Path to State Privacy Law Compliance with the IAB MSPA

December 1, 2022

Michael Hahn
EVP & General Counsel
IAB & IAB Tech Lab

Rowena Lam
Sr. Director, Privacy & Data
IAB Tech Lab

Tony Ficarrotta
Assistant General Counsel
IAB

How did we get here?

New State Privacy Law Requirements

iab.

New State Law Privacy Requirements

- CCPA set the stage for privacy compliance in 2020
- Now, there are **5 state privacy laws coming into effect in 2023** (CA, CO, CT, UT, VA).
- They include new:
  - consumer rights to opt out of “sales,” “sharing,” and processing of personal data for “targeted advertising.”
  - requirements to have contracts in place governing essentially all transfers of personal information.
  - limitations on how service providers can use information on behalf of businesses.
- These requirements will apply to all participants in the digital advertising industry when they process consumer personal data to plan, execute, and measure digital ad campaigns.

Enforcement trends for CCPA

- The CCPA will be enhanced by CPRA and CPPA as an enforcer.
- Pending the coming changes, the California AG and CPPA:
  - Have signaled an increased focus on a business's accountability for the actions of its vendors, including liability for vendor acts if sufficient due diligence is not conducted.
  - The AG is aggressively enforcing current privacy requirements (CCPA) and setting the tone for 2023 (see SEPHORA decision).

What is the MSPA?

iab.

The IAB Multi-State Privacy Agreement

- 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 the new state privacy laws.
  - Functions as a “springing contract”
  - Supplements commercial contracts amongst signatories with required privacy terms
  - Where no commercial contracts exist, the MSPA provides the required baseline set of privacy terms

Structure of the MSPA

- Signatories are “**First Parties**” (publisher or advertiser) and “**Downstream Participants**” (vendor).
- First Parties designate which ads transactions are covered by the MSPA **(“Covered Transactions”**).
- First Parties may operate in either “**Service Provider Mode**” or “**Opt-Out Option Mode**.”
    - Service Provider Mode is for First Parties who do **not** “sell,” “share,” or engage in “targeted advertising” and who wish to engage Downstream Participants as Service Providers by default.
    - Opt-Out Option Mode is for First Parties who **may** “sell,” “share,” or engage in “targeted advertising” and who wish to engage Downstream Participants as Service Providers only after a Consumer has opted out of sales.
    - In either case, the MSPA enables Signatories to engage other Signatories as “service providers” or “processors” to assist with basic advertising activities like contextual targeting, measurement, and frequency capping -- even if a user has opted out, or if the First Party does not “sell” personal information.
- Signatories are required to send and honor GPP privacy signals.

What challenges does the MSPA help solve?

CHALLENGE #1

The LSPA covers California only, but there are now <u>five</u> state privacy laws

Solution #1

- **The State Compliance Working Group of the IAB's Legal Affairs Council has:**
  - Overhauled the existing LSPA to develop the MSPA's multi-state approach, which is intended to meet the requirements of all five state laws going live in 2023.
  - Adopted a modular approach for the MSPA, giving it the flexibility to meet the requirements of any new state laws without structural changes.
  - Provided legal requirements for an updated signaling specification to replace the us_privacy string that will account for the requirements of every state, as well as a national approach.
- **The IAB Tech Lab has:**
  - Developed a Global Privacy Platform (GPP) that will support the signaling to facilitate compliance with state laws coming into effect in 2023 and any future state laws.

CHALLENGE #2

“Sales” of personal information is very broad

iab.

Challenge #2: CPPA Signaled Broad Reach of “Sales”

“There are also newer methods that allow targeted advertising and even **conversion tracking** -- which I described as measuring whether an ad was successful -- without **relying on the sale and sharing of the user’s data across sites**. Presently, the status quo, however, is to create a profile of the user as they traverse the internet for this and many other purposes.”

