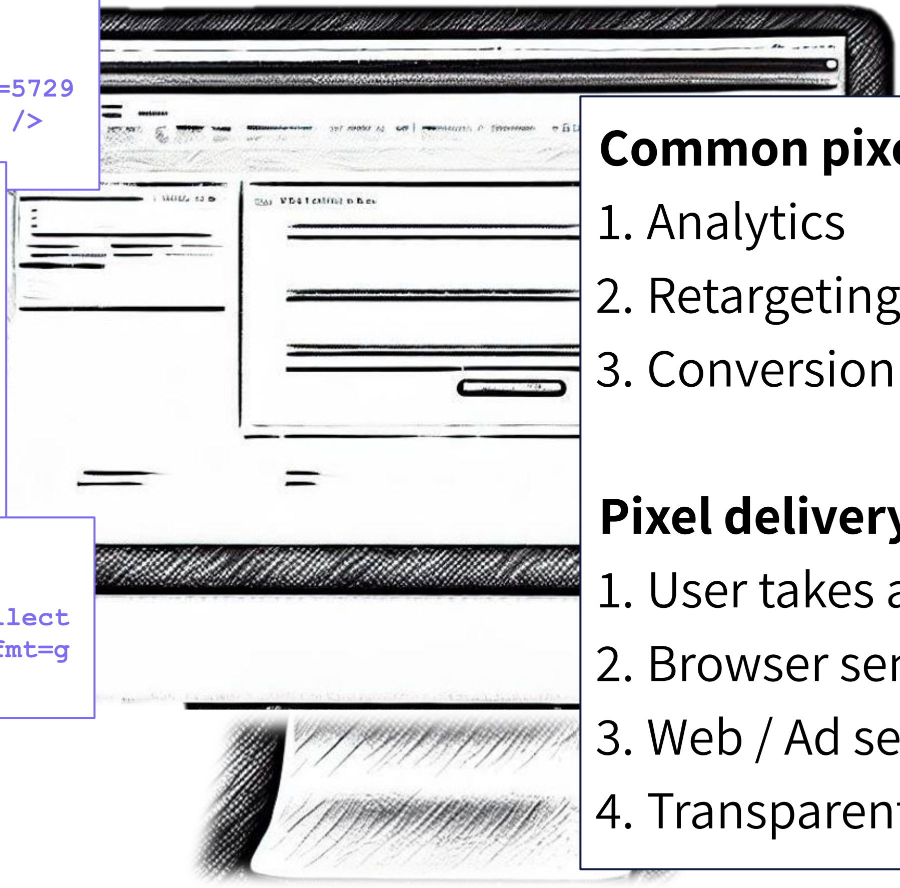
Tags are pieces of javascript in webpage code. One type of tag is a **pixel**. Another type sets **cookies**. Another type may be creative being served.

What Are Common Pixel Types And Pixel Delivery Methods?

```
<img alt="facebook tracking pixel"
height="1" width="1"
style="display:none"
src="https://www.facebook.com/tr?id=5729
69681492733&ev=PageView&noscript=1" />
</noscript>
```

```
</script><noscript><img
src="https://www.autotrader.com/akam/13/
pixel_4c311b9a?a=dD02NTdhYWQxMThiODlhODQ
2M2NiNTY1YTgwZWY4ZWFjYjJiMTlkMTZhJmpzPW9
mZg==" style="visibility: hidden;
position: absolute; left: -999px; top:
-999px;" /></noscript><script
type="text/javascript"
src="/Rvd0Jh/BzKZ/W41y/QYh7/gBAajQM60/fO
S9fkNSmp5p/GBBTSjtmAg/OUEKTDw/ZDUs"></sc
ript></body></html>
```

```
<img height="1" width="1"
style="display:none;" alt=""
src="https://px.ads.linkedin.com/collect
/?pid=4461897&conversionId=9073649&fmt=g
if" />
```



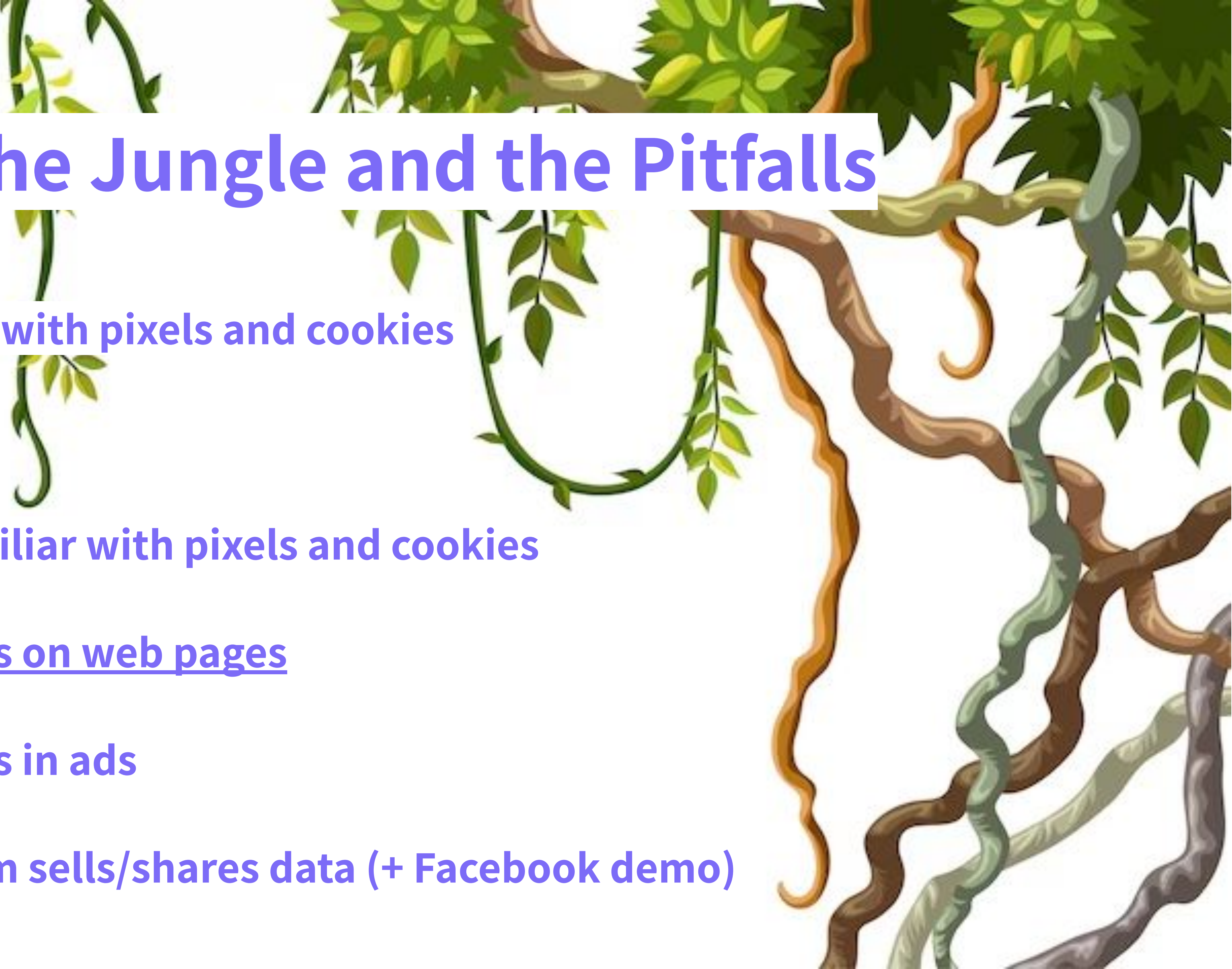
Common pixel types

1. Analytics
2. Retargeting
3. Conversion

Pixel delivery

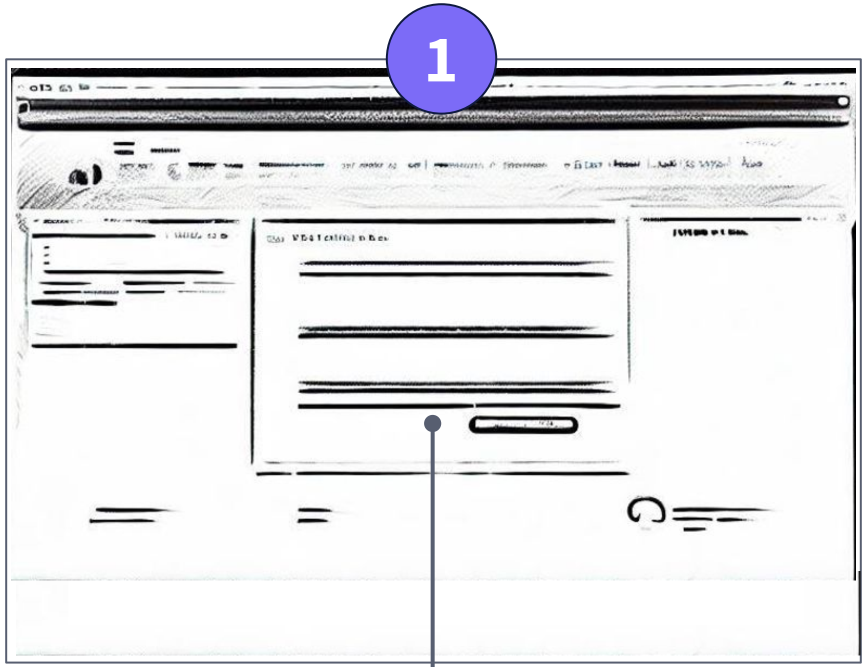
1. User takes action
2. Browser sends request
3. Web / Ad servers respond
4. Transparent element loads

