iab. PRIVACY

How the IAB Multi-State Privacy Agreement Can Help Publishers Meet the 2023 Privacy Challenges

What is the MSPA?

The IAB Multi-State Privacy Agreement (MSPA) is an industry contractual framework intended to aid advertisers, publishers, agencies, and ad tech intermediaries in complying with five state privacy laws that will become effective in 2023 (in California, Virginia, Colorado, Connecticut, Utah). The MSPA is not a "model contract" or a template agreement; instead, it is a set of privacy protective terms that spring into place among a network of signatories and that follow the data as it flows through the digital ad supply chain.

The MSPA does not contain any commercial terms, but instead supplements commercial contracts amongst signatories with required privacy terms; and where no commercial contracts exist, the MSPA provides the baseline set of privacy terms required by law. Further, while publishers can use the MSPA to cover all of their digital ads transactions, the MSPA also provides the flexibility to enter into separate agreements with counterparties for other transactions using independent privacy terms. Such transactions would simply not be MSPA "Covered Transactions."

The MSPA works together with the IAB Tech Lab's Global Privacy Platform, a uniform privacy signaling specification that allows companies to communicate and honor consumer choices throughout the ads ecosystem.

Why is the MSPA Needed to Comply with State Privacy Laws?

The new state privacy laws taking effect in 2023 pose significant challenges for publishers with respect to how they monetize their ad inventory and provide the information necessary to measure ad campaigns, many of which the MSPA is uniquely positioned to solve. Some of these compliance challenges will affect all publishers, but the MSPA also accommodates, and provides solutions for publishers that choose to either:

- "Sell," "share" or engage in "targeted advertising" and provide consumers with corresponding opt-out rights ("Opt-Out Approach");
- Rely solely on service provider relationships to avoid "selling" personal information, and do not otherwise engage in "sharing" or "targeted advertising" ("Service Provider Approach").

The charts below identify the key state privacy law compliance challenges publishers face and the MSPA's solutions.

Challenge for Publishers	Why it's a challenge	MSPA Solution	Examples
Challenges for <u>all</u> publishers			
Publishers are exposed to CPRA liability when they or their partners (*e.g.*, SSPs, ad servers) do not have contracts in place with legally required terms covering the "sale" or "sharing" of personal information.	The CPRA requires contracts for **<u>all</u>** "sales" and "sharing" of personal information, and introduces vendor due diligence requirements that can result in legal liability for publishers who do not vet the personal information they share with advertisers, agencies, and ad tech vendors.	The MSPA creates a scaled network of contractual relationships between parties "selling" or "sharing" personal information with consistent privacy terms that meet the CPRA's requirements for third-party contracts – **<u>especially where no such contracts exist today.</u>**	*Example 1: Ad servers* To deliver a digital ad to a consumer, a publisher and its vendors (e.g., ad server) request ad creative from the advertiser's ad server to fill an ad slot for a consumer. This requires the publisher to disclose consumer personal information (IP address) to the advertiser's ad server, which is likely a "sale" or "share" of personal information requiring a contract. However, at present, ad serving companies do not enter into commercial contracts with each other. With the MSPA, both publisher and advertiser cause their respective ad servers to become signatories, which creates the legally required contractual relationship between them. Without this contractual relationship, the publisher (through its ad server) is at risk of "selling" personal information without a legally required contract. *Example 2: Measurement pixels* When an advertiser's ad creative renders in a publisher's ad slot, pixels placed in the creative by the advertiser's vendors (such as measurement companies, agencies, and DSPs) cause a disclosure of personal information from the publisher site to the company whose pixel is in the ad creative. This is likely a "sale" or "share" of personal information, which, pursuant to the CPRA, requires a contract. However, at present, publishers generally do not enter into commercial contracts with advertiser pixel providers. With the MSPA, publishers and advertisers' vendors can all become signatories, which creates the legally required contractual relationship between them. In this example, advertiser or its agent can include the pixels of MSPA signatory companies in the ad creative that renders on the websites of MSPA signatories, thereby creating contractual privity between publishers and the advertisers' pixel providers.
Challenges for publishers who <u>only use service providers</u> (i.e., don't "sell," "share," or engage in "targeted advertising")			
Monetizing ad inventory through programmatic means.	CPRA prohibits service providers from engaging in "cross-context behavioral advertising," (CCBA) which limits ad targeting to contextual information or publisher first-party data only.	Cause vendors involved in programmatic transactions to become service providers and limit their use publisher information for the targeting and delivery of contextual or first-party ads only.	*Example:* Filling ad inventory programmatically requires publishers to disclose personal information like IP address and device IDs to their vendors (ad servers and SSPs), who in turn disclose that information to advertiser vendors (DSPs) who apply information they have about the user or device to select an ad. To prevent DSPs from using cross-context information (such as third-party segments) to select an ad, the MSPA enables the publisher to designate all downstream vendors as service providers and instruct them to use only contextual information and/or publisher first-party data to select an ad. This enables publishers to monetize ad inventory and use service providers in a way that complies with CPRA's prohibition on service providers engaging in CCBA.

