



UNTANGLING THE ISSUES IN COMMERCE MEDIA NETWORKS

Key Considerations Under
U.S. State Privacy Laws

June 2025

Sponsored by



TABLE OF CONTENTS

I. OVERVIEW	3
A. Different Roles in Commerce Media Networks	3
B. Different Forms of Commerce Media Networks	4
1. Different CMN Outlet Channels	4
2. Advertiser Types in CMNs	4
3. Summary of Common CMN Setups and Examples	5
C. Data Sources of CMNs	5
II. TYPICAL CMN DATA FLOWS	6
A. CMN Onsite Activation and Measurement Flow – Contextual	7
B. CMN Onsite Activation and Measurement Flow – Personal Information Based	8
C. CMN Offsite Activation Flow	9
D. CMN Offsite Measurement Data Flow	10
III. PARTY RELATIONSHIPS FOR ONSITE ACTIVATION AND MEASUREMENT DATA FLOWS	11
A. Relationship between CMNs and Ad Tech Vendors	12
B. Relationship between CMNs and Brands	12
C. Summary of Relationships Based on Data Flows and Functional Roles	13
IV. PARTY RELATIONSHIPS FOR OFFSITE ACTIVATION AND MEASUREMENT DATA FLOWS	15
A. Off-site Activation Analysis	15
B. Offsite Measurement Analysis	15
1. Can a measurement vendor be engaged, jointly or by each party, as a service provider/processor or the measurement purpose?	15
2. How to construe a “sale” relationship among parties who contribute personal information to the measurement vendor to compile the measurement report?	16
V. THE ISSUES OF EMBEDDED ONLINE TRACKING TOOLS IN AD CREATIVES	17
VI. OTHER PRIVACY CONSIDERATIONS	19
VII. CONCLUSION	19
APPENDIX A: DIGITAL ADVERTISING GLOSSARY	20

Commerce Media Networks (CMNs) represent a rapidly growing business model in digital advertising, built around the strategic use of first-party data to drive targeted and measurable campaigns. These networks are operated by retailers, hotels, airlines, ride-share companies, and other consumer-facing businesses that collect substantial volumes of personal and transactional data as part of their interactions directly with consumers. As the digital advertising landscape continues to evolve, CMNs are serving as additional channels for targeting and attribution.

This whitepaper explores the various types of CMNs, maps out the data flows and technological components underpinning each model, clarifies the roles and responsibilities of involved parties under the U.S. state privacy laws, and outlines key privacy legal considerations for building and operating CMNs.

I. OVERVIEW

A. DIFFERENT ROLES IN COMMERCE MEDIA NETWORKS

For this whitepaper, below are the different players in commerce media networks.

- **Consumer-Facing Business:** collects customer data from its websites, apps, and in-store POS systems. It has a direct relationship with consumers and collects first-party data from them. Examples of these businesses include hotels, airlines, travel companies, retailers, and e-commerce platforms.
- **Commerce Media Network:** serves as a division within a Consumer-Facing Business that brings together data, technology, and media to leverage first-party data and enable advertising solutions.
- **Brand (Advertiser):** leverages CMNs' first-party data to reach prospective customers. The Consumer-Facing Business may or may not carry or otherwise offer these Brand's products for sale directly to consumers.
- **Ad Tech Provider:** provides the tools and infrastructure that power CMNs, including demand-side platforms (DSPs), sell-side platforms (SSPs), Data Clean Rooms (DCRs), identity resolution services, and measurement solutions.
- **Publisher:** owns and operates digital platforms or properties, such as websites, apps, or digital content channels, where ads can be displayed. Publishers provide the space (also called ad inventory) for Advertisers to reach audiences through various formats like display ads, video ads, native content, or sponsored articles. Publishers can be independent entities such as news sites, social media, or blogs. When CMNs display ads on their e-commerce properties, they also assume the Publisher's role.

Together, these entities comprise a complex and interdependent ecosystem. In the sections below, we will examine how these components form the different types of CMNs.

B. DIFFERENT FORMS OF COMMERCE MEDIA NETWORKS

CMNs can take multiple forms, depending on several key factors, such as whether the Consumer-Facing Business owns the media outlet, whether the channel is digital or physical, and whether the Consumer-Facing Business carries the advertised product or service.

1. Different CMN Outlet Channels

CMN outlet channels can be categorized by whether CMN owns them and whether they are digital or physical.

Owned Channels refer to advertising spaces directly controlled by Consumer-Facing Businesses. These include both digital and physical environments. **Digital Owned Channels** encompass advertisements delivered through the business' own digital properties, such as its e-commerce website, mobile applications, marketing emails, or digital loyalty platforms. These channels allow for precise targeting using first-party data and provide closed-loop measurement capabilities that tie ad exposure directly to transaction data. **Physical Owned Channels** involve advertisements displayed on digital media within the Consumer-Facing Business's platform's physical footprint. Examples include in-store kiosks, digital signage, in-store audio systems, gas station pump screens owned by the retailer, in-flight entertainment screens, or hotel room televisions. While some of these physical touchpoints are directly owned by the Consumer-Facing Businesses, others may be provided through partnerships with external vendors.

Offsite Channels, by contrast, involve placements on external platforms that are not owned by the CMNs but are leveraged to extend the reach of commerce media campaigns. These are typically digital in nature and include advertisements served on Publishers' websites and apps, such as social media, streaming TV websites, news websites, or digital out-of-home (DOOH) displays. Offsite channels may include paid social media placements, programmatic display ads, or native content integrations, allowing brands to connect with consumers beyond the Consumer-Facing Business's own ecosystem while still using the Consumer-Facing Business's first-party data for targeting and attribution.

See illustrative examples of the outlet channels described in Section (I)(B)3 below.

2. Advertiser Types in CMNs

Advertisers in CMNs can generally be categorized into two primary types: endemic and non-endemic. This classification is based on the nature of the relationship between the Advertiser and the CMN, particularly whether the advertised brand is sold through, or has a commercial relationship with, the Consumer-Facing Business.

Endemic Advertisers are typically Brands whose products and services are sold by the Consumer-Facing Businesses. **Non-endemic Advertisers**, by contrast, do not have a product or vendor relationship with the Consumer-Facing Businesses. These Advertisers may operate in entirely different verticals—such as financial services, entertainment, insurance, or automotive—and use CMNs to reach prospective customers. For instance, a Consumer who bought a high-end washer

and dryer set at a retailer may be the right audience for a high-end car ad, even though the retailer does not sell cars. In this case, while the product is not available for purchase through the retailer, non-endemic advertising leverages the retailer's first-party data and customer engagement infrastructure to target relevant audiences.

It is important to note that the definition and structure of a CMN may vary across organizations, as each company tailors its approach based on its unique business model, assets, and strategic objectives.

3. Summary of Common CMN Setups and Examples

	OWNED DIGITAL	OWNED PHYSICAL	OFFSITE
ENDEMIC	Consumers browse digital sites owned by the Consumer-Facing Business and see ads for products/services of a certain Brand carried by the business (e.g., "sponsored product") in exchange for payment by the Brand.	Consumers encounter the digital interface located on the Consumer-Facing Business's physical property (e.g., gas station screen owned by the retailer, in-flight digital screen, or hotel room TV screen), and on which products/services of a certain Brand carried by the Consumer-Facing Business are advertised (e.g., "sponsored product") in exchange for payment by Brand.	Consumers browse a third-party news media site and see targeted advertising for the products/services a certain Brand carried by the Consumer-Facing Business. The Brand pays for the campaign, which leverages data supplied by the Consumer-Facing Business.
NON-ENDEMIC	Consumers browse digital sites owned by the Consumer-Facing Business and they see advertisements of products/services of a certain Brand <u>not</u> carried by the Consumer-Facing Business (e.g., moving service offerings displayed when a Consumer is browsing home improvement products).	Consumers encounter the digital interface located on the Consumer-Facing Business's physical property (e.g., gas station screen owned by the retailer, in-flight digital screen, hotel room TV screen) and see products/services of a certain Brand <u>not</u> carried by the business are prioritized in placement.	Consumers browse a third-party news media site and see targeted advertising for the products/services of a certain Brand <u>not</u> carried by the Consumer-Facing Business. The Brand pays for the campaign, which leverages data supplied by the Consumer-Facing Business (e.g., targeted ads for luxury cars to customers who bought high-end purses at the retailer).