Demystify the Jungle and the Pitfalls



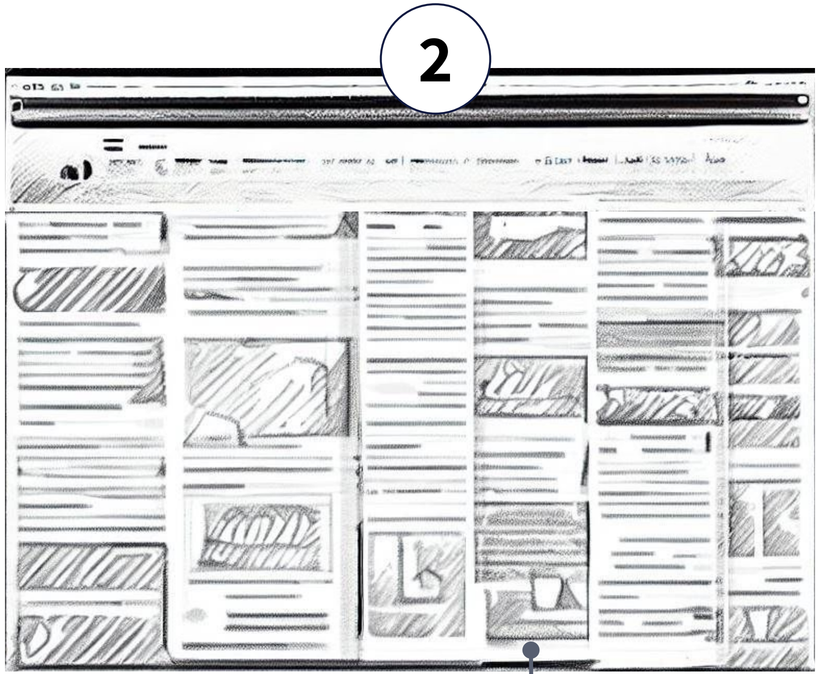
- Legal risks issues with pixels and cookies
- Risk mitigations
- Getting more familiar with pixels and cookies
- Pixels and cookies on web pages
- Pixels and cookies in ads
- How ad ecosystem sells/shares data (+ Facebook demo)

How Do Pixels And Cookies Appear On Web Pages AND In Ads?



https://simage2.pubmatic.com/AdServer/Pug?vcode=bz [illegible]

On Web Pages

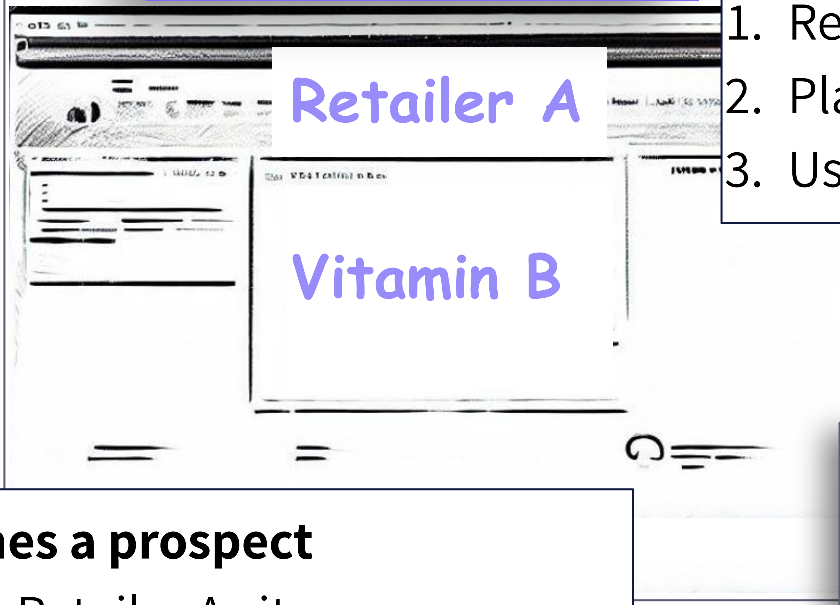


https://simage2.pubmatic.com/AdServer/Pug?vcode=bz [illegible]

In Ads

How Do Web Pages Share User Data?

```
<img height="1" width="1"
style="display:none;" alt=""
src="https://px.ads.linkedin.com/collect/?pid=
4461897&conversionId=9073649&fmt=gif" />
```



User becomes a prospect

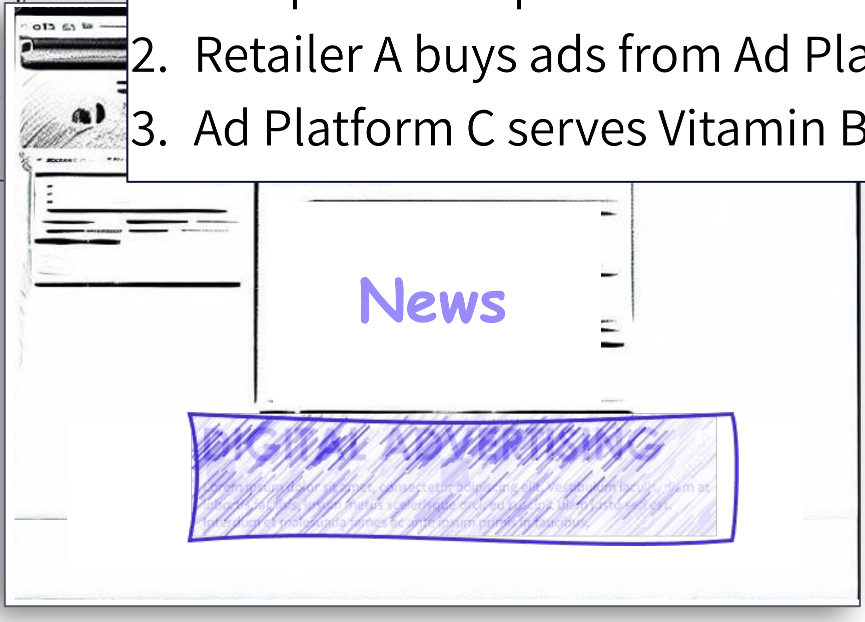
1. User visits Retailer A site
2. User browses Vitamin B
3. User qualifies for tracking

Retailer marks prospect for Vitamin B ads

1. Retailer A placed Ad Platform C's pixel*
2. Platform C's pixel drops cookie
3. User can be tracked, data can be shared

User visits another site

1. Site provides space to Ad Platform C
2. Retailer A buys ads from Ad Platform C
3. Ad Platform C serves Vitamin B ad to User



*Or "tag"