Ashkan Soltani, Executive Director, CPPA (Pre-Rulemaking Meeting)

Challenge #2: AG Enforcement Action Premised on a Broad Application of “Sale”

- Online retailer Sephora paid $1.2 million in connection with a settlement with the California AG for alleged CCPA violations.
- “[Where the business discloses or makes available CONSUMERS’ PERSONAL INFORMATION to third parties through the use of online tracking technologies such as pixels, web beacons, software developer kits, third party libraries, and cookies, in exchange for monetary or other valuable consideration, including, but not limited to: (1) personal information or other information such as analytics; or (2) free or discounted services.”
- “[I]f companies make consumer personal information available to third parties and receive a benefit from the arrangement—such as in the form of ads targeting specific consumers—they are deemed to be “selling” consumer personal information under the law.”
- “Both the trade of personal information for analytics and the trade of personal information for an advertising option constituted sales under the CCPA”

Challenge #2: Industry Impact of the Broad Definition of “Sale”

- **Consumers have the right to opt out of certain ad delivery and reporting activities:**
  - **Frequency capping** is likely a “sale” because a unique user ID must be passed to count impressions against.
  - **Measurement** is likely a “sale”, because unique user IDs are often passed to count the number of people reached by an ad, where, and how often it was shown.
  - **Conversion tracking** is likely a “sale”, because advertisers often pass unique user IDs to match against impressions.

Challenge #2: Industry Impact of the Broad Definition of “Sale”

- **Consumers have the right to opt out of ad targeting based on:**
    - **Publisher audience segments** that are **sold programmatically**, such as seller-defined audiences, because the ad delivery process requires at a minimum making the consumer’s IP address available to the winning bidder. This is likely a “sale”.
    - **Contextual targeting** on inventory that is **sold programmatically**, because the ad delivery process requires at a minimum making the consumer’s IP address available to the winning bidder. This is likely a “sale”.

Solution #2: MSPA Creates a Network of Service Provider Relationships

- The MSPA creates **service provider relationships** to support the following key use cases while honoring consumer opt-out choices, including "sales" opt out:
  - Measurement and frequency capping (these are carved out of "targeted advertising," but not "sales")
  - Programmatic advertising involving contextual signals or first party segments
- When a consumer opts-out, these activities cannot be undertaken **unless there is a service provider agreement in place**. The MSPA accomplishes this function.
- For advertisers that operate solely with service providers (i.e., do not sell, share or engage in targeted advertising), they can leverage the MSPA's broad network of ad-tech firms who will serve as service providers using the MSPA's privacy protective terms.

CHALLENGE #3

When a publisher or advertiser engages a measurement company or DSP as a service provider, it cannot measure or frequency cap insofar as those activities typically require a combination of personal information, which is limited by the CPRA

iab.

Solution #3: MSPA Creates Limited Joint Service Provide Relationships

- The MSPA creates:
  - Springing service provider relationships between First Parties and Downstream Participants that follows the data.
  - Limited joint control for measurement purposes between the advertiser serving an ad and the publisher which owns the digital property upon which the ad is served.
    - The advertiser and publisher jointly designate the measurement company as their limited joint service provider solely to measure a particular ad served to the consumer.
    - In doing so, the measurement company can combine the personal information of the advertiser and publisher because the combination is for the same shared business purpose – measuring the ad (as opposed to combing personal information for multiple different business purposes).
  - Limited joint control to engage in frequency capping between the advertiser serving an ad and the publishers owning the digital properties upon which the ad is served.
    - The advertiser and publishers jointly designate the DSP as their limited joint service provider solely to frequency cap a particular ad served to the consumer.
    - In doing so, the DSP can combine the personal information of the advertiser and publishers because the combination is for the same shared business purpose – limiting the number of times the consumer views the ad (as opposed to combing personal information for multiple different business purposes).

CHALLENGE #4

The CPRA requires contracts when industry participants make available (i.e., “sells”) personal information to others

Challenge #4: CPRA’s Third Party Contract Requirement

- The CPRA has specific requirements for third-party contracts, so the MSPA includes provisions that satisfy the CPRA’s requirement for these contracts to:
  - Specify the limited and specific purposes for which personal information is disclosed.
  - Require the recipient of the information to provide the same level of privacy protection required by CPRA.
  - Grant the business rights to take reasonable and appropriate steps to ensure privacy obligations are met.
  - Require the recipient to notify the business if it can no longer meet the CPRA’s requirements and grant the business rights to remediate.