Challenge for Publishers	Why it's a challenge	MSPA Solution	Examples
Enabling measurement and frequency capping of ads delivered to publisher ad inventory typically requires "combining" personal information obtained from different sources.	CPRA prohibits service providers from "combining" different data sets obtained outside of the service provider relationship.	Cause publishers and advertisers to jointly designate advertiser's vendors as their limited joint service providers for the advertiser and relevant publisher(s) solely to perform measurement and frequency capping, as applicable. Creates a scaled network of service providers available to act as joint service providers for the necessary use cases.	*Examples:* Many measurement methodologies require the advertiser's measurement vendor to combine information obtained from multiple sources – such as impression data from publishers with conversion event data from the advertiser (to measure frequency, reach, and attribution). Similarly, capping frequency requires combining impression data from multiple publishers. While a service provider would otherwise be restricted in its ability to do this under the CPRA, the MSPA lawfully permits the advertiser and relevant publisher(s) to jointly designate the vendors performing measurement and/or frequency capping as their joint service providers and enable data processing for those purposes.
Challenges for publishers who may "sell" or "share" personal information			
Conducting basic advertising activities while honoring consumer opt-out choices for "sales," "sharing," and "targeted advertising."	Regulators have signaled a very broad interpretation of "sale," indicating that even measurement, frequency capping, and contextual ad delivery involve "sales" that cannot proceed after a consumer opts out, except through service provider arrangements. Scaling these service provider agreements in a short time frame presents challenges.	After a consumer opts out, the MSPA creates a scaled network of service provider relationships that enable limited advertising activities while honoring the consumer's opt-out choices.	*Example 1: Filling ad inventory through real-time bidding* When a publisher sends a bid request for its ad inventory through real-time bidding, it sends personal information like device ID and IP address to ad tech vendors who facilitate the transaction. In addition, those vendors may match the information in bid requests to third-party audience segments resulting in "targeted advertising" or "cross-context behavioral advertising" that requires an opt-out choice. After a consumer has opted out, the MSPA creates a uniform way for publishers to signal the consumer's opt-out choices to ad tech vendors, requires them to honor those choices in a consistent way, and creates a scaled network of service provider relationships to enable more limited processing after a consumer opts out - for example, the use of contextual information to bid on the ad space can continue after an opt-out, but only in a service provider context. *Example 2: Measurement* An advertiser's measurement partners may collect impression data from a publisher's site through pixels included in the advertiser's ad creative. This is likely a "sale" of personal information under the CPRA requiring the publisher to present the consumer with an opt-out choice. The MSPA creates a scaled, uniform way for publishers to signal consumer opt-outs to measurement companies, requires them to honor those choices in a consistent way, and creates service provider relationships to enable purpose-limited processing for measurement to continue after a consumer opts out. It also provides a lawful way for measurement companies to "combine" information from different sources to measure more effectively.