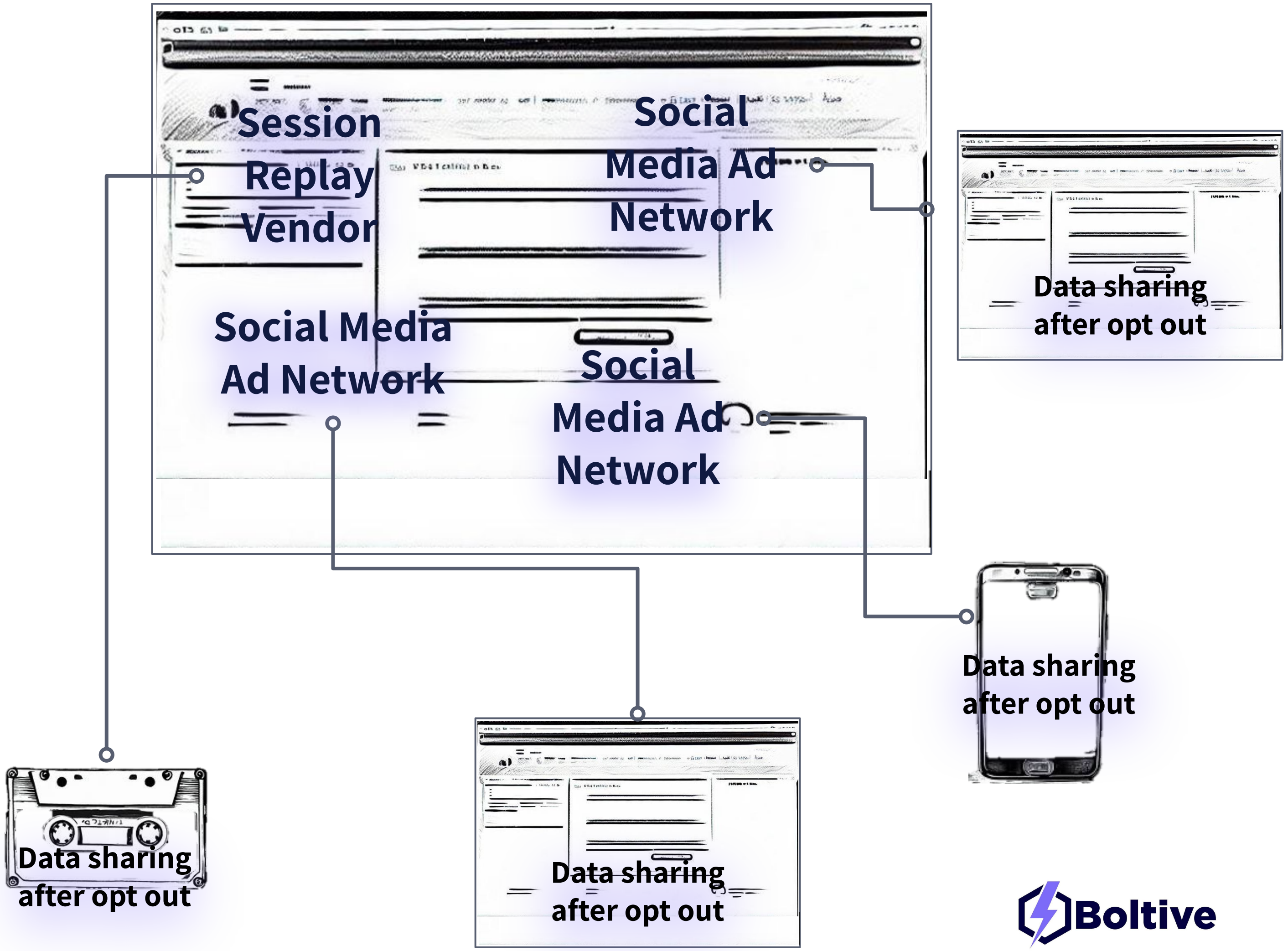
Finding And Eliminating On-Page Cookies And Tags Sharing Information

Company: $15B Travel Company

Problem: Unsure if pixels and cookies were being suppressed when users opted out

Solution:

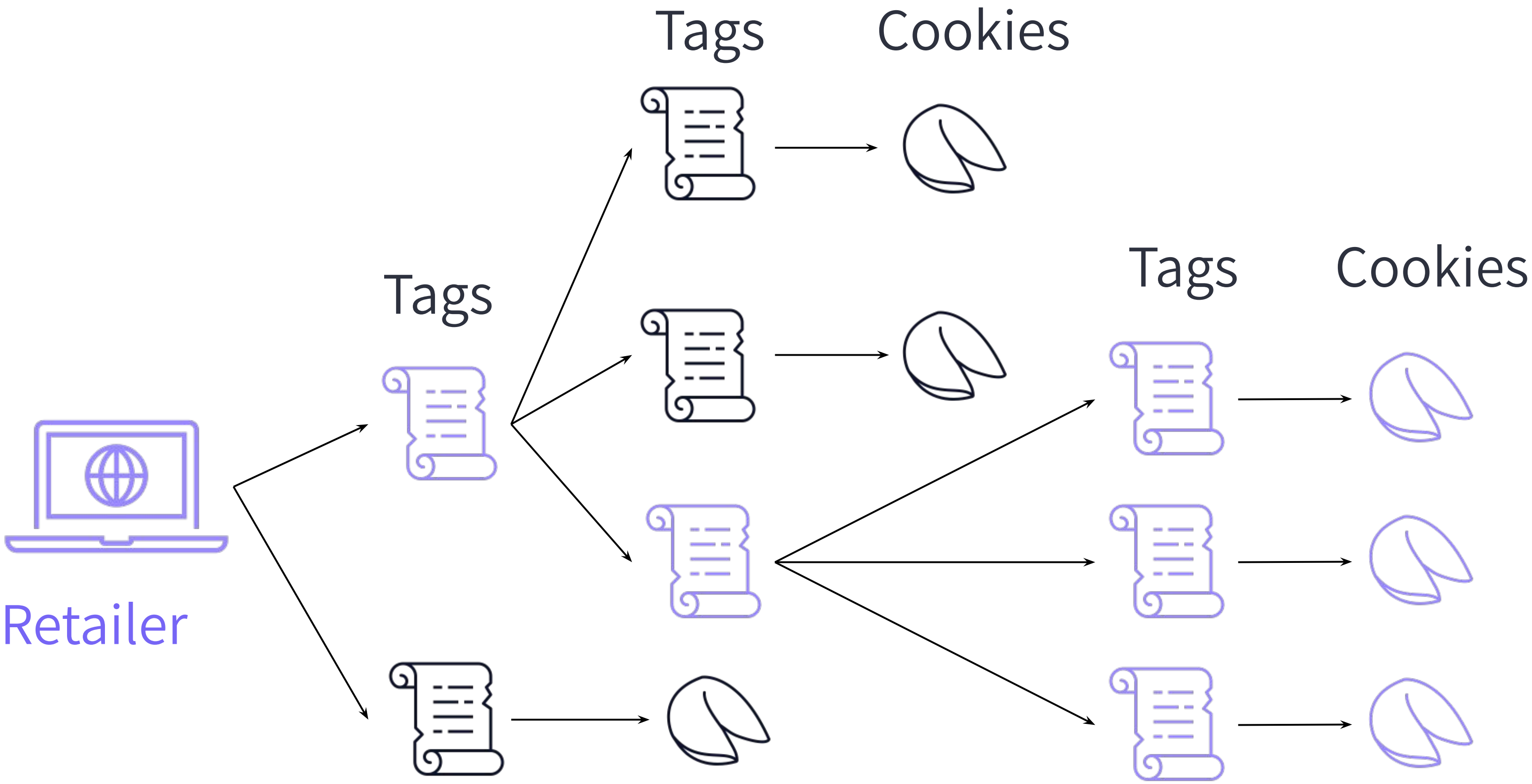
- Found 3 social media networks, a retail media network, and session replay software were sharing data of opted out users
- Created internal governance program providing visibility to existing and new pixels and cookies


Session Replay Vendor
Social Media Ad Network
Social Media Ad Network
Social Media Ad Network
Data sharing after opt out
Data sharing after opt out
Data sharing after opt out
Data sharing after opt out