Solution #4: The MSPA Fills Gaps in the Digital Supply Chain

- Any business that makes consumer personal information available to third party must have a contract with specific data protection language in place, even if the consumer has not opted out.
- However, contracts typically do not exist for:
    - Publishers who have no relationship with the provider of a tag or pixel that fires in ad creative served on their properties
    - Publishers and DSPs who receive bid requests from them
    - Publisher and Advertiser ad servers that interact to retrieve ad creative and track ad serving
- The MSPA creates contractual privity among signatories that do not have an underlying agreement

CHALLENGE #5

The CPRA adds contract requirements for third-party, contractor, and service provider agreements that must be solved at scale

iab.

Solution #5: The MSPA Creates a Scaled Contracting Solution

- The MSPA meets the specific requirements for third-party contracts.
- The MSPA is also designed to meet all of the requirements for contracts between a business/controller and a service provider/contractor/processor.
  - If service provider/contractor/processor relationships are not in place with vendors where they are needed for compliance (e.g., after a “sale” opt out), the MSPA creates them.
  - For existing service provider/processor relationships, any gaps between CCPA compliance and CPRA/Multi-State compliance for those agreements will be covered.

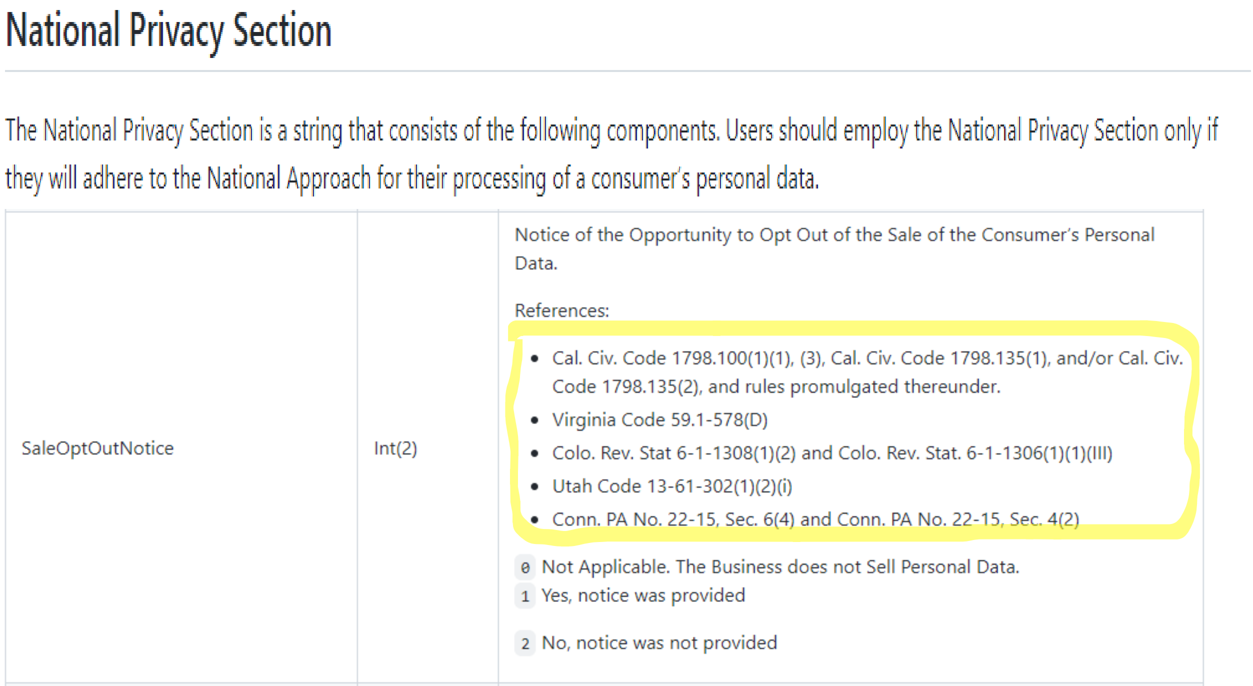
CHALLENGE #6

Some publishers and advertisers may choose to identify the residency of the consumer, while others may not