C. DATA SOURCES OF CMNs

The efficacy of CMNs is underpinned by a robust and multifaceted data infrastructure. At the core of this ecosystem lies first-party customer data, which is collected directly through consumer interactions with the Consumer-Facing Business. This includes data obtained through loyalty program registrations, personal information provided during purchases (e.g., for e-receipts, delivery, or pickup), and behavioral insights captured via online advertising technologies such as cookies, pixels, tags, and software development kits (SDKs).

In addition to customer data, CMNs may also leverage transactional and engagement data, including point-of-sale (POS) activities (e.g., items purchased), online checkout behavior, and fulfillment details. It also includes digital data about how consumers interacted with the advertised products, capturing impressions, clicks, and engagement across media channels.

CMNs also augment their first-party data with third-party data sources. These may include licensed data points to enhance the consumer profile (e.g., consumer preferences and inferences). It may also include data from integrated data products, such as connected devices, wearable technologies, mobile applications, browser plug-ins, and Publisher partnerships. Brands may also provide third-party data such as data pertaining to consumer interactions with the Brand site that are not mediated by the Consumer-Facing Business.

The CMNs also leverage non-personal information, such as the store location and product SKU number.

The data sources described are by no means comprehensive or exhaustive. When leveraged responsibly, these diverse data inputs enable CMNs to tailor their promotion messages to consumers while facilitating measurement, attribution, and optimization at scale. However, legal and compliance considerations around the collection, use, and sharing of personal information remain critical, particularly in light of evolving privacy regulations and consumer expectations.

II. TYPICAL CMN DATA FLOWS

IAB develops a representative set of data flows that reflect the current industry practices across the CMN ecosystem in collaboration with the IAB Commerce Media Network Working Group, which is composed of leading retail and commerce media networks operating in the United States.

Specifically, the group detailed how advertisements are activated through either contextual signals or personal information on CMN-owned outlet channels. In addition, it mapped the data flows supporting off-site ad activation, where audience targeting takes place across third-party Publisher environments using first-party and/or third-party data. For both on-site and off-site scenarios, the group also identified the corresponding “feedback loop”—the personal information flow that enables ad measurement and attribution—illustrating how campaign effectiveness is assessed throughout the commerce media lifecycle.

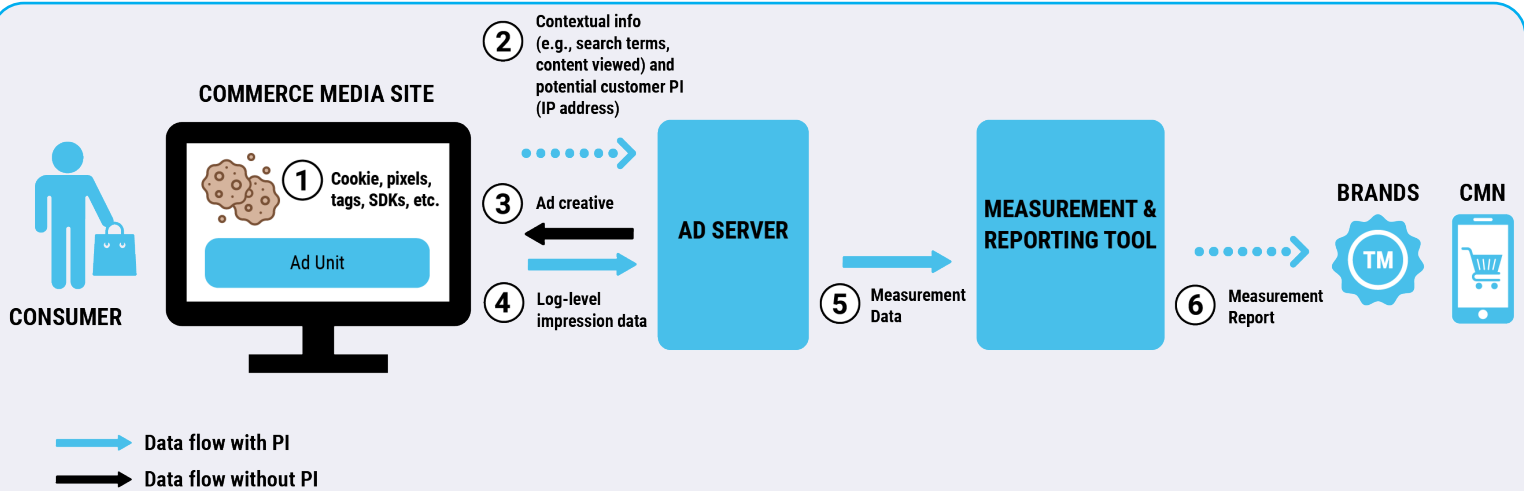
These data flow diagrams reflect prevailing business practices and are intended to serve as a common reference point for industry participants. However, implementation may vary across organizations depending on business models, technology stacks, and data governance frameworks.

In addition, each functional component within the data flow represents a distinct operational role, but in practice, vendors and platforms may assume multiple roles within the same ecosystem, or some of these functional components may be built and owned by the CMN. As such, the diagrams are not prescriptive architectures, but rather illustrative tools designed to facilitate shared understanding and informed privacy legal analysis.

Below are several representative CMN data flows. For a more detailed description of each functional component, please refer to the Digital Advertising Glossary in **Appendix A**.

A. CMN ONSITE ACTIVATION AND MEASUREMENT FLOW - CONTEXTUAL

This data flow outlines the onsite activation process for a CMN using contextual advertising and its measurement feedback loop.