troutman pepper

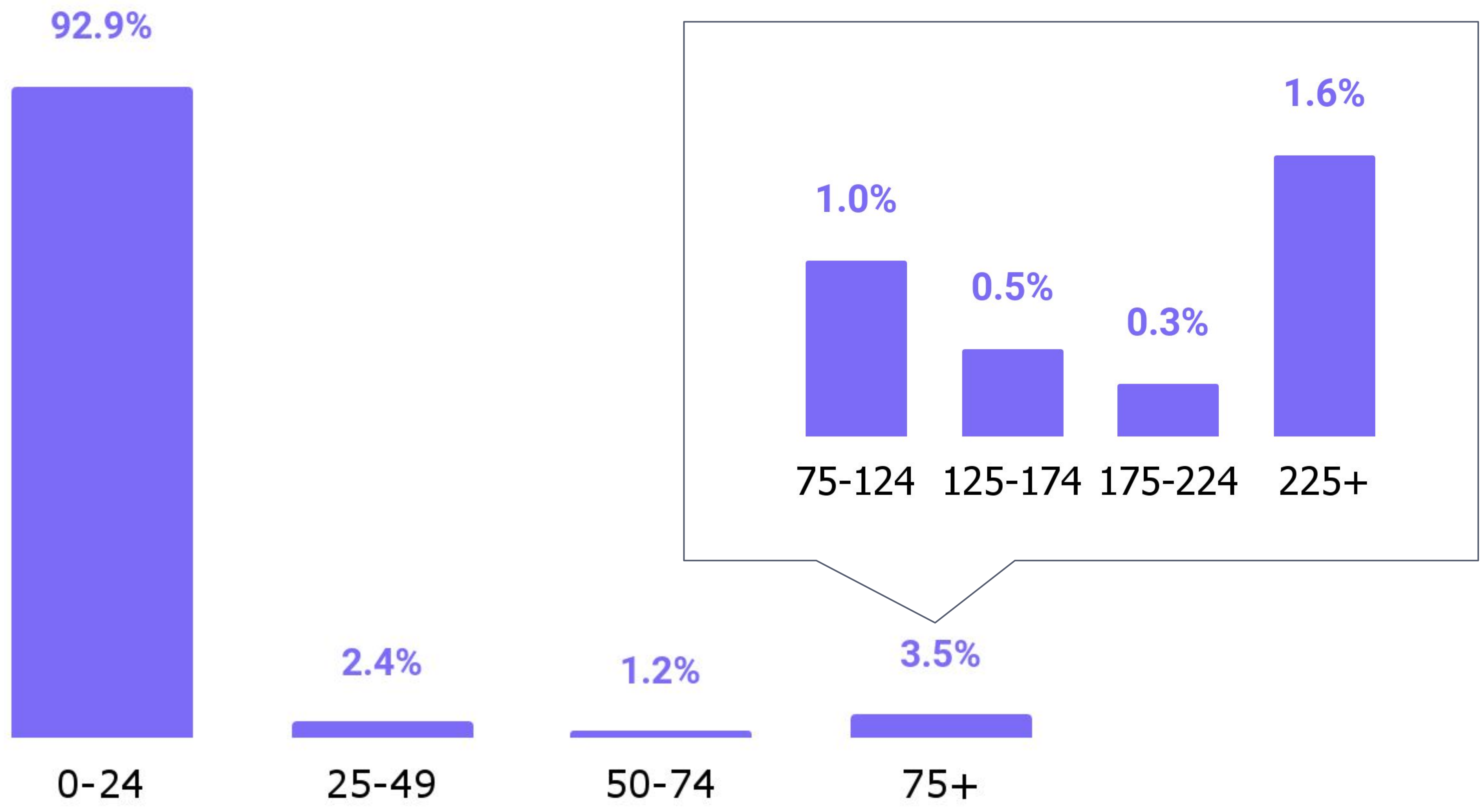
Boltive

When Cookies Piggyback, 4th+ Parties Can Access Consumer Data



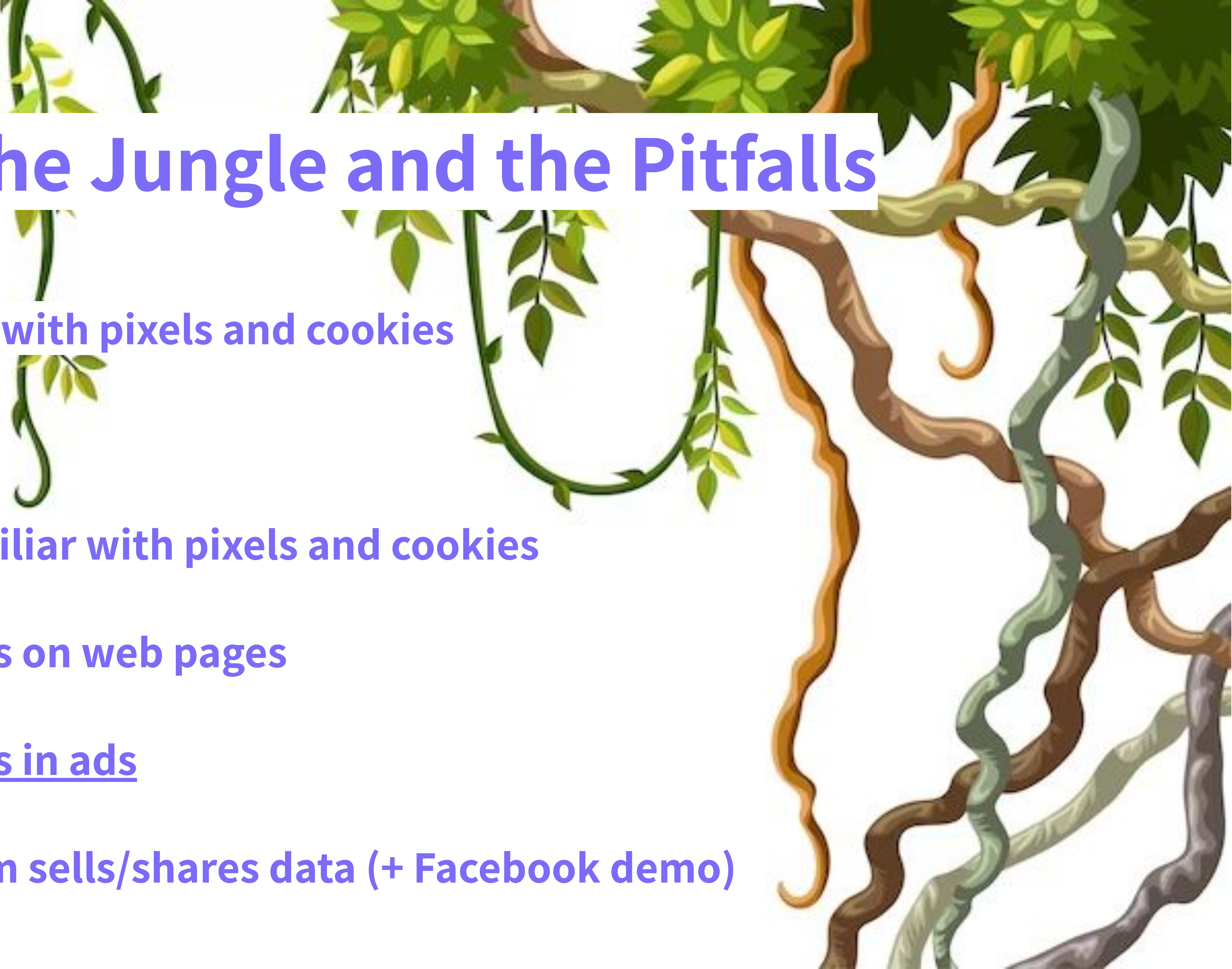
Tags are code snippets or scripts present on web pages. They come from analytics, advertising, and other marketing vendors.

Most Home Pages Have <24 Cookies, While Some Exceed 200



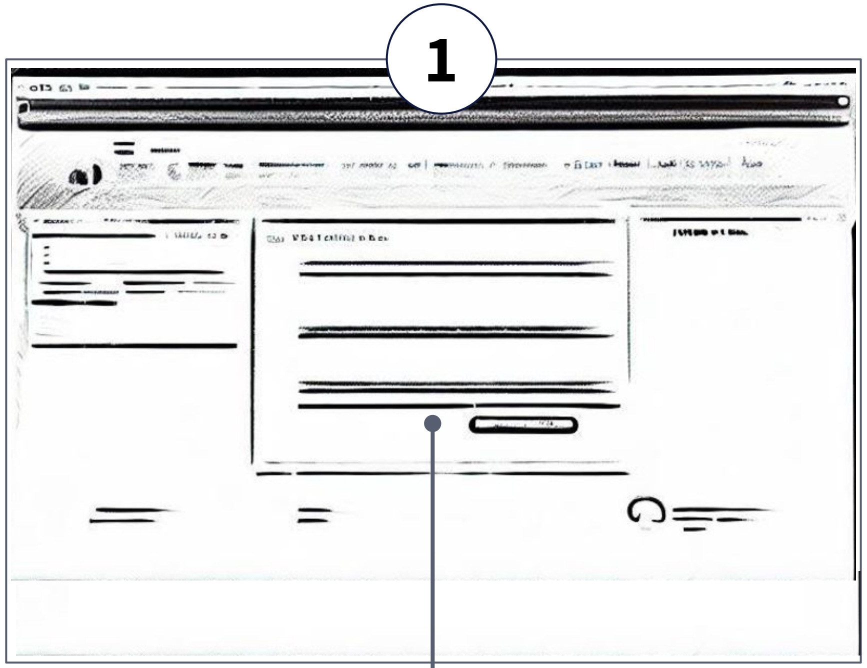
Source: Boltive data and analysis

Demystify the Jungle and the Pitfalls



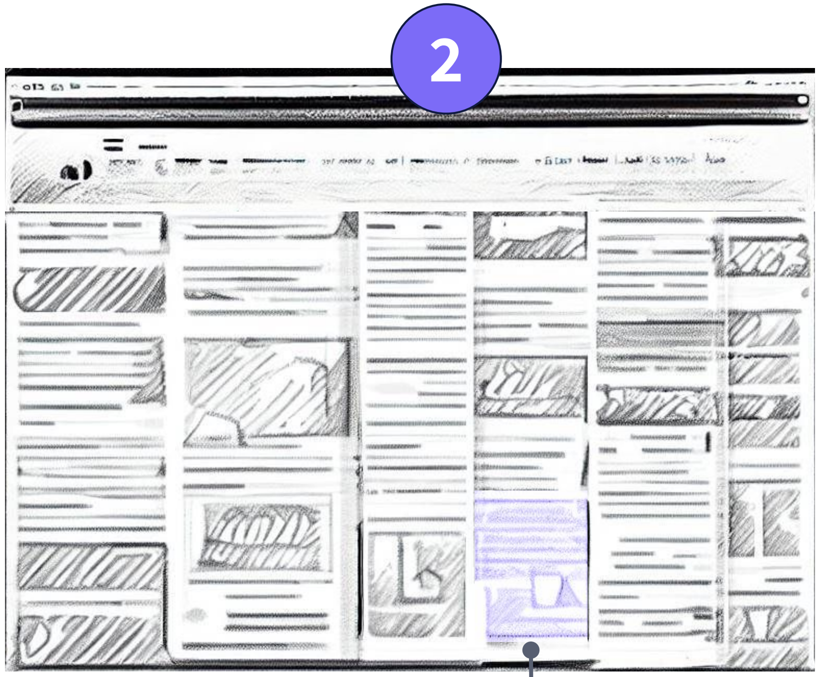
- Legal risks issues with pixels and cookies
- Risk mitigations
- Getting more familiar with pixels and cookies
- Pixels and cookies on web pages
- Pixels and cookies in ads
- How ad ecosystem sells/shares data (+ Facebook demo)

