

AdTech and Privacy: Managing Risk in a Complex and Evolving Digital Economy

April 15, 2020

The Hogan Lovells logo consists of the words "Hogan" and "Lovells" stacked vertically in a serif font, enclosed within a solid lime green square.

Hogan
Lovells

Our Panel



Heather Dunning

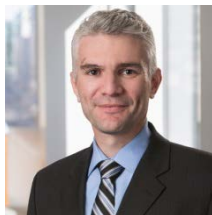
Senior Director
Ankura, Chicago

PANELIST

Heather is a Senior Director in Ankura's Technology, Privacy and Cyber Risk Advisory practice. Heather has led countless global data privacy initiatives for one of the world's largest media conglomerates.

She has extensive experience in assessing organizations for compliance with the GDPR and CCPA by spearheading data privacy reviews of proprietary technology, performing vendor risk assessments and overseeing multiple legally mandated recordkeeping exercises. She is currently serving as a privacy manager for a large household electronics company where she has overseen the organization's data inventory, created and implemented a consumer rights request process and drafted and operationalized several data privacy policies and procedures. In addition, Heather has extensive knowledge in advertising technology, product management and big data.

She holds both CIPM and CIPP/E certifications from the International Association of Privacy Professionals. Heather excels at creating new and repeatable processes for organizations and understanding how data privacy laws apply to technology.



W. James Denvil

Senior Associate
Hogan Lovells, Washington, D.C.

PANELIST

James Denvil is a senior associate in the Privacy and Cybersecurity practice at Hogan Lovells. He helps brands, publishers, and intermediaries develop strategic compliance programs designed to address risk globally and across platforms.

By closely following legal developments and monitoring the positions taken by key academics and advocacy groups, James is able to help clients anticipate and prepare for future challenges.



Darin Bielby

Senior Managing Director
Ankura, Philadelphia

HOST

Darin Bielby is a Senior Managing Director with 25 years of experience assisting companies, and their law firm advisors, to address critical business risks.

Darin helped build Ankura's industry leading Cybersecurity Practice which has worked on over 3,500 cyber investigations for companies globally over the last 10 years. Darin works with clients to help them address compliance with GDPR, CCPA, and other evolving global privacy and data regulations.

Agenda

Our Panel

What Are Cookies?

Legal & Regulatory Challenges For Cookies

The Future Of Cookies

Best Practices In A GDPR And CCPA World

What's In The News

Upcoming Webinars

What are Cookies and/or Tracking Technologies?

Cookies are perhaps the most common tracking tool, but there are others such as Mobile Ad Ids, pixels, beacons, and more. **The core issues tend to be the same.**

What is a web cookie?

A small text file generated by a website and saved by your web browser.



Strictly Necessary Cookies

Essential in order for a website to function.



Functional Cookies

Allows the website to remember visitors' choices such as their username, language, or region and provide more enhanced, personal features.