Data Flow Description

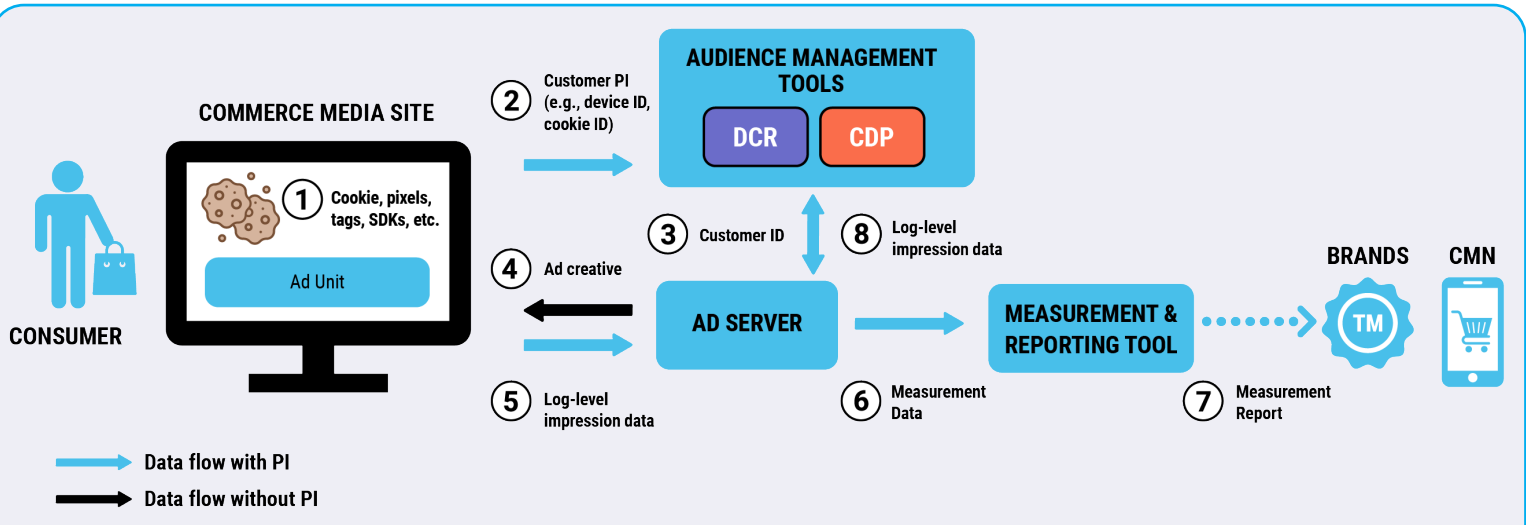
1. Consumer visits a CMN site, triggering the ad serving script to orchestrate the ad placement process. Consumer's data can be collected and transmitted through cookies, pixels, SDKs or server-to-server calls.
2. The ad serving script sends contextual information about the consumer's interaction with the website to the ad server. Although contextual ads do not necessarily need personal information to deliver ads, depending on the setup, personal information is likely to be exposed and passed to the ad server for brand safety and ad validation purposes. In addition, depending on how "contextual" is defined, it could include personal information (e.g., location data).
3. Ad server returns the ad creative.¹ The ad creative embeds measurement pixels to record impressions. The ad server can be an internal system built by the CMN or hosted by a third party (e.g., Criteo, Google Ad Manager, Koddi). In practice, the onsite activation can also be programmatic which involves DSPs and SSPs. As such, measurement pixels can be embedded in the ad creative by different parties (e.g., DSP) and may send log-level measurement data to the other Ad Tech Provider to which the pixels belong. For clarity, the illustration simplified the data flow.
4. Measurement pixel embedded in the ad creative sends log-level measurement data to ad server.
5. Ad server sends measurement data to a measurement and reporting tool to compile measurement reports.²
6. CMN shares the measurement report with the Brand. While most CMNs share aggregated reports without personal information, the report can contain individual record-level data with personal information. Measurement vendors often share log-level measurement reports with CMNs.

¹ What is the desired audience may be determined by the ad server or by other ad tech provider in the bidding process. In practice, third party ad servers will generally serve an impression whenever they receive an ad request to avoid serving blanks.

² Several ad tech tools may be involved in sending the measurement data and compiling the measurement report. These ad tech tools may have overlapping capabilities.

B. CMN ONSITE ACTIVATION AND MEASUREMENT FLOW – PERSONAL INFORMATION BASED

This data flow outlines the onsite activation process for a CMN using personal information and its measurement feedback loop.



Data Flow Description

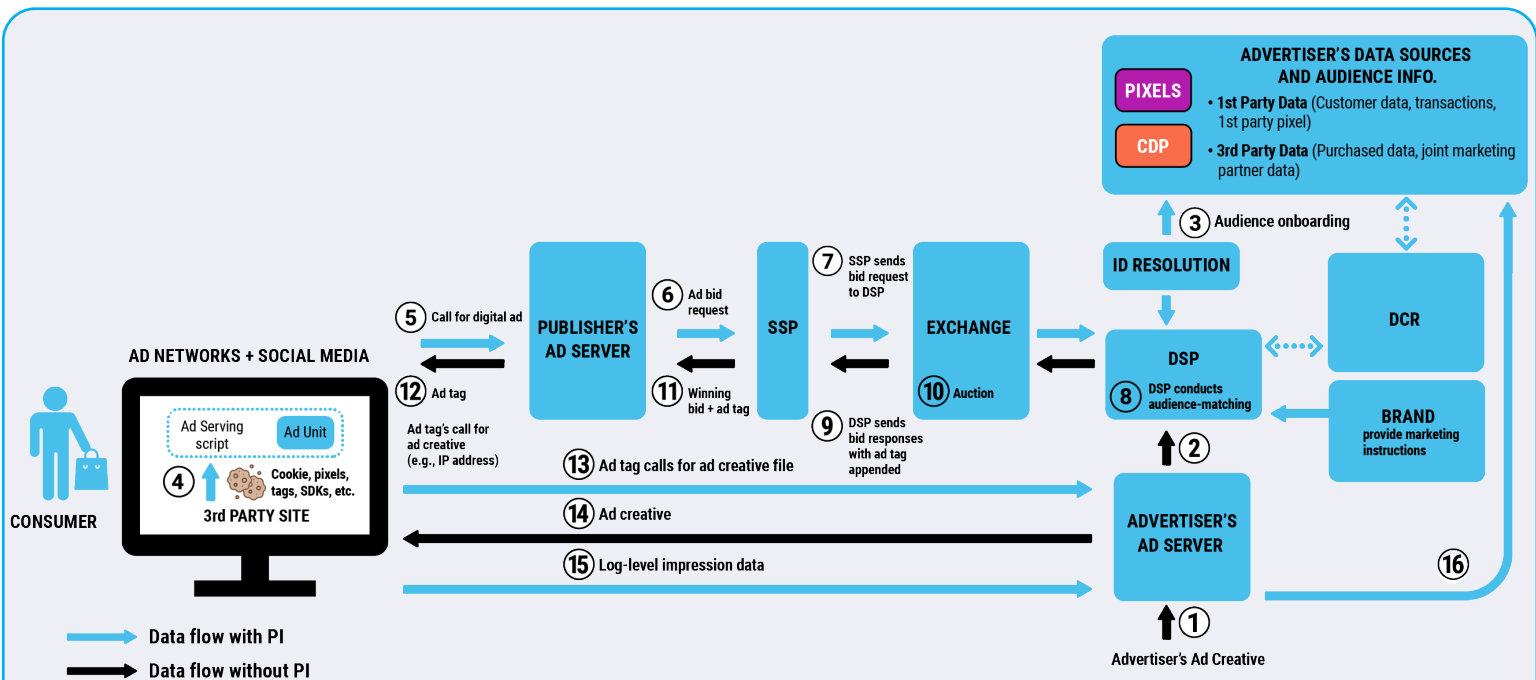
- Consumer visits a CMN site, triggering the ad serving script to orchestrate the ad placement process. Consumer's data can be collected and transmitted through cookies, pixels, SDKs or server-to-server calls.
- The ad serving script sends customer personal information to audience management tool(s), including Customer Data Platform (CDP), DCR, etc. The audience management tool stitches IDs, potentially augments the first-party data with third-party data, and determines whether the customer is within the targeted segmentation. Some CMNs may also use an identity resolution vendor to stitch IDs instead of using an internal tool.
- If the audience management tool determines the site visitor is a targeted audience, it sends the customer ID to the ad server.
- Ad server sends the ad creative, and the ad serving script displays the ad to the customer.³
- Measurement pixel embedded in the ad creative sends log-level measurement data to ad server.
- Ad server sends measurement data to a measurement and report tool to compile measurement reports.⁴
- CMN shares the measurement report with the Brand. The prevailing practice is that the CMN shares aggregated reports without personal information. However, the report can contain individual record-level data with personal information. Measurement vendors often share log-level measurement reports with CMNs.
- Ad server may also return log-level measurement data to CMNs and store it in its CDP.