How Do Pixels And Cookies Appear On Web Pages AND In Ads?



```
https://simage2.pubmatic.com/AdServer/Pug?vcode=bz
0yJnRlcGxhdGU9MGZjbI9ldF9yMDMmdGw9MDYyMDA&piggybackCo
okie=RX 9e07e4d2 11b4 4741 bf22 474a1e6f8bd6 0054c
e4cb-7964409832
```

On Web Pages



```
https://simage2.pubmatic.com/AdServer/Pug?vcode=bz
0yJnRlcGxhdGU9MGZjbI9ldF9yMDMmdGw9MDYyMDA&piggybackCo
okie=RX 9e07e4d2 11b4 4741 bf22 474a1e6f8bd6 0054c
e4cb-7964409832
```

In Ads

Finding and Eliminating Unauthorized Facebook Pixels

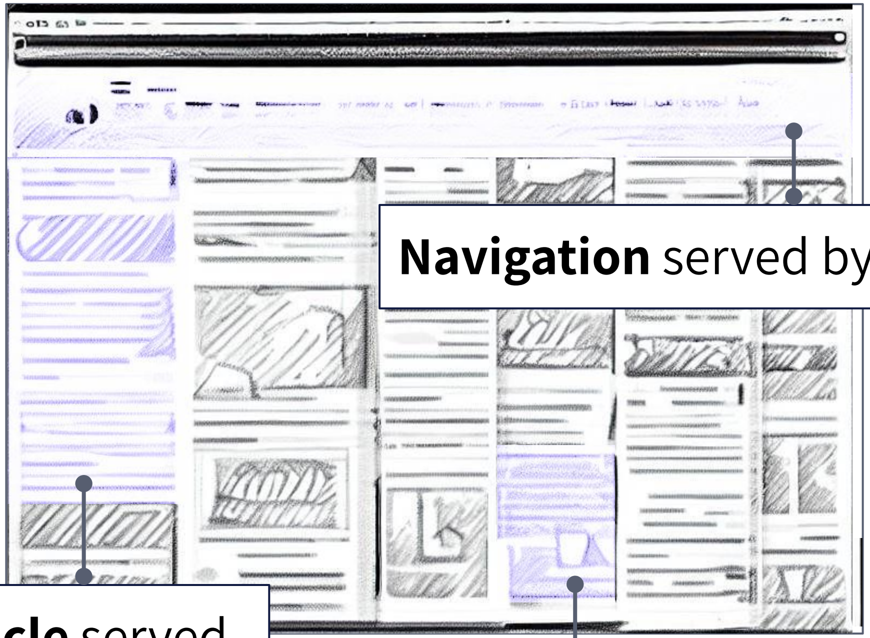
Company: Top Ten Global News Organization

Problem: Leadership received complaints about unauthorized Meta Pixels, but operations team could not find and eliminate them

Solution:

- Scans discovered ads were source of pixels
- Reports identified which SSPs responsible
- Company added blocks to their denylist to prevent recurrence

How Are Third Parties Involved In Page Loads…Including Ads?

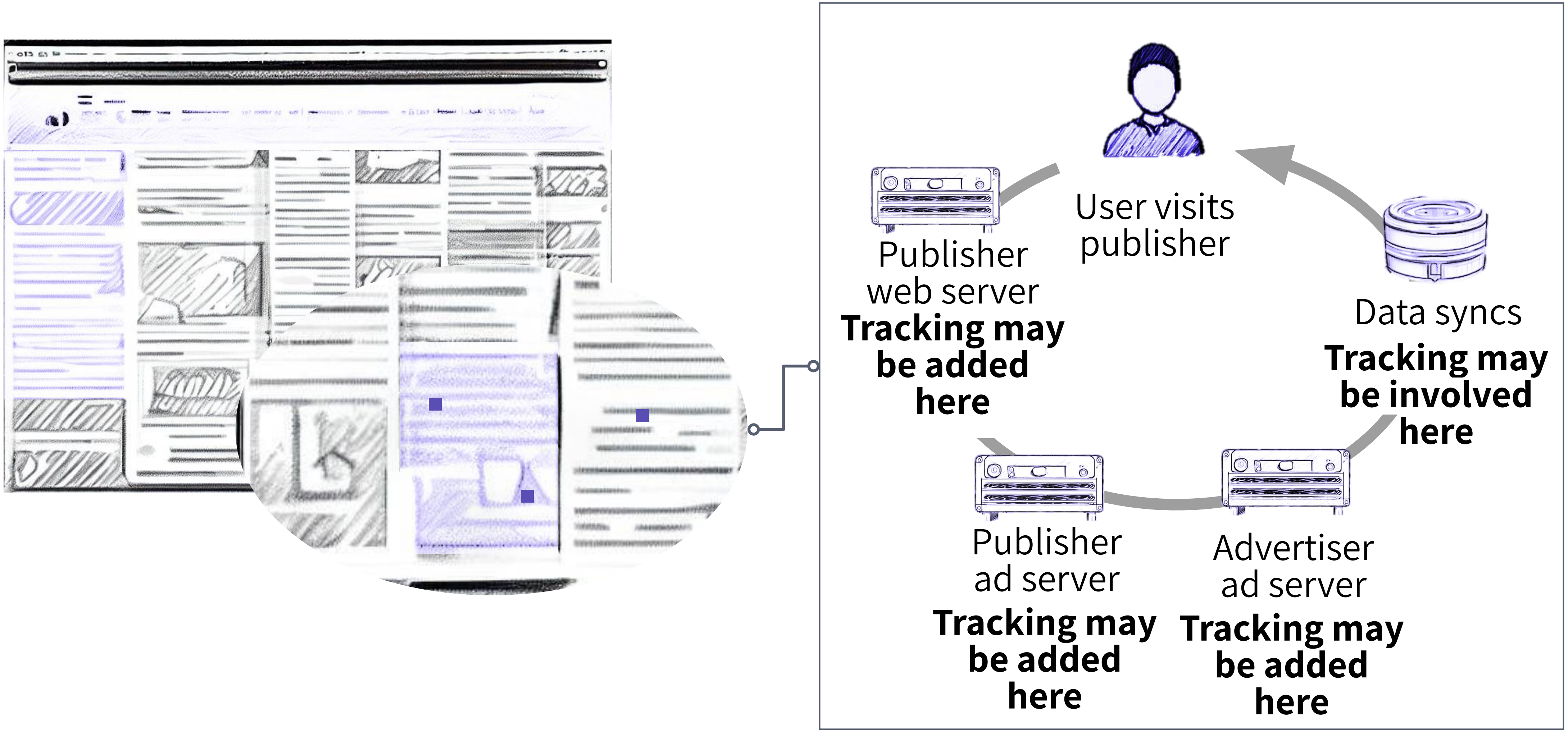


Navigation served by a web server

Article served by a Content Management System (CMS)

Ad served by an ad server

How Is Data Shared By Pixels And Other Means When A User Visits A Site?



User visits publisher

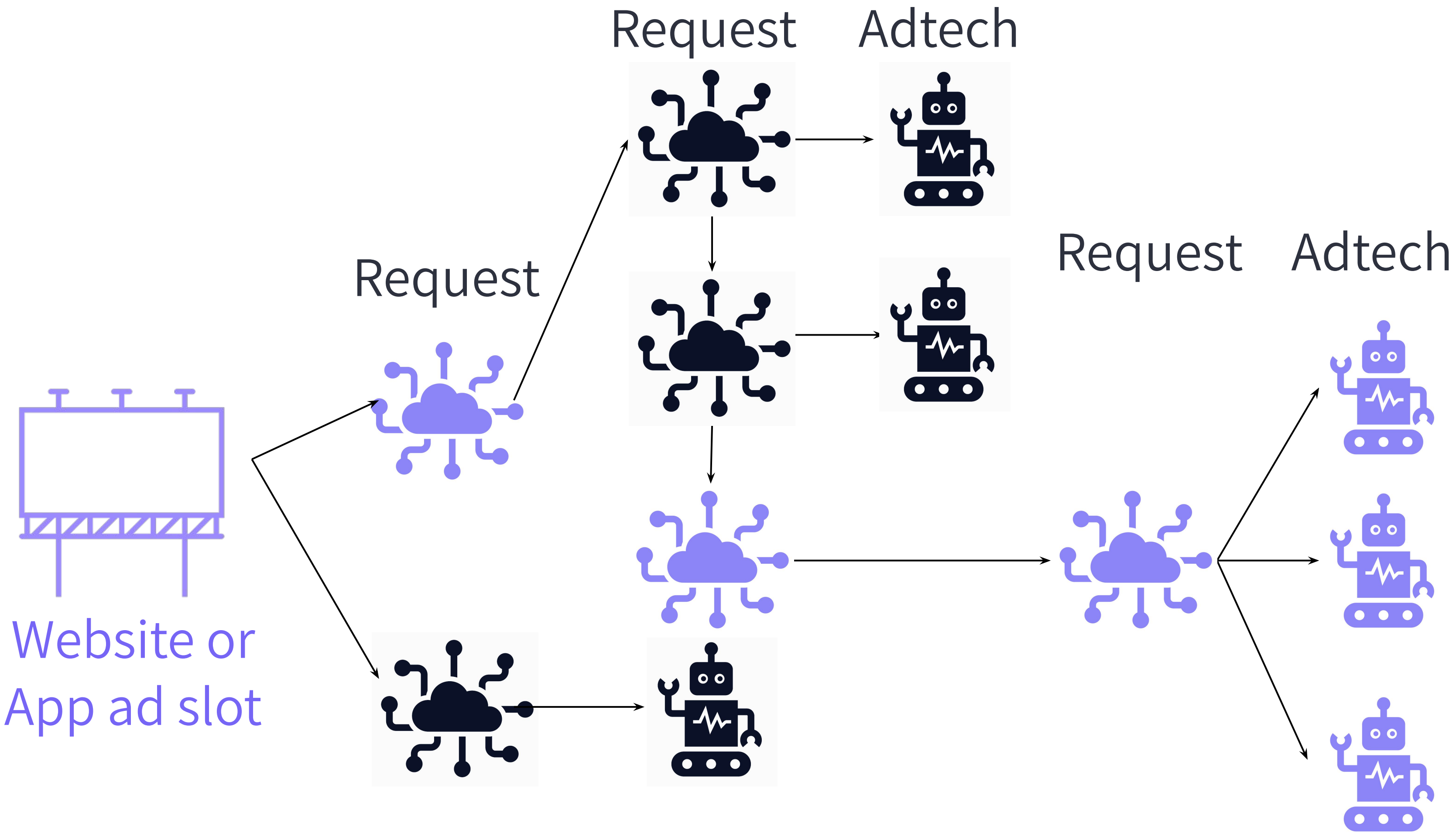
Data syncs
Tracking may be involved here