Performance Cookies

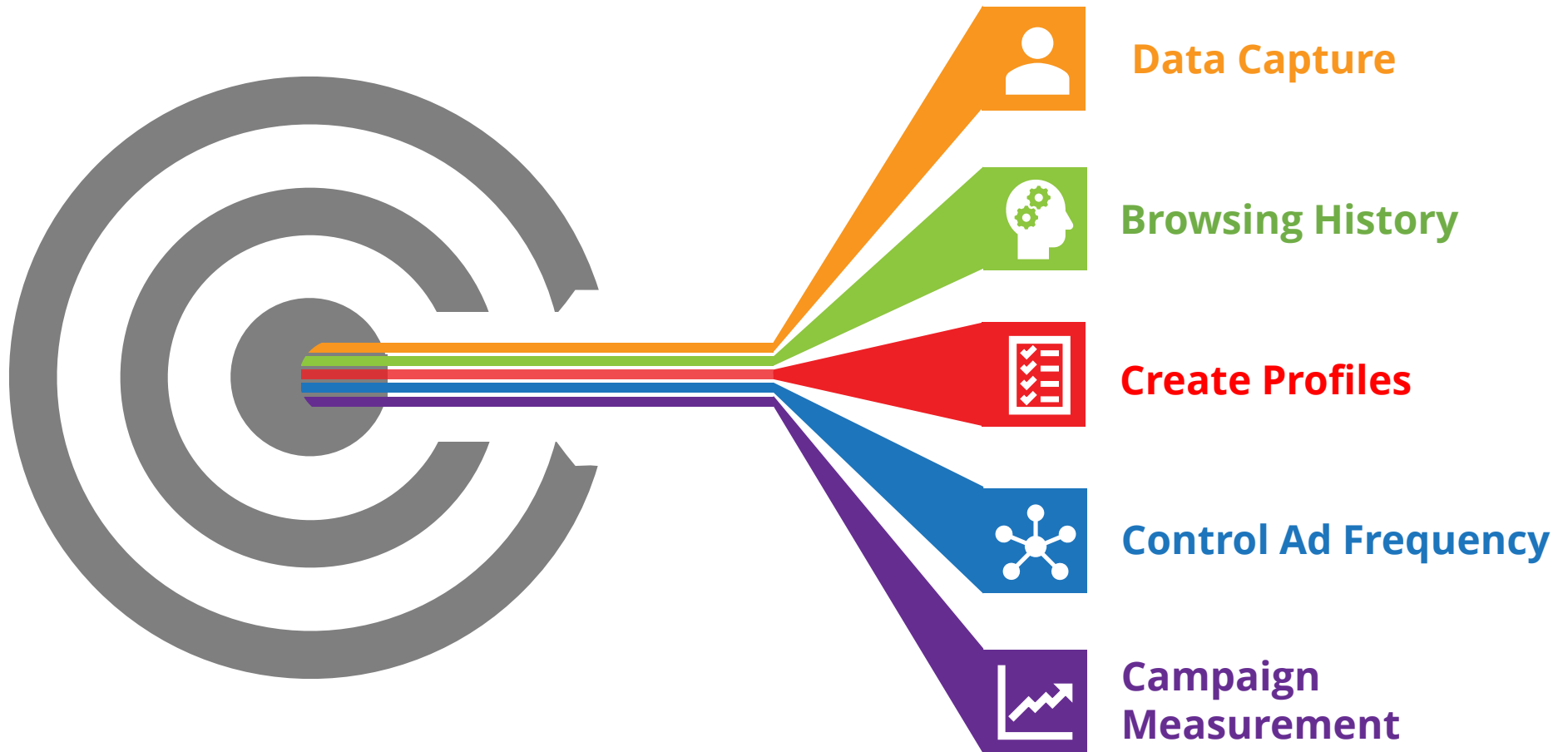
Collects information about how visitors use a website..



Targeting/Marketing Cookies

Used to deliver ads that are more relevant to site visitors and their interests.

Marketing Cookies



First Party vs. Third Party COOKIES

FIRST PARTY



First-party cookies are set by the website owner visited by the user. Primarily, publishers (website owners) have access to data collected using first-party cookies, which can later be shared with advertisers or agencies for ad targeting.

First-party cookies may be preferable because you have a direct relationship with the individual visiting your website and can provide appropriate notice.

Example

- Analytics tools use first-party cookies to understand user behavior and present it in tabular or graphical form for the publisher's understanding.

THIRD PARTY



Third Party cookies are set by domains that are not directly visited by the user. This happens when publishers add third-party elements (like chatbots, social plugins, or ads) on their websites. Third-party cookies can track user activities for ad targeting and behavioral advertising, including for use by other third parties.