³ The onsite activation can also be programmatic, which involves demand-side platforms and sell-side platforms. As such, measurement pixels can be embedded in the ad creative by different parties (e.g., DSP) and may send log-level measurement data to the other ad tech vendors to which the pixels belong. For simplicity, the illustration simplified the data flow.

⁴ See footnote 2.

C. CMN OFFSITE ACTIVATION FLOW

This data flow outlines the offsite activation process for a CMN using personal information, and its measurement feedback loop.



Data Flow Description

1. Brand (or its ad agency) uploads ad creative to the Advertiser's Ad Server.
2. Advertiser's Ad Server sends an ad tag that represents the ad creative to DSP.
3. Advertiser onboards its audience to DSP through an ID resolution provider⁵ or DCR.
4. A Consumer visits a Publisher's site, and the site's ad-serving scripts read the Consumer's cookie (or use other identity information, like login) to identify the user. Consumer's data can be collected and transmitted through cookies, pixels, SDKs, or server-to-server calls.
5. Ad serving script calls the Publisher's Ad Server to call for a digital ad.
6. Publisher's Ad Server initiates ad bid requests to SSP.
7. SSP sends the bid request to the DSP.
8. DSP conducts audience matching.
9. DSP sends bid responses with ad tag appended.
10. Multiple SSPs and DSPs participate in auctions on the bid request on an Ad Exchange.
11. The winning SSP sends the winning bid and ad tag to the Publisher's Ad Server.
12. Publisher's Ad Server sends the ad tag to the ad serving script.
13. Ad serving script makes a call to the Advertiser's Ad Server.
14. Advertiser's Ad Server returns the ad creative, and the ad is presented on the third-party Publisher's site.
15. Measurement pixel embedded in ad creative sends log-level measurement data to the ad server.⁶
16. Ad server may also return log-level measurement data to CMNs and store it in its CDP.⁷

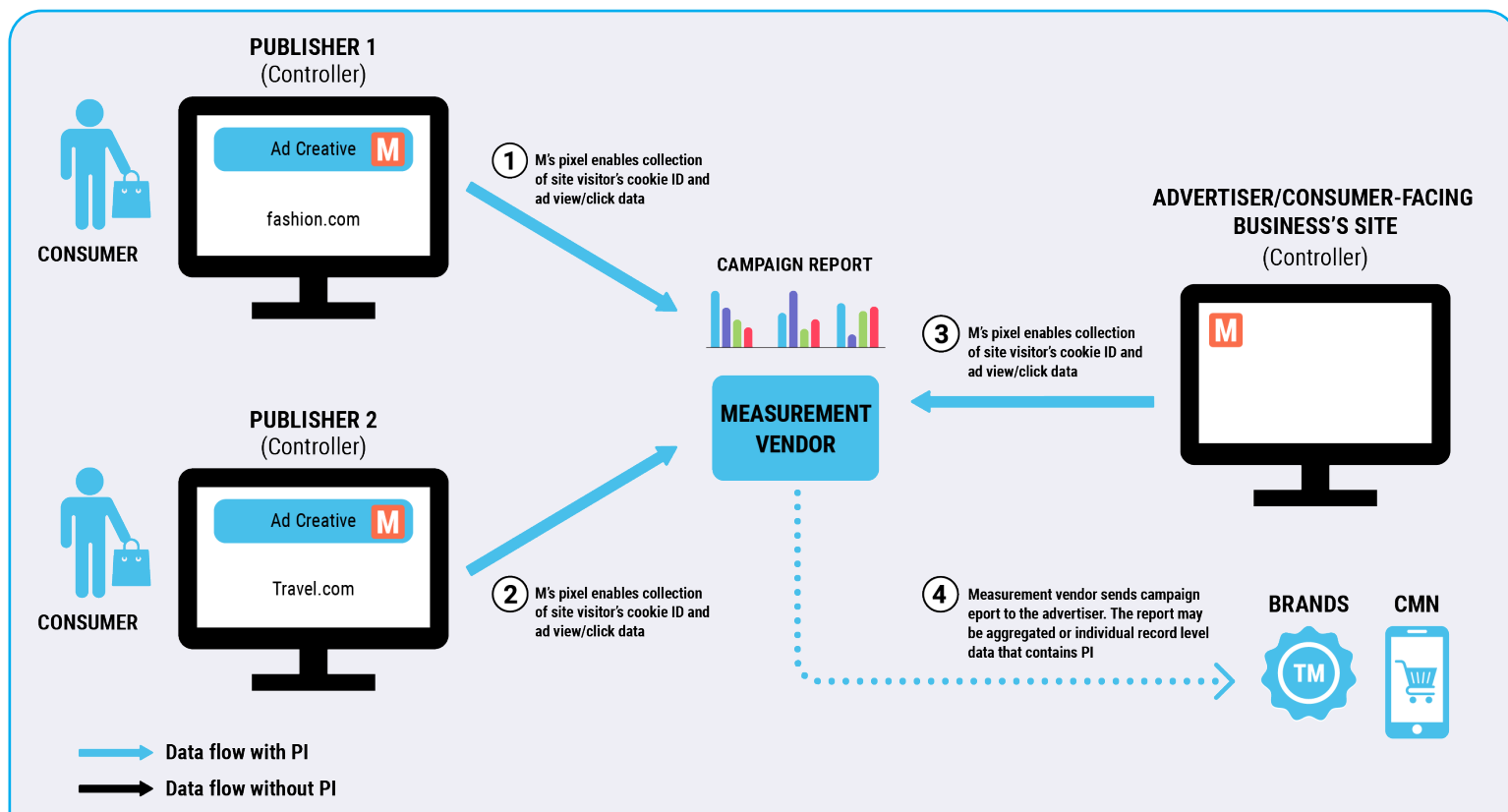
⁵ ID resolution vendors can work with many functional components, including SSP, publisher, etc. across the digital advertising system. ID resolution can also be an internal function within the Advertiser's CDP.

⁶ See footnote 3

⁷ See footnote 2.

D. CMN OFFSITE MEASUREMENT DATA FLOW

This data flow offers another view of the off-site measurement process for a CMN using personal information.



Data Flow Description

1. When a Consumer visits Publisher 1's digital property, the measurement pixel embedded in the ad creative sends log-level measurement data that may contain personal information to the measurement vendor.
2. A similar data flow is triggered when the same Consumer visits Publisher 2's digital property.
3. When the same Consumer visits the Brand's or the Consumer-Facing Business's site that sells the advertised product, the measurement pixel on that site sends the Consumer's log-level measurement data that may contain personal information to the measurement vendor.
4. The measurement company generates and shares the measurement report with the Brand and/or the CMN. While most CMNs share aggregated reports without personal information, the report can contain individual record-level data that may contain personal information.

Each digital advertising data flow within the CMNs described above—whether for onsite or offsite activation—may involve multiple vendors fulfilling the same functional role. For example, several SSPs may simultaneously participate in inventory auctions, and multiple DSPs may bid on the same CMN ad placement.

III. PARTY RELATIONSHIPS FOR ONSITE ACTIVATION AND MEASUREMENT DATA FLOWS

This section examines whether, for each CMN use case outlined in Section II, personal information is “sold”⁸ and how the “sale” relationship should be construed. It also evaluates whether CMNs can engage various participants in the digital advertising ecosystem as service providers/processors or third parties under applicable U.S. state privacy laws.

