iab. PRIVACY

How the IAB Multi-State Privacy Agreement Can Help Ad Tech Companies 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 (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 and advertisers can use the MSPA to cover all of their digital ads transactions, the MSPA also provides them flexibility to enter into separate agreements with their ad tech vendors 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 ad tech vendors facilitating the targeting, delivery, and measurement of digital advertising, many of which the MSPA is uniquely positioned to solve. These compliance challenges will affect all ad tech companies, both when they are acting as "third parties" under state privacy law, and when they act as "service providers." The charts below identify the key state privacy law compliance challenges ad tech vendors face and MSPA's solutions.

Challenge for ad tech vendors	Why it's a challenge	MSPA Solution	Examples
Challenges for ad tech vendors acting as "third parties"			
The CPRA requires third parties to have a contract in place with any business that "sells" or "shares" personal information with them.	When acting as third parties, ad tech vendors are often the recipients of personal information that is "sold" or "shared" to them by publishers, advertisers, and other ad tech companies. Today, there are gaps where ad tech vendors lack contracts with those companies selling or sharing personal information with them.	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 – **especially where no such contracts exist today.**	*Example 1: Ad servers* To deliver a digital ad to a consumer, a publisher and its vendors (e.g., SSPs, ad server) request an ad from the advertiser's vendors (e.g., DSPs and ad servers) to fill an ad slot for a consumer. Once an ad is selected, the publisher's ad server must disclose consumer personal information (like device ID and IP address) to the advertiser's ad server to facilitate delivery of the ad, 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 ad servers can become signatories, which creates the legally required contractual relationship between them. Without this contractual relationship, the ad servers are at risk of processing information "sold" or "shared" with them without the 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 ad tech companies who provide pixels. With the MSPA, publishers, advertisers, and ad tech vendors can all become signatories, which creates the legally required contractual relationships among them. This protects ad tech companies from unlawfully processing information "sold" or "shared" with them without the legally required contract terms in place.
Challenges for ad tech vendors acting as service providers			
CPRA prohibits service providers from "combining" different data sets obtained outside of the service provider relationship.	Conducting measurement and frequency capping typically requires ad tech vendors to "combine" personal information obtained from different sources.	Cause publishers and advertisers to designate ad tech vendors as their limited joint service providers solely to perform measurement and frequency capping, as applicable.	Many measurement methodologies require combining personal 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 ad tech vendors performing measurement and/or frequency capping as their joint service providers and enables them to process personal information for those narrow purposes.

Challenge for ad tech vendors	Why it's a challenge	MSPA Solution	Examples
Honoring consumer opt-out choices for “sales,” “sharing,” and “targeted advertising.	Ad tech vendors need a way to understand and honor consumer choices, and ensure those choices are honored by other participants in the advertising supply chain.	The MSPA provides ad tech vendors with representations and warranties concerning the Global Privacy Platform signals they receive from other signatories.	*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. The MSPA creates a uniform way for publishers and advertisers to signal to ad tech vendors whether or not a consumer has opted out, as well as provide representations and warranties to those signals.
Conducting basic advertising activities after a consumer opts of “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 enables limited advertising activities while honoring consumer opt-out choices.	*Example: Ad tech vendors offering multiple functions to their clients* A DSP or other vendor may place a pixel on an advertiser client'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 scaled, uniform way for ad tech vendors to act as service providers only after a user has opted out, and enables more limited processing to continue in a service provider context (for example, site analytics and conversion tracking can continue in a service provider context after an opt-out).