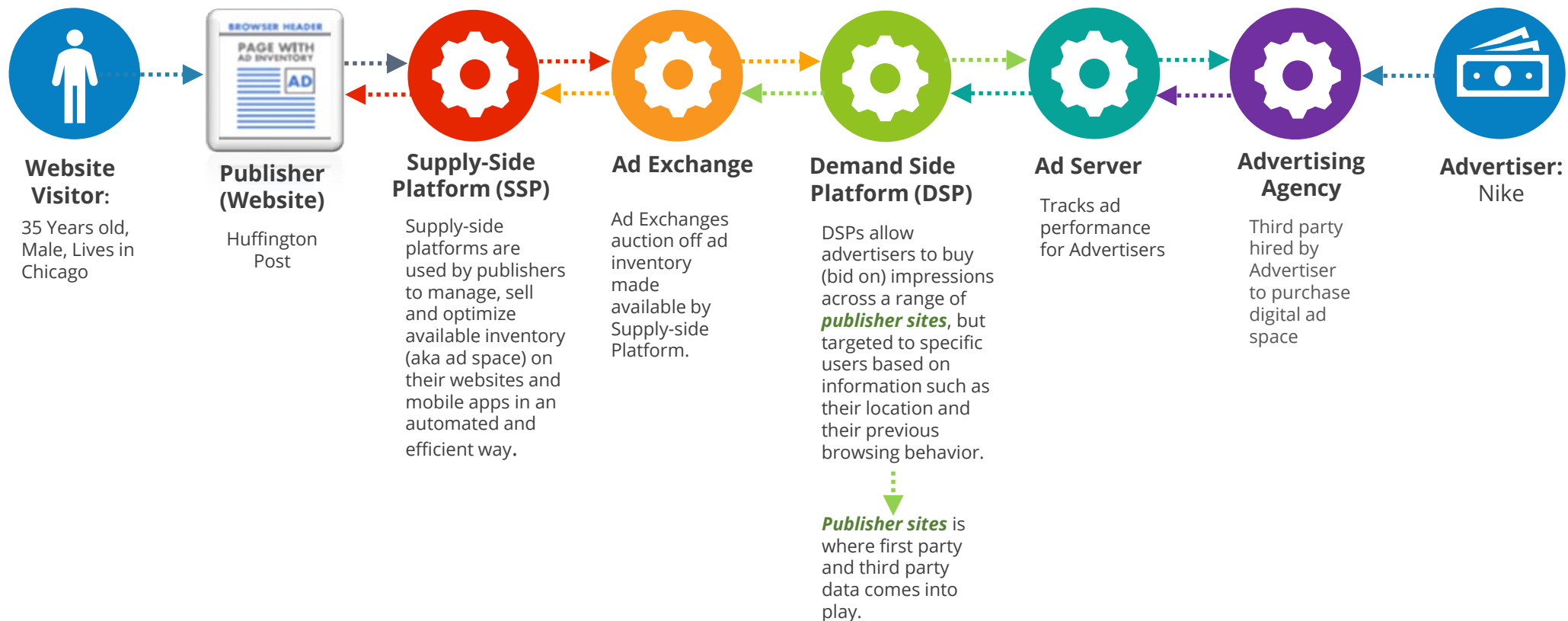
Example

- A third-party advertising partner sets and reads a cookie on your website's visitors. That cookie allows the third party to learn about the visitors' activities on any sites that allow the third party to set cookies.

Online Behavioral Advertising (OBA)