U.S. state privacy laws broadly define the “sale” of personal information to include disclosures to *third parties* in exchange for *monetary or other valuable consideration*.⁹ However, disclosures to processors¹⁰ or service providers¹¹—who handle data on behalf of a business or controller—are generally exempt, provided they operate under the controller’s instructions and are bound by specific contractual obligations.

California imposes stricter rules when operating as a service provider under the California Consumer Privacy Act (CCPA). Service providers must process personal information solely for defined “business purposes,” such as auditing, security, account servicing, and certain marketing or analytics activities. These purposes explicitly exclude cross-context behavioral advertising, or sharing data with third parties therefor.¹² As such, the CCPA prohibits service providers from engaging in cross-context behavioral advertising.¹³ The CCPA further prohibits service providers from combining personal information received from different businesses unless it does so in accordance with regulations promulgated by the California Privacy Protection Agency (CPPA).¹⁴

To determine whether a disclosure of personal information is a “sale” or a disclosure to a service provider under U.S. state privacy laws, one should conduct thorough due diligence and ask the following detailed questions:

- Is the recipient acting independently or on behalf of the CMN?
- Is there a written contract with legally required restrictions on personal information use?
In other words, is the recipient prohibited from retaining, using, or disclosing the data beyond the service scope?

⁸ See, e.g., Cal. Civ. Code § 1798.140(ad), Conn. Gen. Stat. § 42-515(26), and Colo. Rev. Stat. 6-1-1303(23).

⁹ See, e.g., Colo. Rev. Stat. 6-1-1303(23) (emphasis added).

¹⁰ See, e.g., Conn. Gen. Stat. § 42-515(21), Colo. Rev. Stat. 6-1-1303(19).

¹¹ Cal. Civ. Code § 1798.140(ag).

¹² See Cal. Civ. Code § 1798.140(e).

¹³ Cal. Civ. Code § 1798.140(k) (defining “cross-context behavioral advertising” as “the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-Branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts”), and Cal. Code. Regs. tit. 11 § 7050(b) (prohibiting a service provider from engaging in cross-context behavioral advertising).

¹⁴ See Cal. Civ. Code § 1798.140(e), Cal. Civ. Code § 1798.140(ag)(1)(d), and Cal. Code. Regs. tit. 11 § 7050(b).

- Does the recipient use the data solely as directed, or for its own purposes (e.g., combining with other personal information except as permitted by the regulations, or conducting further cross-context behavioral advertising or targeted advertising)?
- Is the relationship accurately disclosed in the Consumer-Facing Business's privacy policy?

Because companies in the digital advertising ecosystem often provide multiple services and play various roles, the following analysis focuses on individual data flows and functional components. While CMNs may sometimes build certain capabilities in-house (e.g., identity resolution or DSP functionality), we assume, for this whitepaper, that other entities provide these services.

The following analysis is strictly based on the data flows described above. If the data flow changes in any way, or if any party uses personal information for purposes not outlined here, a separate and updated legal analysis will be necessary.

A. RELATIONSHIP BETWEEN CMNS AND AD TECH PROVIDERS

The prevailing legal construct in the market is for CMNs to establish a service provider/processor relationship with the Ad Tech Providers for closed-loop onsite activation and measurement data flows. This is primarily because in the onsite activation flows, the Ad Tech Providers act on behalf of the CMN to perform services—such as serving ads on the CMN's properties, measuring campaign performance, and generating analytics. These services fit within the CCPA's defined business purposes, including 1798.140(e)(1) (ad auditing), (5) (analytics service), and (6) (advertising and marketing). To establish the service provider/processor relationship, CMNs also bound the Ad Tech Providers with written contracts that include required service provider/processor terms. Therefore, these disclosures fall within the statutory exemption from becoming a "sale" if parties establish a service provider/processor relationship and the Ad Tech Providers do not combine the data across clients for cross-context behavioral advertising.

B. RELATIONSHIP BETWEEN CMNS AND BRANDS

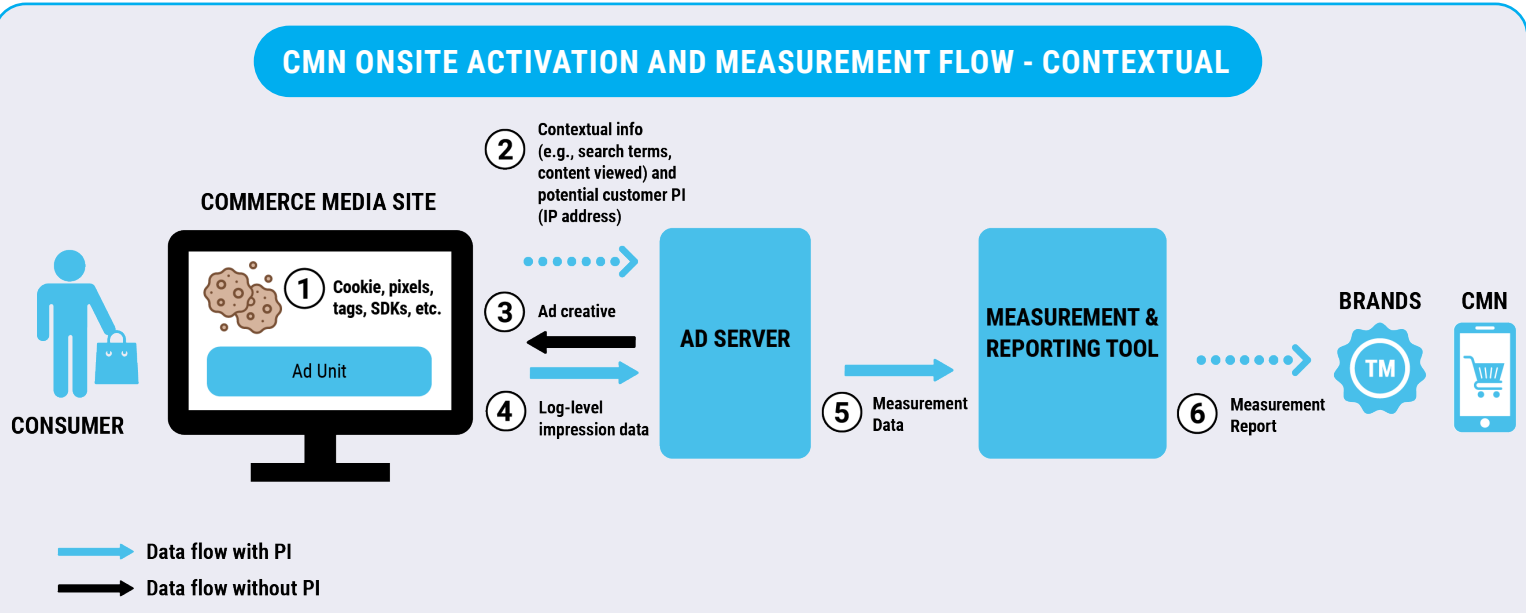
As outlined in each data flow above, CMNs typically do not disclose personal information to Brand for onsite and off-site activation and measurement purposes. Therefore, the prevailing legal construct is that CMNs do not "sell" personal information to Brand because there is no disclosure of personal information. Instead, CMNs allow Brands to target users based on their characteristics (e.g., interests, behavior, demographics), and Brands do not get access to personal information.

There are certain use cases where a CMN may provide Brands with measurement reports containing personal information. In these use cases, CMNs "sell" personal information to Brands unless they establish a service provider/processor relationship with the Brand. We understand that the prevailing practice is to exclude opted-out personal information when generating these reports.