Advertiser ad server
Tracking may be added here

Publisher ad server
Tracking may be added here

Publisher web server
Tracking may be added here

When Ad Tech Firms Synch, 4th+ Parties Can Access Consumer Data



Network requests transmit between web entities and ad tech vendors. During RTB these data syncs happens in milliseconds.

CASE STUDY

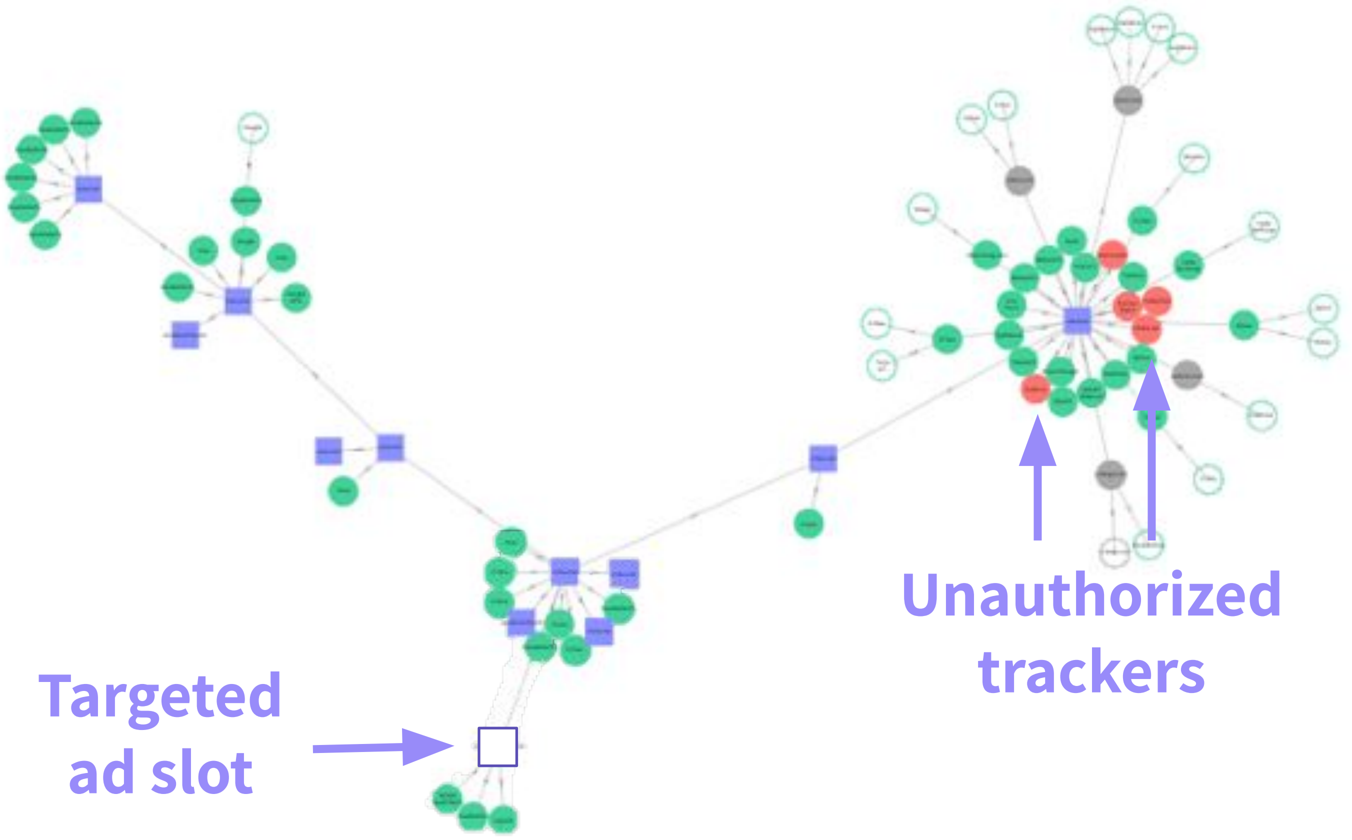
Stopping Leaks To Unauthorized Parties

Client: Top Ten Global Hospitality Company

Problem: $24M fine, unknown parties skimming data

Solution

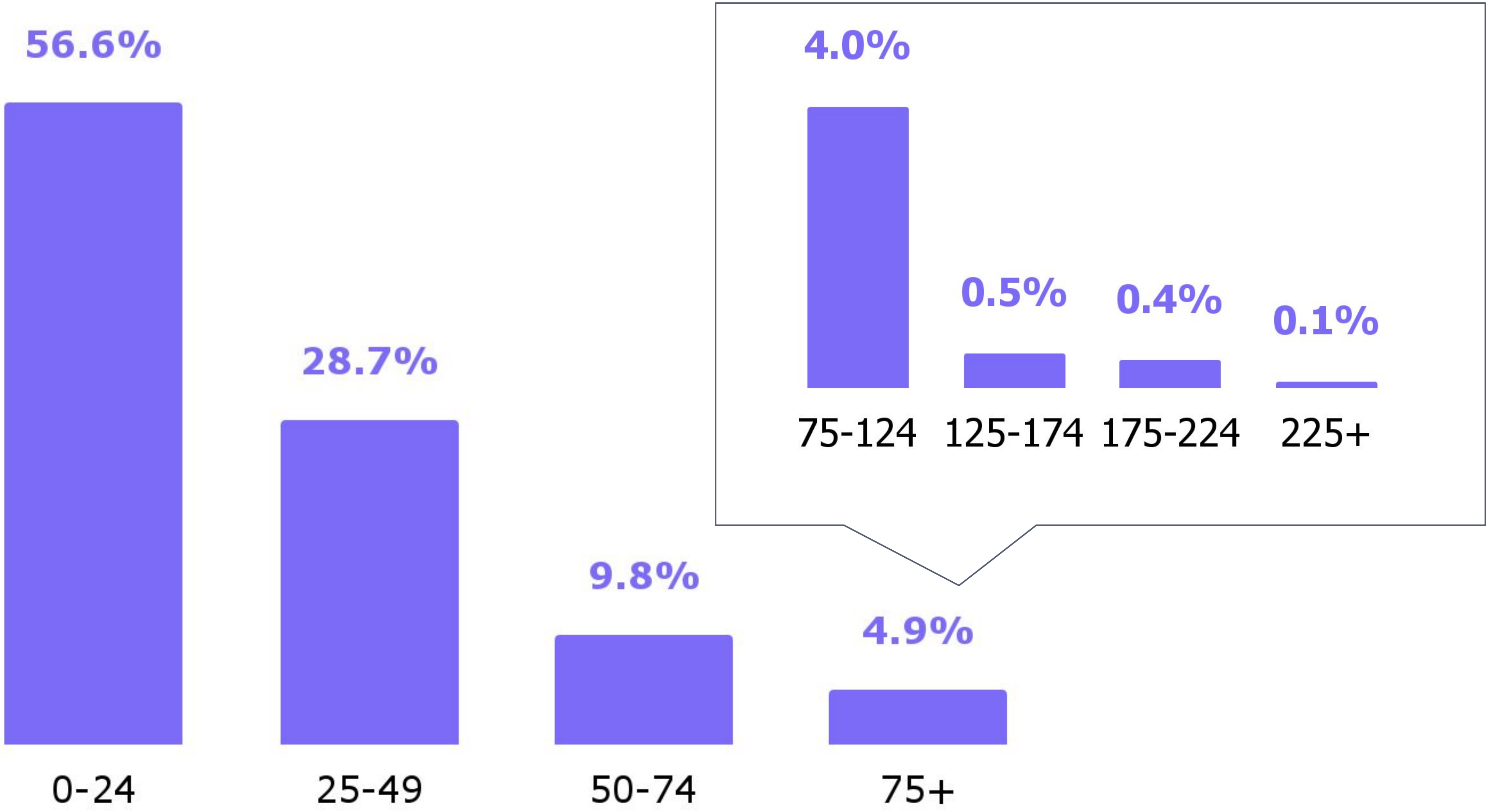
- Stopped leaks to five invalid vendors, including malware distributor
- Avoided further fines and reputation damage