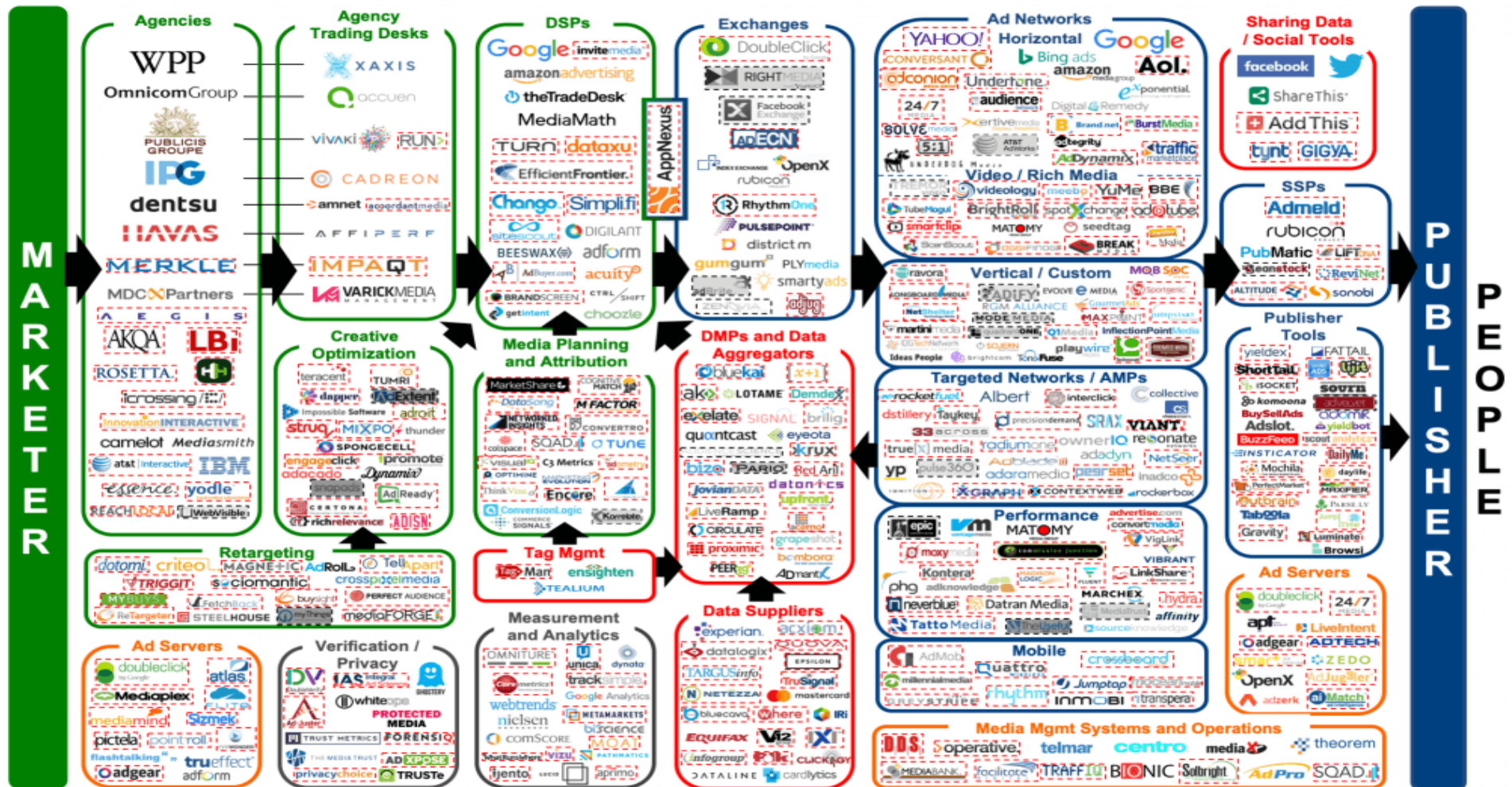
OBA uses information collected from marketing cookies and other sources to display ads or content more relevant to the website visitor.

Real-time Bidding (RTB) is a means by which advertising inventory is bought and sold on a per-impression basis, via programmatic instantaneous auctions, similar to financial markets.



AdTech Partners At A Glance

DISPLAY LUMAscape



Denotes acquired company

Denotes shuttered company

© LUMA Partners LLC 2020

Sources: <https://lumapartners.com/content/lumascapes/display-ad-tech-lumascapes/>

So what's the big deal?

- Cookies look fairly innocuous: UserID A9A3BECE0563982D www.goto.com/.
- For years, cookies were considered anonymous or non-personally identifiable information.
- Some advocates and policymakers became concerned about the potential for profiling.
- Cookie data is generally considered personal information or personal data, subject to privacy laws.
- In the European Union, cookie collection is subject to the ePrivacy Directive and the General Data Protection Regulation.
 - As a general rule, businesses must obtain specific, informed, opt-in consent to collect information via cookies or similar technologies.
- But the California Consumer Privacy Act has different requirements.
 - California residents have a right to opt out of “sales” of personal information, and businesses that sell personal information must include “Do Not Sell” links on websites and in apps.
 - Sales generally include “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . personal information . . . for money or other valuable consideration.”
- Many regulators are eager to exercise their authority in the area of digital advertising.

AdTech Industry Solutions

AdTech Industry Solutions for GDPR

CMP

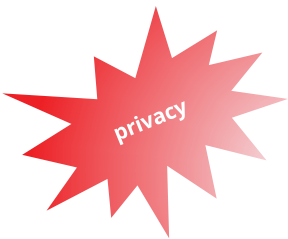
A consent management platform (CMP) is a tool that can support GDPR compliance for websites and apps. It prompts users for consent, collecting and managing that information, and passing the data to downstream ad partners.

CMPs can be implemented by:

- Integrating a third-party CMP solution
- Building a proprietary or “home grown” solution

FRAMEWORK

The Interactive Advertising Bureau (IAB) has developed a [Transparency & Consent Framework](#) for Europe and the CMPs registered with them.