For activation purposes, Brands may also share their own audience lists and request targeted activation based on that list. In such scenarios, Brands "sell" personal information to CMNs, and if a consumer opted out from "sale" from the Brand, such consumer's personal information should be excluded from disclosure.

C. SUMMARY OF RELATIONSHIPS BASED ON DATA FLOWS AND FUNCTIONAL ROLES

To summarize, below is the prevailing legal construct for CMN onsite activation and measurement, both based on contextual and personal information-based advertising.¹⁵



Prevailing Practices

The explanation applies to the functional roles served by each entity. In practice, legal agreements may reflect a party serving as a “processor” in certain capacities, while serving as a “third party” in others.

Step 2. CMN delivers contextual information to the ad server.

- If no personal information is exposed to the ad server, there is no need to contemplate a data protection agreement, and state privacy laws do not apply.
- If personal information (e.g., IP address) is shared, the ad server can be engaged as a processor, otherwise it constitutes a “sale” under state privacy laws.

Steps 4 & 5. CMN shares log-level impression data with the ad server and, subsequently, with the measurement vendor.

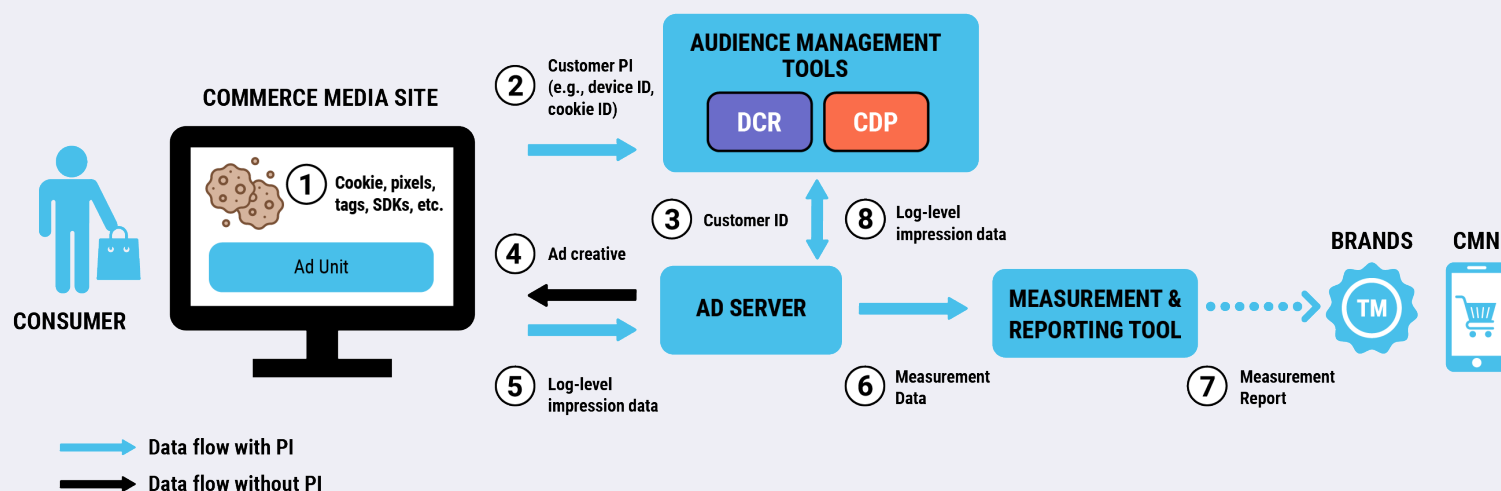
- Ad server and measurement vendors can be engaged as service providers/processors with legally required data protection contract terms, otherwise it constitutes a “sale” under state privacy laws.

Step 6. CMN shares the measurement report with the Brand.

- If the measurement report is aggregated and deidentified, there is no disclosure of personal information and state privacy laws do not apply.
- If the measurement report contains personal information, a “sale” is construed between the CMN and Brand. Unless the CMN and Brand form a processor relationship, opted out personal information should be excluded from measurement. We understand that, in cases where personal information is provided to the Brand, the prevailing practice is to construe a sale relationship and remove opted out data from being shared.

¹⁵ In practice, a more advanced CMN setup can be programmatic, allowing a Brand to bid across multiple CMN outlet channels based on specific audience cohorts. For purpose of this whitepaper, we focus on the foundational set ups of the CMNs. Additionally, Brand Advertisers can contribute their own audience lists to target overlapping segments or identify look-alike audiences for broader reach and increased relevance. If such measurement report contains personal information, a “sale” of personal information should be construed from the CMN to the Brand unless there is an established service provider/processor relationship.

CMN ONSITE ACTIVATION AND MEASUREMENT FLOW – PERSONAL INFORMATION BASED



Prevailing Practices

The explanation applies to the *functional roles* served by each entity. In practice, a legal agreement may reflect a party serving as a “processor” in certain capacities, while serving as a “third party” in others.

Step 2. CMN delivers personal information to various audience management tools.

- Audience management vendors (CDPs) are typically subject to contractual terms with service provider/processor restrictions. Some businesses have their own internally built CDPs.
- Note that if the Brand contributes personal information to the audience, often through DCR audience matching or look-alike modeling, the Brand may sell personal information to the CMN.

Step 3. CMN sends personal information (e.g., customer ID) to the ad server

- Ad server is typically engaged as a service provider/processor with legally required data protection contract terms. Otherwise, a “sale” results under state privacy laws.

Steps 5-6 and 8. CMN shares log-level impression data with the ad server and, subsequently, with the measurement vendor. Ad server sends the log-level impression data back to CMN’s CDP.

- Ad server and measurement vendors can be engaged as service providers/processors with legally required service provider/processor contract terms.

Step 7. CMN shares the measurement report with the Brand.

- If the measurement report is aggregated and deidentified, there is no disclosure of personal information.
- If the measurement report contains record-level personal information, a “sale” results between the CMN and the Brand. Unless the CMN and Brand form a processor relationship, opted out personal information should be excluded from measurement. We understand the prevailing practice, to the extent personal information is included in such a report to the Brand, is to construe a sale and suppress opted out data.

IV. PARTY RELATIONSHIPS FOR OFFSITE ACTIVATION AND MEASUREMENT DATA FLOWS

A. OFFSITE ACTIVATION ANALYSIS

CMNs typically disclose user-level personal information—such as device IDs, IP addresses, and browsing behavior—to DSPs. This data is sometimes enhanced through identity resolution vendors using DCRs¹⁶ for off-site activation.

DSPs typically use personal information for additional commercial purposes (e.g., adding personal information to their identity graph). In addition, the CCPA specifically excludes cross-context behavioral advertising from the definition of “Business Purpose” and prohibits engaging service providers for cross-context behavioral advertising.¹⁷ In other words, a DSP’s use of data usually goes beyond the limited scope allowed under service provider exceptions. As a result, these arrangements often meet the legal definition of “sale” or “sharing,” and CMNs and DSPs often establish a third-party relationship whereby CMNs sell/share personal information to Ad Tech Providers for cross-context behavioral advertising.

B. OFFSITE MEASUREMENT ANALYSIS

For off-site measurement flows, we begin by evaluating whether measurement vendors can qualify as service providers/processors under state privacy laws. We then examine the appropriate relationships among the parties contributing personal information to the measurement vendor for the purpose of compiling the measurement report.

1. Can a measurement vendor be engaged, jointly or by each party, as a service provider/processor for the measurement purpose?

Measurement vendors must combine personal information from multiple sources to generate measurement reports that assess the effectiveness of off-site targeting. This section explores whether a measurement vendor can qualify as a service provider or processor for such measurement purposes and concludes with a yes.