Targeted ad slot

Unauthorized trackers

Most Ads Have <49 Pixels And Other Trackers, While Some Exceed 200



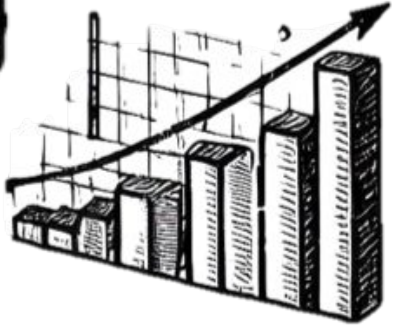
Source: Boltive data and analysis

Demystify the Jungle and the Pitfalls

- Legal risks issues with pixels and cookies
- Risk mitigations
- Getting more familiar with pixels and cookies
- Pixels and cookies on web pages
- Pixels and cookies in ads
- How ad ecosystem sells/shares data (+ Facebook demo)

What Is Third Party Data?

1st party: from people who directly interact with an org's brand
2nd party: 1st party data collected by one org and sold or traded to another
3rd party: supplied by data brokers or DMPs



Publishers and merchants collect data…

- Geolocation
- Browsing history
- Content interactions
- Purchases
- Form info

..And monetize data

- 3rd party trackers on their websites
- Tracking SDK in their apps
- **Pass data to data brokers & DMPs**

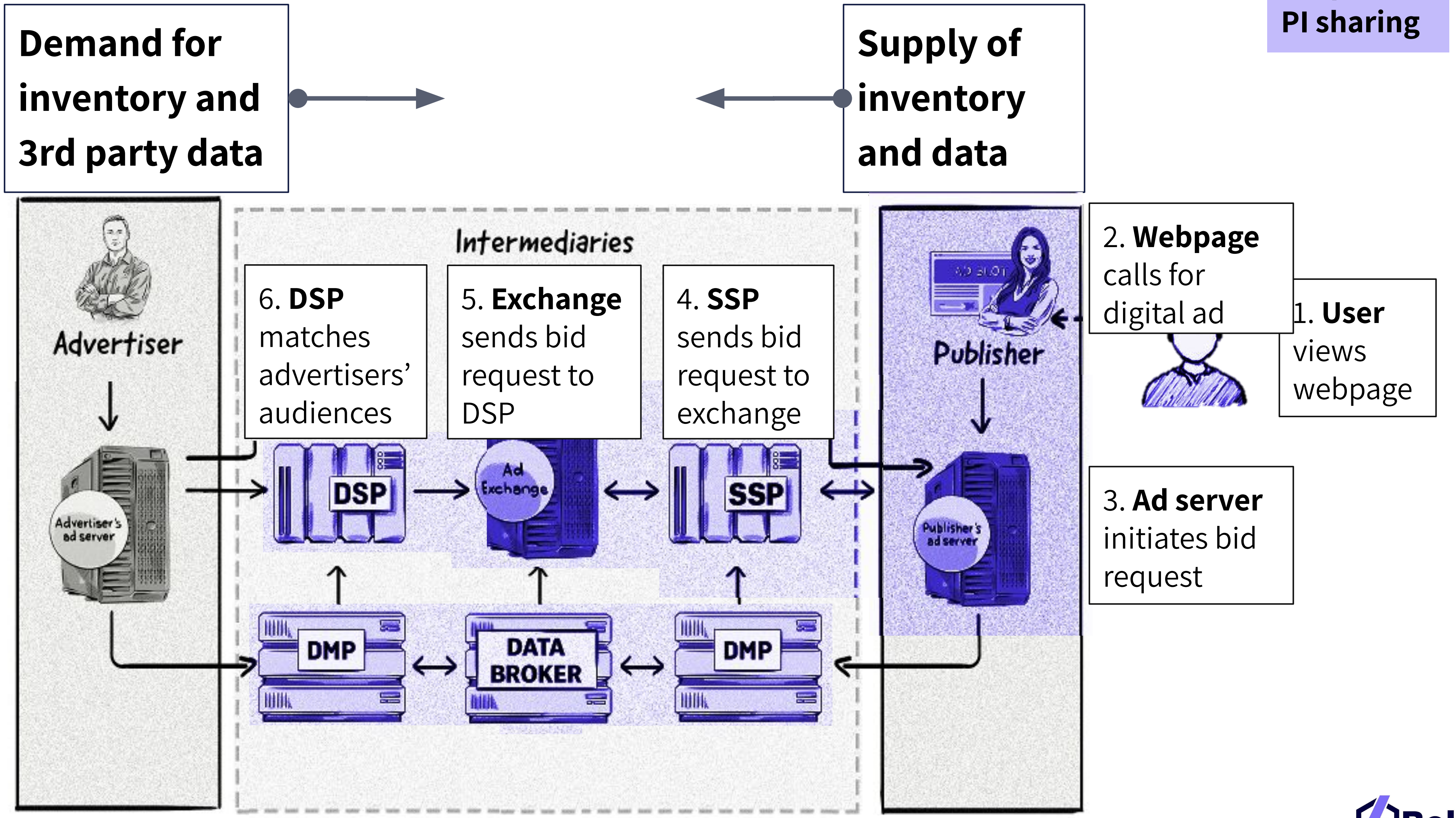
Data brokers and DMPs aggregate so much data they cover almost **every user on the internet.**

How Does The Ad Ecosystem Sell/Share Data?

Purple = PI sharing

Demand for inventory and 3rd party data

Supply of inventory and data



6. **DSP** matches advertisers’ audiences

5. **Exchange** sends bid request to DSP

4. **SSP** sends bid request to exchange

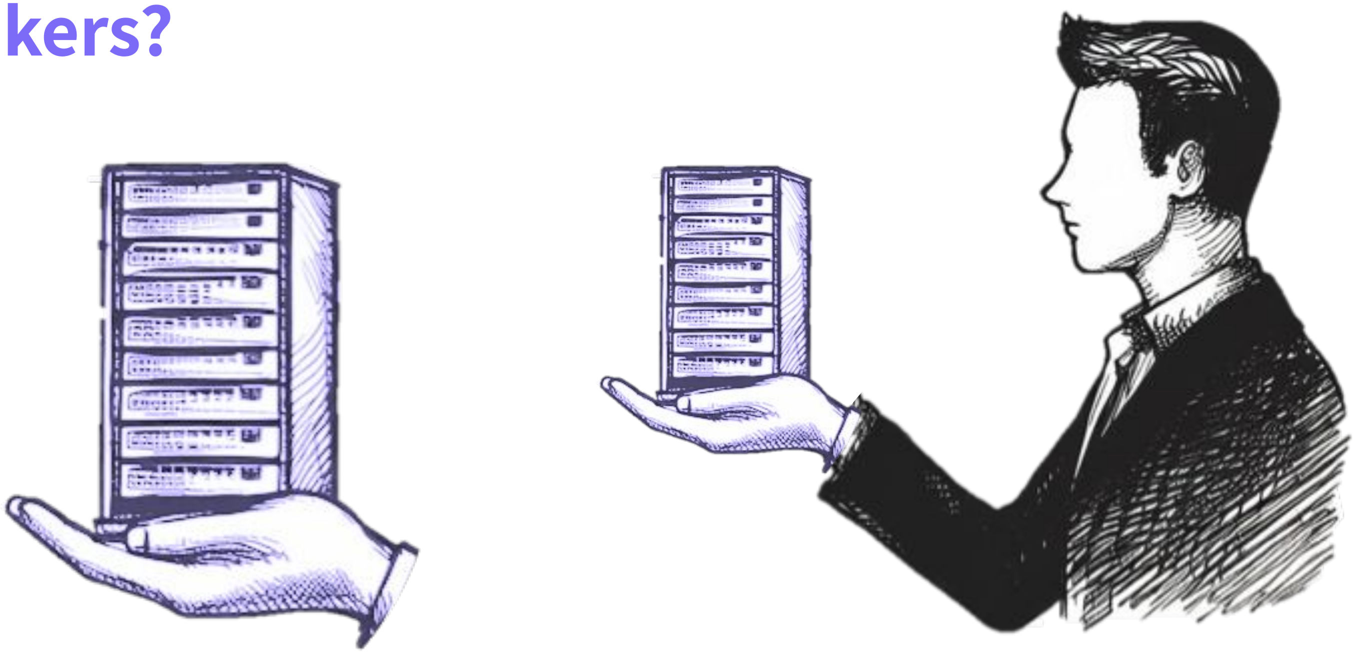
2. **Webpage** calls for digital ad

1. **User** views webpage

3. **Ad server** initiates bid request

Adapted from https://adtechbook.clearcode.cc/adtech-platforms-and-intermediaries/

Who Are DMPs And Data Brokers?