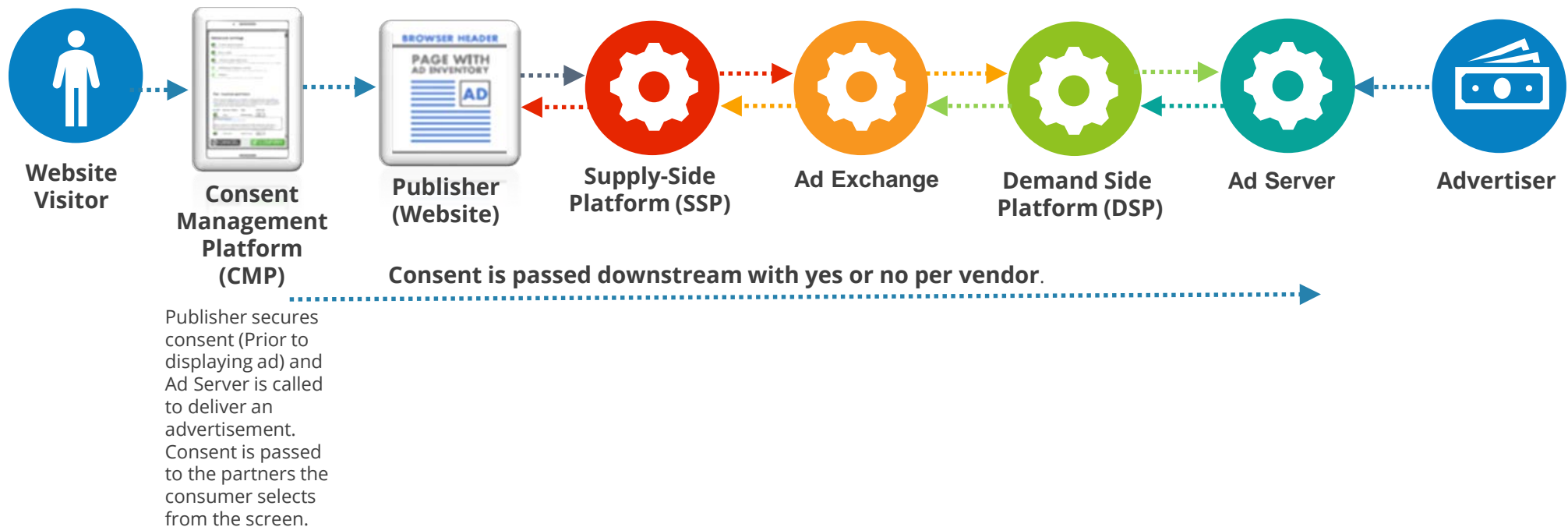


- Consent must be tracked when it serves as a legal basis for processing (GDPR).
- CMPs can support CCPA do not sell requests

AdTech Industry Solutions for GDPR

Interactive Advertising Bureau (IAB) Transparency & Consent Framework (TCF) Version 2 to meet GDPR

- Comprised of technical specifications and policy documents enabling companies that participate in the delivery of digital advertising and personalized content to work under an appropriate legal basis for processing personal data in each market where they operate.
- It is a framework for publishers, technology vendors, agencies and advertisers to clearly and consistently communicate with end users about how their data is being used, while also providing an opportunity for users to object.



Adtech Industry's Solutions for CCPA

Interactive Advertising Bureau (IAB) CCPA Compliance Framework

The IAB CCPA Framework requires participating publishers that **sell** the personal information of California consumers for digital advertising purposes to provide “explicit” notice regarding rights under the CCPA, to explain in clear terms what will happen to their data, and to notify the downstream technology companies with which the publishers do business that such disclosures were given.

Digital Advertising Alliance (DAA) Do-Not-Sell Tool

The DAA framework is designed to enable consumers to inform downstream recipients about sales opt outs. Consumers can exercise their CA Do Not Sell rights on publisher sites or at a single location.

Sources:

- <https://www.iab.com/guidelines/ccpa-framework/>
- <https://digitaladvertisingalliance.org/digital-advertising-alliance-do-not-sell-tool-publishers-and-third-parties>

Future of Cookies

What does the future hold?