IAB has already provided a detailed analysis explaining why DCRs can combine personal information for measurement and analytics under U.S. state privacy laws,¹⁸ and the argument for measurement here follows the same rationale; we provide a high-level summary of that reasoning below for reference.

¹⁶ See detailed analysis in *Data Clean Rooms, A U.S. State Privacy Law Perspective*, at https://www.iab.com/wp-content/uploads/2025/04/IAB_Data_Clean_Rooms_A_U.S._State_Privacy_Law_Perspective_April_2025.pdf.

¹⁷ See Cal. Civ. Code § 1798.185(e), Cal. Civ. Code § 1798.185(a)(10) and Cal. Code. Regs. tit. 11 § 7050(b) (“A service provider or contractor cannot contract with a business to provide cross-context behavioral advertising. Pursuant to Civil Code section 1798.140, subdivision (e) (6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-context behavioral advertising is a third party and not a service provider or contractor with respect to cross-context behavioral advertising services.”)

Under most U.S. state privacy laws, which require processors to operate under the instructions of controllers and be subject to contract terms mandated by statute, a measurement vendor can function as a processor to the controller with a properly established processor agreement. The transfer of personal information does not constitute a “sale” under these laws.

Under the CCPA, which sets a different standard, a measurement vendor can lawfully combine personal information as service providers when doing so for permitted “business purposes” such as measurement and analytics. Section 7050 of the CCPA²⁰ outlines the parameters under which service providers may use personal information, including combining it, so long as such use is limited to defined “business purposes” explicitly defined in the law and governed by a written contract. The California Privacy Protection Agency clarified in its rulemaking that combining PI falls within the scope of “use” and is permitted when done for purposes such as advertising (excluding cross-context behavioral advertising), analytics, and ad auditing—provided the service provider does not use the data for its own benefit.²¹

2. How to construe a “sale” relationship among parties who contribute personal information to the measurement vendor to compile the measurement report?

In measurement, analytics, and insights use cases, Advertisers and Publishers typically designate the measurement vendor as their service provider or processor. When this relationship is properly established, the measurement can generate outputs—whether aggregated, deidentified, or individual-record level—on behalf of the contributors.

If the output is aggregated and deidentified, no sale of personal information occurs between the Publisher and the Advertiser. However, the analysis differs when the output includes individual-level data that is not anonymized. While the measurement vendor acting as a service provider/processor to the Publisher, Advertiser or CMN typically does not involve a “sale” between the engaging party and the measurement vendor, a “sale” occurs between parties contributing personal information to the measurement vendor, unless these parties establish a service provider/processor relationship. The prevailing practice is to treat such transfers as a sale and exclude opted-out users, rather than attempting to establish a processor relationship.

¹⁸ See detailed analysis Section VII, *Data Clean Rooms, A U.S. State Privacy Law Perspective*, at https://www.iab.com/wp-content/uploads/2025/04/IAB_Data_Clean_Rooms_A_U.S._State_Privacy_Law_Perspective_April_2025.pdf.

¹⁹ See, e.g., Colo. Rev. Stat. 6-1-1303(23).

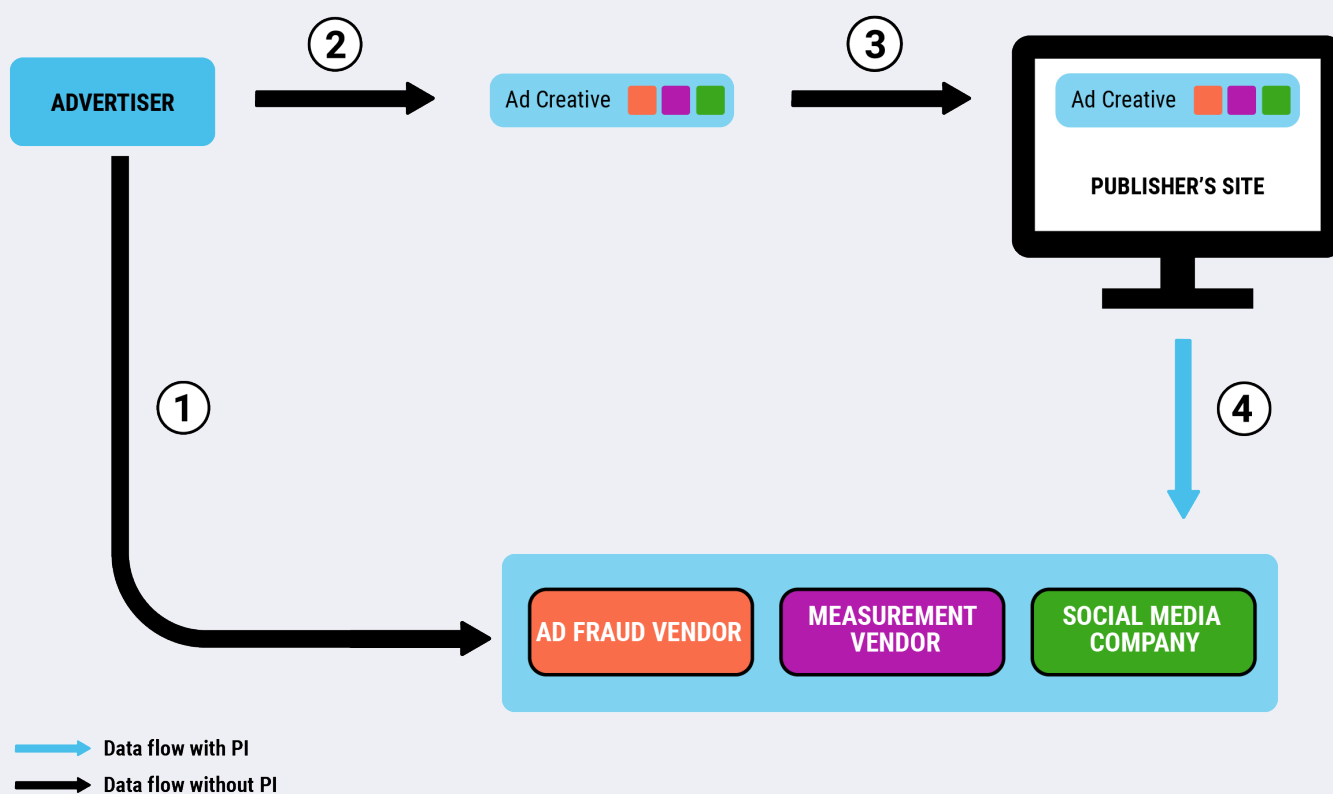
²⁰ Cal. Code. Regs. tit. 11 § 7050.

²¹ See Final Statement of Reasons, available at: https://cppa.ca.gov/meetings/materials/20230203_item4_fsor.pdf, Page 25-26.

V. THE ISSUES OF EMBEDDED ONLINE ADVERTISING TOOLS IN AD CREATIVES

By operating the onsite commerce media networks, the Consumer-Facing Businesses, such as retailers, hotels, and airlines are stepping into Publishers' roles. As a result, they encounter challenges typically faced by traditional media companies, particularly those related to embedded online advertising tools like pixels and tags used in ad creatives.

Below is a description of the data flows and the issues in the traditional Publisher's context:



Data Flow Description

1. Advertiser engages Ad Tech Providers for various services.
2. Advertiser (with their ad agencies) creates ad creative files. Such files contain embedded pixels and tags from the Ad Tech Providers in Step 1.
3. Ad creative is delivered on the Publisher's site.
4. Pixels/tags from these Ad Tech Providers fire in ad creative, resulting in personal information disclosure from the Publisher to the pixel providers.