Solution #6

- The MSPA and the corresponding state-level privacy signals encoded into the GPP will allow first parties to use commercially reasonable methods to determine the residency of a consumer and provide the consumer with choices consistent with applicable state law.
- Some publishers and advertisers may choose not to determine the residency of a consumer, in which case the MSPA provides for a "national approach" to facilitate compliance for Covered Transactions. Under the national approach:
    - The MSPA assumes that the consumer is a resident of <u>each</u> state.
    - The MSPA applies the "highest standard" for each applicable concept.
    - The GPP will include "national approach" signaling

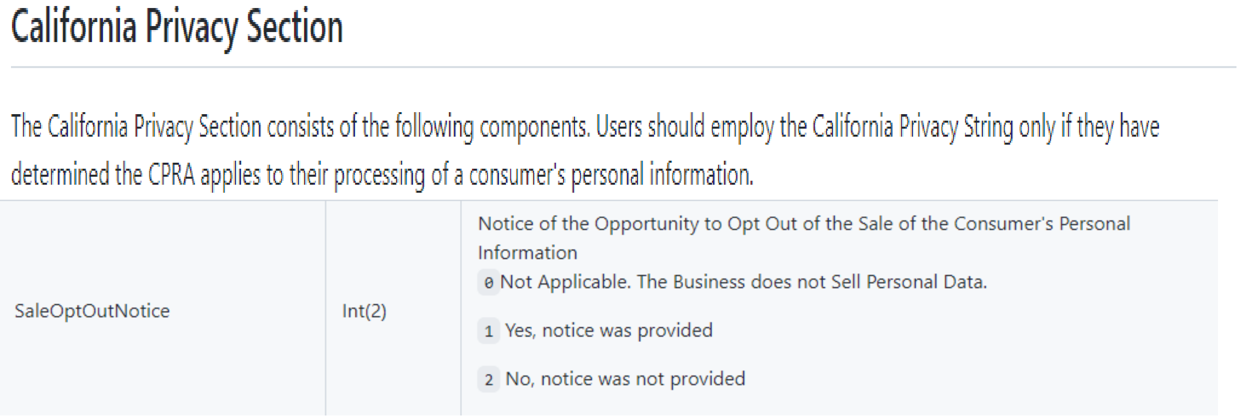
National vs. State Specific Signaling



National Privacy Section

The National Privacy Section is a string that consists of the following components. Users should employ the National Privacy Section only if they will adhere to the National Approach for their processing of a consumer's personal data.

SaleOptOutNotice	Int(2)	Notice of the Opportunity to Opt Out of the Sale of the Consumer's Personal Data. References: • Cal. Civ. Code 1798.100(1)(1), (3), Cal. Civ. Code 1798.135(1), and/or Cal. Civ. Code 1798.135(2), and rules promulgated thereunder. • Virginia Code 59.1-578(D) • Colo. Rev. Stat 6-1-1308(1)(2) and Colo. Rev. Stat. 6-1-1306(1)(1)(III) • Utah Code 13-61-302(1)(2)(i) • Conn. PA No. 22-15, Sec. 6(4) and Conn. PA No. 22-15, Sec. 4(2) 0 Not Applicable. The Business does not Sell Personal Data. 1 Yes, notice was provided 2 No, notice was not provided



California Privacy Section

The California Privacy Section consists of the following components. Users should employ the California Privacy String only if they have determined the CPRA applies to their processing of a consumer's personal information.

SaleOptOutNotice	Int(2)	Notice of the Opportunity to Opt Out of the Sale of the Consumer's Personal Information 0 Not Applicable. The Business does not Sell Personal Data. 1 Yes, notice was provided 2 No, notice was not provided

- The GPP string section for the National Approach enables users of the string to communicate whether they have adhered to notice and choice requirements in each state privacy law.
- If different states set a different standard, the National Privacy String format uses the higher standard.

- State-specific privacy strings enable users of the string to take a state-specific approach to compliance by communicating only the notice and choice requirements that appear in that state's privacy law.