1. More US state privacy laws will arise (i.e. CCPA 2.0)
2. Other jurisdictions around the world will adopt comprehensive frameworks
3. Third-party cookies will disappear
4. Publishers, brands, and advertising partners will seek new solutions
 - Enhanced contextual advertising
 - New tracking technologies will emerge
 - Publishers will seek to leverage first-party data
 - Increased reliance on AI
 - Increased use of logins
 - Cross-platform measurement tools
 - Potential for cross-sector collaboration

Recommendations and Best Practices for the Current World and What's to come

1. Take inventory of the cookies and tracking technologies you currently deploy
2. Assess applicability of privacy laws to those practices
3. Train relevant teams to treat cookie data as personal data and personal information
4. Be skeptical of the terms “anonymous” and “deidentified”
5. Consider whether to implement a CMP
6. Develop processes for complying with requests to access or delete cookie information
7. Consider adopting industry tools
8. Consider whether and how to deploy a Do Not Sell Button
9. Conduct due diligence of third party partners
10. Confirm that third parties are subject to appropriate contracts
11. Evaluate the use of 1st and 3rd party data by your organization
12. Prepare for the end of the 3rd party cookie

What's in the news

1

[TCF-Transparency & Consent Framework v2.0](#)

2

[Proposed California Privacy Regs Violate First Amendment, Ad Groups Claim](#)

3

[COVID-19 Warrants Delaying Enforcement Of California Privacy Law, Ad Groups Say](#)

Questions & Answers from Webinar

The following responses are intended for information purposes only. The responses are not to be considered as creating an attorney-client relationship with Hogan Lovells US LLP or indeed any contractual relationship or as rendering legal or professional advice for any specific matter.

1 - Q: Thanks - this is really helpful. My question is: Under CCPA compliance frameworks, does a "do not sell" request typically require the website publisher to request all third parties who previously obtained information about the consumer to delete it all and stop using it? And if so, how does a website publisher go about practicing that?

- **A:** Under the statute and the second set of revised draft regulations proposed by the California Attorney General, businesses are required to respond to do-not-sell requests only in a prospective manner. There currently is no requirement to look back to prior "sales."

2 - Q: Re: the comment as to whether the CA AG will consider cookies a "sale," does that also go for "pixels"?

- **A:** Cookies themselves do not constitute sales. However, cookies can be used to transfer personal information to third parties in ways that would constitute sales. The same is true for pixels or any other data collection technology. The key issue is the nature of the sharing, not the mechanism by which the information is shared.

3 - Q: What is the definition of "publisher" for the IAB CCPA compliance framework?

- **A:** Publishers are entities that own, control, or operate a digital properties.

4 - Q: If consent was given and later the individual realizes how broad the personal data use is with range of advertisers, can individual revoke, that is "opt-out" both under GDPR, Eprivacy ad CCPA?

- **A:** For websites covered by GDPR and the ePrivacy frameworks, users must be able to withdraw consent easily. The CCPA does not establish a straightforward opt-in regime for cookies. The right to opt out of sales is perpetual.

5 - Q: What will be the impact of the EU e-privacy regulation on the use of adtech?

- **A:** At this time, it is difficult to predict what the impact will be. The key stakeholders have not been able to reach agreement on the regulation, which was first introduced over three years ago.

Questions & Answers from Webinar

The following responses are intended for information purposes only. The responses are not to be considered as creating an attorney-client relationship with Hogan Lovells US LLP or indeed any contractual relationship or as rendering legal or professional advice for any specific matter.

6 - Q: If legitimate interest does not serve the RTB ecosystem and consent remains; how is the publisher then to ask for "well-informed" consent if the publisher at the moment of asking consent has no way of knowing what parties (hooked up to the ecosystem) will receive/process the personal data of the visitor? Is that information (what parties will receive the personal data) not essential for consent?

- **A:** The UK Information Commissioner's office notes in its June 2019 report on real-time bidding that publishers may need only specify the categories of recipients in association with obtaining consent for the publisher's processing and sharing of personal data. However, if the publisher is obtaining consent for the third-party activities (e.g., profiling), the ICO notes that the GDPR may require that the recipients be named. The ICO acknowledges that this is challenging.

