iab. PRIVACY

How the IAB Multi-State Privacy Agreement Can Help Advertisers Meet their 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, and Utah). The MSPA is not a "model contract" or a template agreement; instead, it is a set of privacy protective terms that apply to transactions that the advertiser declares as covered by the MSPA. When doing so, those privacy terms spring into place among a network of signatories and 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 advertisers 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 ad 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 advertisers' ability to target, execute, and measure their digital ad campaigns, many of which the MSPA is uniquely positioned to solve. Some of these compliance challenges will affect all advertisers, but the MSPA also accommodates, and provides solutions for advertisers 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 advertisers face and the MSPA's solutions.

Challenge for Advertisers	Why it's a challenge	MSPA Solution	Examples
Challenges for <u>all</u> advertisers			
Advertisers are exposed to CPRA liability when their partners (e.g., agencies, ad servers, DSPs) do not ensure that contracts are 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 create legal liability for advertisers who do not vet the receipt and disclosure of personal information by ad tech vendors, agencies, or other data providers.	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 the publisher and advertiser cause their respective ad servers to become signatories, creating the legally required contractual relationship between them. *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 CPRA, requires a contract. However, at present, publishers generally do not enter into commercial contracts with advertiser pixel providers. Advertisers have legal risk when they or their agents include such pixels in the ad creative knowing that it results in sale from a publisher to pixel provider with no contract in place. This is particularly concerning in light of the CPRA's and the draft regulations enhanced audit and diligence requirements. With the MSPA, publishers' and advertisers' vendors can all become signatories, creating 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 the publisher sites and pixel providers.
Challenges for advertisers who <u>only use service providers</u> (i.e., don't "sell," "share" or engage in "target advertising")			
The CPRA prohibits "service providers" from offering "cross-context behavioral advertising."	Advertisers who do not "sell" (because they only use service providers) will be unable to use service providers to engage in cross-context behavioral advertising.	None – the MSPA cannot bypass the explicit restrictions in the CPRA and its implementing regulations.	*Example: Custom audiences and retargeting* Advertisers cannot use "service providers" to create retargeting audiences (e.g., for abandoned cart users) or provide a custom audience list to a social media platform because both of those are "cross-context behavioral advertising" according to the CPRA implementing regulations.

Challenge for Advertisers	Why it's a challenge	MSPA Solution	Examples
Measurement and frequency capping 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 solely to perform activities requiring a "combination" of personal information (e.g., measurement and frequency capping)s. Creates a scaled network of service providers available to act as joint service providers for the necessary use cases.	*Example 1: Frequency capping* Frequency capping requires multiple publishers to provide impression data to the advertiser's vendor (DSP or ad server), and that vendor must combine the cross-site impression information to manage the frequency of the ad. While a service provider would otherwise be restricted in its ability to do this under the CPRA, the MSPA lawfully permits the publisher and advertiser to jointly designate the vendor managing frequency as their joint service provider to enable frequency capping. *Example 2: Measurement* Many measurement methodologies require the advertiser's measurement vendor to combine personal information obtained from multiple sources – such as impression data from publishers with conversion event data from the advertiser to measure lift and attribution. While a service provider would otherwise be restricted in its ability to "combine" data do this under the CPRA, the MSPA lawfully permits the publisher and advertiser to jointly designate the measurement vendor as their joint service provider to enable measurement using both advertiser and publisher data.
Challenges for advertisers <u>who may "sell," "share" or engage in "targeted advertising"</u>			
Conducting basic digital 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 and frequency capping 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. The MSPA also includes all of the required contractual terms for service provider and third-party contracts.	*Example 1: Using an ad tech vendor with multiple functions* An advertiser's DSP or other vendor may place a pixel on the advertiser's site to perform multiple functions like site analytics, conversion event tracking, and creating retargeting audiences. After a consumer opts out of "sales" and "sharing" for cross-context behavioral advertising, retargeting is no longer permitted. The MSPA creates a uniform way for advertisers to signal to their vendors that a consumer has opted out, require them to honor those choices in a consistent way, and causes service provider relationships to spring into place that enable more limited processing after a consumer opts out (for example, site analytics and conversion tracking can continue after in a service provider context after an opt-out). *Example 2: Measurement* An advertiser's measurement partners may receive conversion event data from an advertiser's site. This is likely a "sale" of personal information under the CPRA requiring the advertiser to present the consumer with an opt-out choice. The MSPA creates a uniform, scaled way for advertisers to signal consumer opt-outs to their partners, 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 provides a lawful way for partners to "combine" information from different sources to measure more effectively.