Becoming an MSPA Signatory

Existing LSPA Signatories

- **For entities that have already signed the LSPA:**
  - The MSPA will act as an amendment to the LSPA.
  - All LSPA Signatories will receive notice today (12/1/2022) of the amendment.
  - The amendment will take effect on January 1, 2023, at which time all LSPA Signatories will become MSPA Signatories.
- **Legacy LSPA Signatories will need to update certain information through the MSPA registration portal (**https://tools.iabtechlab.com/mspa) **as follows:**
  - When they have completed their GPP builds, making an update to indicate this. They can then begin processing Covered Transactions using the GPP.
  - Downstream Participants must indicate whether they will act as Contractors under CPRA and must list Subproviders who will assist with Covered Transactions.

New MSPA Signatories

- Entities that have **not** already signed the LSPA and are signing the MSPA for the first time will become MSPA Signatories effective immediately after completing registration and signing the agreement.
- To become an MSPA Signatory, use the registration portal available at https://tools.iabtechlab.com/mspa to provide the required registration information and sign the Agreement. The portal can also be found through https://www.iabprivacy.com/

MSPA Implementation – Timeline for Completing GPP Builds

iab.

The “Bullpen” – MSPA Signatories with GPP builds in progress

- **The MSPA allows a grace period for Signatories to complete GPP builds.**
  - Companies relying on the grace period (*i.e.* waiting in the “Bullpen”) have until July 1, 2023 to complete their GPP builds. Signatories in the Bullpen will not be able to participate in Covered Transactions that include GPP signals, but may do so using USPrivacy signals for California residents.
  - Once MSPA Signatories complete their GPP builds, they must make an update in the MSPA portal indicating they are ready to process GPP strings as part of Covered Transactions, and may at that time commence participation in Covered Transactions that use GPP strings.
  - The grace period sunsets on July 1, 2023 and all MSPA Signatories must then use GPP for Covered Transactions.

Using USPrivacy with the MSPA

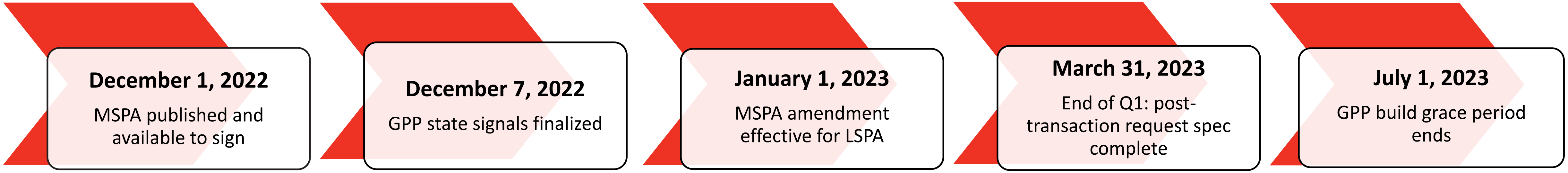
- The MSPA includes a provision that allows companies to use the legacy USPrivacy signaling specification before July 1, 2023 to support MSPA Covered Transactions for California residents while all Signatories complete their GPP builds.
  - The MSPA Technical Signaling Implementation Guidelines explain how USPrivacy strings should be handled for MSPA Covered Transactions.
  - Companies may continue using USPrivacy for MSPA Covered Transactions until July 1, 2023. The grace period then sunsets and all MSPA Signatories must use GPP for Covered Transactions.

Technical Signaling Implementation Guidelines

- The IAB has developed additional Technical Signaling Implementation Guidelines that explain how the requirements of the MSPA connect to the IAB Tech Lab's GPP signaling specification, including:
  - Rules for how to use different sections of the GPP string for different jurisdictions;
  - When and how to set opt out signals (for sales, sharing, and targeted advertising); and
  - How different signals interact with one another.
- The Guidelines also include instructions for how to use the USPrivacy signaling specification for MSPA Covered Transactions before July 1, 2023.
- The Guidelines are available at https://www.iabprivacy.com/mspa.html.

TIMELINES

MSPA, GPP & Other Specs Timeline



December 1, 2022
MSPA published and available to sign

December 7, 2022
GPP state signals finalized

January 1, 2023
MSPA amendment effective for LSPA

March 31, 2023
End of Q1: post-transaction request spec complete

July 1, 2023
GPP build grace period ends