7 - Q: What about 3rd party analytics tool that are used in products (access restricted by ID& PW) and lay cookies ? If we have signed an agreement with a customer (subscription to the Product) that states that we will use analytics tools to improve the product, do we still need consent from each individual users before we lay those specific analytics cookies ? Or are we covered by the agreement ?

- **A:** Under the EU framework for cookies, user consent is required for the use of all cookies except those that are strictly necessary. The terms between publishers and analytics providers do not satisfy the consent requirement.

8 - Q: Following on from the Legitimate Interest question, does James take the view that the ePrivacy rules apply outside the EU? If not, it appears that consent may not be required for cookies.

- **A:** Although the ePrivacy Directive may not have extraterritorial scope, the GDPR does. Businesses subject to GDPR must consider what the lawful basis for processing personal data will be, whether using cookies or other technologies.

Questions & Answers from Webinar

The following responses are intended for information purposes only. The responses are not to be considered as creating an attorney-client relationship with Hogan Lovells US LLP or indeed any contractual relationship or as rendering legal or professional advice for any specific matter.

9 – Q: What's your take on Google Analytics - can a high-traffic website be subjected to CCPA rules?

- **A:** The amount of traffic is not dispositive. The key questions to ask are whether the website is operated by a for-profit entity that does business in California, whether personal information is collected, and whether the entity meets the requirements for jurisdiction under the CCPA.

10 – Q: Can James' elaborate on how he thinks "other valuable consideration" is tied to general contractual commitments? Wouldn't the recipient party's use for their own purposes also somehow need to be a benefit to the business?

- **A:** The CCPA does not define "consideration." In the absence of a statutory definition, courts may look to contract case law, which suggests that promises to act or refrain from acting (e.g., data use limitations or permissions) may constitute consideration

THANK YOU – QUESTIONS?



Heather Dunning

Senior Director
Ankura

heather.dunning@ankura.com



W. James Denvil

Senior Associate
Hogan Lovells

w.james.denvil@hoganlovells.com



Darin Bielby

Senior Managing Director
Ankura

darin.bielby@ankura.com

UPCOMING WEBINARS

May 2020: Reasonable Security: Best Practices and Breach Preparedness

PRIVACY

- Readiness Assessments
- Data Mapping
- Consumer Rights
- De-Identification Experts
- Data Governance and Minimization
- Litigation Support
- Staff Augmentation

CYBERSECURITY

- Cybersecurity Assessments
- Penetration Testing
- Breach Preparedness
- Threat Hunting
- Incident Response
- CISO-as-a-Service
- Data Mining and Analytics
- Litigation Support

The material in this presentation has been prepared by Ankura Consulting Group, LLC (“Ankura”) and is general background information about the matters described herein to be used for informational purposes only. This information is given in summary form and does not purport to be complete. This information should not be considered legal or financial advice. You should consult with an attorney or other professional to determine what may be best for your individual needs.

Information in this presentation should not be considered as advice or a recommendation to investors or potential investors in relation to holding, purchasing or selling securities or other financial products or instruments and does not take into account your particular investment objectives, financial situation or needs. No one should make any investment decision without first consulting his or her own financial advisor and conducting his or her own research and due diligence.

Ankura does not make any guarantee or other promise as to any results that may be obtained from using the information in this presentation. Ankura shall have no liability to the recipient of this presentation or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of any data or calculations contained and/or referred to in this presentation nor for any special, direct, indirect, incidental or consequential loss or damage that may be sustained because of the use of the information contained and/or referred to in this presentation or otherwise arising in connection with the information contained and/or referred to in this presentation, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to Ankura that may not be excluded or restricted.

IRS Circular 230 Disclosure: Ankura and its affiliates do not provide tax or legal advice. Any discussion of tax matters in these materials (i) is not intended or written to be used, and cannot be used or relied upon, by you for the purpose of avoiding any tax penalties and (ii) may have been written in connection with the “promotion or marketing” of a transaction (if relevant) contemplated in these materials. Accordingly, you should seek advice based your particular circumstances from an independent tax advisor.

This presentation contains data compilations, writings and information that are confidential and proprietary to Ankura and protected under copyright and other intellectual property laws, and may not be reproduced, distributed or otherwise transmitted by you to any other person for any purpose unless Ankura’s prior written consent have been obtained.