How DMPs collect & combine data:

1. Adding pixels
2. Piggybacking
3. Server-to-server

Vast data collection allows advertisers to improve performance

A DMP is a tech platform. It collects, stores, analyzes, segments, and activates data.

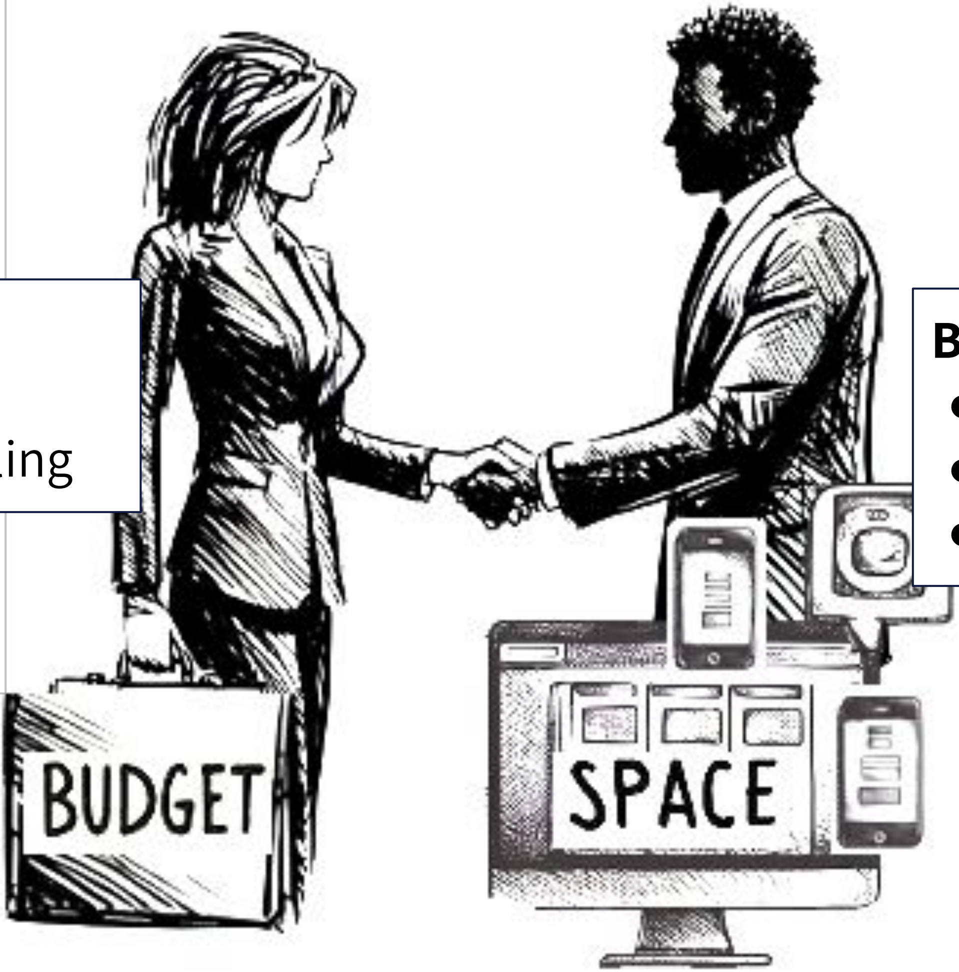
A Data Broker is a business. It performs these functions and licenses data to other orgs.

For today’s purposes, they are similar. Data brokers and DMPs create audience segments. They sell these data sets to marketers

How Is Data Activated?

By advertisers

- Cookie synching
- Lookalike modeling



By publishers

- Cookie syncing
- Segment ID
- Audience extension

Live Demonstration Of Sharing Health Data With Facebook (and Google, and Bing…)

How User-Centric Audits Can Help!

Tracking Technologies 7 Tips for Risk Reduction

Seven Tips to Address Potential Tracking Technology Issues

1. **Prevent:** Internal controls (e.g. SDLC for web/app) checkpoints limiting who can can change code

2. **Prevent:** Add a checkpoint in your vendor contracting and PIA processes

3. **Detect:** Prepare an inventory of cookies and trackers

4. **Detect:** Determine what they're sharing and with whom

5. **Detect:** Determine internal/external uses (e.g., marketing, IT, 3Ps)

6. **Remediate:** Implement notices and consents–use a cookie banner

7. **Remediate:** Verify agreements and consents operate as designed

Audits Support Detect & Remediate Tips For Risk Reduction

	Assessments		
	Data	**Legal**	**Trade-off**
A. Consent	Are your consent systems operating as intended?	Does consent required satisfy legal requirement for a jurisdiction?	What is business value vs. legal risk of collecting your data elements?
B. Third parties	What pixels, cookies are on your web pages? What SDKs and other external data sharing mechanisms are in your apps? What other adtech vendors see data?	Do your notice and consent disclosures accurately describe what you're doing?	What is business value vs. legal risk of partnering with third parties?
C. Sharing	What data are you sharing with these third parties? How do third parties use data they receive?	Do you have agreements with the recipients? Do the agreements put the recipient in the right category by restricting use?	What is business value vs. legal risk of sharing particular data with particular third parties?
Specifically ….	Are you including trackers (pixels, cookies, SDKs) in B, C? Does your current DSR process include this expanded scope of data?	Are you compliant?	Are you including trackers in B, C? Are there less intrusive methods to achieve the business value of A, B, C? What are your processes for approving data elements and auditing third parties?

Questions?

The Ad Tech Ecosystem:
Demystify the Jungle and the Pitfalls

James Koenig
Partner
Troutman Pepper
jim.koenig@troutman.com

Dan Frechtling
CEO
Boltive
dan@boltive.com

Joel Lutz
Counsel
Troutman Pepper
joel.lutz@troutman.com

Appendix: Ad Tech Ecosystem Glossary

Key Ad Tech Lingo

- **RTB—**Real Time Bidding—process for bidding on digital ad impressions as the webpage or app serves content to the visitor.
- **Programmatic Advertising**—automated method of buying ad space in digital media using data, usually in real time, to make decisions on whether and how much to bid on an ad impression on an impression by impression basis.
- **SSP**--Supply (or Sell) Side Platform—technology (or company providing the tech) for publishers to sell their advertising inventory through RTB. Enables publishers to auction their ad space/impressions to multiple advertisers who have demands to bid for the right to place their clients' ads.
- **DSP**—Demand Side Platform—technology (or company providing the tech) for digital media (e.g. ad impression) buyers that want to buy the right to display advertisers' ads in particular ad spaces/impressions
- **DMP**—Data Management Platform—technology platform that can combine 1st and 3rd party data about individuals from any source, including online, offlilne, mobile etc. Often used to combine 1st party data with data obtained from data brokers. Used by both supply and demand side, including for cookie synching.

Key Ad Tech Lingo

- **CMP—Consent Management Platform—**technology platform that helps ad tech platforms collect user consent and pass that data to downstream advertising platforms.

- **Ad Server—**On supply (publisher side) technology (literally a server) that makes decisions about which ads to show on a digital media and report information about the ad that is displayed to other parties in the ad tech ecosystem. These can be 1st party (i.e., the publisher's own ad server) or 3rd party (i.e., a service provider to the publisher) On the demand (advertiser side) this technology usually handles the actual ad creative and literally serves it into the ad space once the ad winning the bid is selected. This can be done directly or through the ad exchange platform connecting to the supply-side ad server.

- **Ad Exchange**—technology platform that facilitates buying and selling process of available impressions between advertisers, who place their bids via DSPs, and publishers, who sell their inventory of ad space/impressions through SSPs or directly with the ad exchange. These technology platforms run the access process.

Appendix: Third Party Cookie Alternatives

Third Party Cookie Alternatives

- **Universal IDs and device graphs—**essentially the ad tech players must agree to adopt a common ID that users can control (opt out of) and those ad tech players in the "network" can use. Open source concept (e.g., Tradedesk UID2.0)
- **Data Clean Rooms—**two party exchange of 1st party data with advertiser without putting 1st party user data in the wild (e.g. Amazon creating a clean room service). Use hashed email etc to make match
- **Google Chrome's Privacy Sandbox—**open standard for adoption that will restrict user data shared but enable segmented and retargeting and attribution.
- **The IAB Tech Lab's Seller Defined Audiences—**standard segmentation created by publisher and passed to advertiser through OpentRTB. Publisher 1st party data not shared.
- **Self-serve ad platforms—**Publishers build their own platforms to sell ad space directly to advertisers
- **Contextual Targeting—**Old fashioned contextual advertising but with more dynamic information about context