In this data flow, pixels and tags embedded in ad creatives may bypass the Publisher's consent and tag management controls. Due to the dynamic nature of real-time bidding, Publishers often lack visibility into these elements because they do not have full control over which exact ad creative is displayed.

This creates two issues: (1) Publishers may not have contractual relationships with the Ad Tech Provider involved, causing a lack of contractual privity with required privacy terms mandated by the CCPA and other state privacy laws amongst the parties; and (2) they may not be able to effectively enforce consumer privacy opt-outs, such as those for sales, sharing, or targeted advertising.

In onsite activation flows, CMNs take on the role of Publishers and may encounter similar challenges. However, unlike traditional Publishers, CMNs often maintain greater control over the ad creatives. The working group identified several best practices commonly adopted to manage these risks:

1. CMN maintains control of which pixels are embedded in ad creatives, and directly engage with these Ad Tech Providers. Brands are prohibited from embedding their designated pixels in ad creatives.
2. Only Ad Tech Providers on an approved list are allowed to embed pixels, and these vendors must enter into appropriate agreements with the CMNs. These agreements include requirements to honor consumer opt-outs or impose service provider/processor terms.
3. If CMNs lack visibility into or control over the pixels embedded in creatives, they cease serving those ads when consumers opt out.

As CMNs evolve into more complex, programmatic structures—where multiple Brands can bid on the same inventory—the challenges outlined above may become more pronounced, making it increasingly difficult to enforce the same level of control over ad creatives and embedded tracking tools.

The IAB Multi-State Privacy Agreement (MSPA) can also serve as a valuable compliance tool to help address these challenges. The MSPA operates as a “springing contract,” establishing contractual relationships among signatories as personal information is exchanged to deliver digital advertising. While signatories may not be in direct contractual privity with every other participant upfront, such privity is automatically established when a specific data flow occurs between them. All signatories agree to a standardized, transparent set of privacy terms that align with U.S. state privacy law requirements. These terms either supplement existing commercial contracts or fill gaps where no contracts exist, ensuring that the necessary statutory privacy provisions are in place. The MSPAs are also supported by IAB Tech Lab's Global Privacy Protocol that communicates the corresponding opt-out signals accompanying the data flow.

Further, to address the above technical challenge of enforcing an opt-out in the ad creative, the MSPA shifts the burden to the downstream participants, which are in a better technical position to detect the opt-out signal and effectuate the opt-out. It requires an Ad Tech Provider to use commercially reasonable efforts to access and receive opt-out signals. When the pixel of an ad tech vendor fires in the ad creative of an ad that renders

²² Most of the U.S. state privacy laws require a controller/business to incorporate certain data protection terms with its service providers. See e.g., Cal. Civ. Code § 1798.140(ag), Cal. Code. Regs. tit. 11 § 7051, Colo. Rev. Stat. 6-1-1305(5), Conn. Gen. Stat. § 42-521(b). CCPA requires a business to incorporate certain data protection terms with third parties. Cal. Civ. Code § 1798.100(d), Cal. Code. Regs. tit. 11 § 7053.

on the Publisher's site, such Ad Tech Provider must look for and access the opt-out signal set by the Publisher prior to receiving personal information.²³

VI. OTHER PRIVACY CONSIDERATIONS

The working group explored a wide range of important issues that businesses should consider when establishing CMNs, such as operating the CMN within consumers' reasonable expectations, evaluating data broker registration requirements, assessing privacy-enhancing technologies, and personal information de-identification, etc. While many of these considerations are relevant, they are not exclusive to CMNs and often require further regulatory clarification. Given the diversity in how CMNs are structured and the complexity of the issues involved, this whitepaper does not attempt to address each topic in depth.

VII. CONCLUSION

Commerce Media Networks presents powerful opportunities for Brands and Consumer-Facing Businesses, but navigating the privacy landscape requires diligence. CMNs must assess functional roles, manage downstream relationships, and honor consumer choices across complex data ecosystems to comply with the U.S. state privacy laws.

²³ See Section 7.1(a) of the Third Amended and Restated MSPA (Downstream Participant shall use commercially reasonable efforts to access and receive Signals set or sent by other Signatories and by Certified Partners for Covered Transactions. For the avoidance of doubt, when the pixel of a Downstream Participant fires in the ad creative of an ad that renders on the Digital Property of the First Party, such Downstream Participant must look for and access the Signal set by the First Party prior to receiving Personal Information), at <https://www.iabprivacy.com/#>.

APPENDIX A: DIGITAL ADVERTISING GLOSSARY

- **Ad Exchange.** A digital marketplace that facilitates the real-time buying and selling of ad inventory between supply-side platforms (SSPs) and demand-side platforms (DSPs). Ad exchanges support auction-based transactions and provide transparency and efficiency at scale.
- **Advertiser's Ad Server.** A technology platform used by Advertisers to manage and serve creatives, track campaign performance, and collect data across multiple media environments. It ensures consistent delivery, frequency capping, and de-duplication of impressions across channels.
- **Customer Data Platform (CDP).** A centralized platform that aggregates, organizes, and activates first-party customer data from various sources (e.g., CRM, website, mobile app). CDPs enable personalized marketing and segmentation by creating a persistent, unified view of each customer.
- **Data Clean Room (DCR).** A data collaboration environment, often provided by a vendor, that allows two or more participants to leverage data assets for mutually agreed-upon use cases (e.g., analytics & insights, measurement, profile augmentation, and campaign planning), while enforcing strict data access limitations and security controls.
- **Demand-Side Platform (DSP).** A software platform that enables Advertisers and agencies to automate the purchase of digital ad inventory across multiple Publishers, exchanges, and SSPs. DSPs offer audience targeting, bidding strategies, budget controls, and real-time performance reporting.
- **Identity Resolution (ID Resolution).** Technology that connects multiple identifiers—such as device IDs, email addresses, cookies, or login credentials—into a unified consumer profile. This allows Advertisers and platforms to recognize and reach the same user across devices and channels in a privacy-compliant manner.
- **Measurement and Reporting Tool.** A platform or service that collects, analyzes, and visualizes performance metrics related to digital advertising campaigns. These tools enable Advertisers, Publishers, and intermediaries to evaluate effectiveness, optimize campaigns, and support attribution by reporting on key indicators such as impressions, clicks, conversions, return on ad spend (ROAS), and audience reach. Measurement solutions may rely on data from ad servers, clean rooms, or third-party analytics platforms.
- **Publisher's Ad Server.** A technology platform used by Publishers to manage, deliver, and report on digital advertisements served on their owned and operated media properties. It determines which ad to show, when to show it, and tracks impressions, clicks, and revenue performance.
- **Supply-Side Platform (SSP).** A technology platform used by Publishers to automate the selling of their advertising inventory. SSPs may connect to multiple ad exchanges and demand-side platforms (DSPs), enabling real-time bidding and yield optimization across multiple demand sources.

Interactive Advertising Bureau, Inc. ("IAB") provides this whitepaper as a resource for general information. Please be aware that this whitepaper does not constitute legal advice, and if you have any legal questions, please consult your attorney. While IAB has made efforts to assure the accuracy of the material in this whitepaper, it should not be treated as a basis for formulating business and legal decisions without individualized legal advice.

IAB makes no representations or warranties, express or implied, as to the completeness, correctness, or utility of the information contained in this whitepaper and assumes no liability of any kind whatsoever resulting from the use or reliance upon its contents.

© 2025 Interactive Advertising Bureau, Inc. All rights reserved. No part of this whitepaper may be sold, licensed, or otherwise commercialized without the prior written permission of IAB.