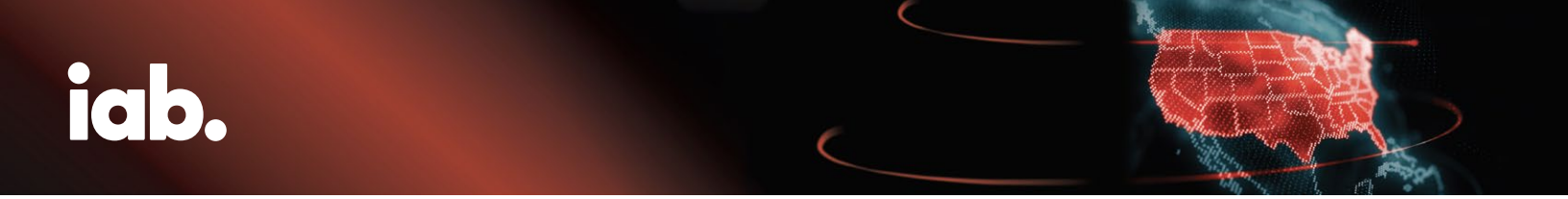
iab.

State Privacy Law Survey Results

August 2023

Sponsored by:

Kelley Drye | Ketch



Executive Summary

Introduction

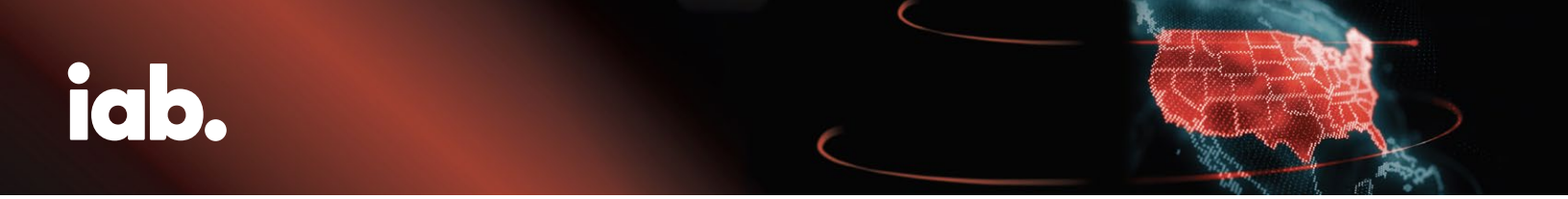
This year, five states—California, Colorado, Connecticut, Utah, and Virginia—have comprehensive consumer privacy laws going into effect. The laws going into effect in each of these states introduce new requirements that will broadly impact the digital advertising ecosystem. How new generally applicable legal requirements translate into changes to personal data management and sharing practices is perfectly clear in some instances and, in others, market participants have multiple interpretations.

The IAB Legal Affairs Council seeks to improve clarity and consensus around the application of state privacy laws to the digital advertising industry, especially with respect to practices that regulators have not yet opined on (as often is the case with any new law). In furtherance of that goal, the Legal Affairs Council recently surveyed industry participants, across publishers, sell-side and buy-side ad tech companies, agencies, brands, and law firms regarding the implementation of the new state privacy laws as well as best practices. Just under half of respondents were publishers, whereas the remaining respondents represented media buyers or other market participants (such as technology providers or law firms). The survey—which garnered nearly 100 responses—posed questions on critical topics, including:

- The distinction between "sales" and "shares" of personal information for common digital advertising activities under California privacy law;
- Industry readiness for new opt-out and consent requirements, including operationalizing opt-out preference signals, sensitive personal information consent requirements, and opt-outs related to profiling and/or automated decision-making;
- The impact of the IAB Multi-State Privacy Agreement (MSPA) on compliance with state privacy law requirements;
- Whether advertising agencies face potential liability under state privacy laws given the different roles and interactions they have with personal data in ad campaigns;
- The types of advertising, if any, that are permitted after a consumer exercises an opt-out request; and
- The impact on ad campaign measurement activities of the California Consumer Privacy Act's (CCPA's) restriction on service providers "combining" personal information.

The survey reveals important areas of consensus on how the state privacy laws apply to the digital advertising industry, as well as areas where views and practices diverge amongst participants, including:

- Most respondents believe that the term "sale" is a broad concept under each state privacy law and generally captures making personal information available for sharing or targeted advertising, ad delivery, and measurement activities.
- The MSPA plays a central role in supporting compliance with state privacy law contractual requirements.
- Nearly half of respondents do not feel prepared to comply with the vendor due diligence obligations required under the laws.



- A majority of respondents believe that after a user opts out, ads can be selected using publisher first party data or contextual signals only—but there is still a significant percentage of the market that expressed the problematic belief that ad selection based on advertiser personal information can be leveraged (for example, for retargeting or custom audience activation).
- Ad agencies can have liability if they fail to conduct adequate diligence on privacy compliance requirements in effectuating ad campaigns.

We hope these survey results, which are appended here, provide insight to industry participants and observers about how obligations under new state privacy laws are being interpreted, as well as provide a roadmap to benchmark their compliance practices.

Sales and Shares in Digital Advertising

The question of what constituted a "sale" of personal information in the context of digital advertising was fiercely debated in the early days of the CCPA. Three years later, and with significant rulemaking and enforcement history to rely on, the survey results show broad industry consensus on the topic.

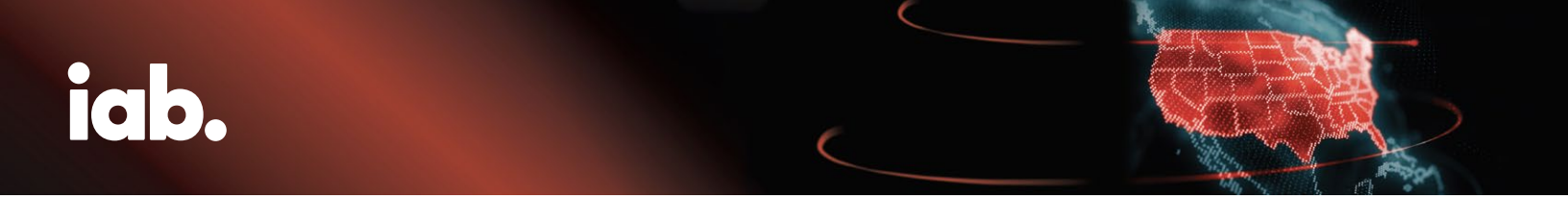
In particular, survey respondents overwhelmingly indicated that the term "sale" is a broad concept and that it generally captures both the "sharing" of personal information for cross-context behavioral advertising, as well as transfers of personal information for ad delivery and measurement activities. This viewpoint is consistent with the statement made by the California Attorney General's office in its complaint against Sephora that "if 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" and are required to give notice to the customer.[1] While regulators have not yet elaborated on the scope of the term "sale" under other state privacy laws, over half of respondents expect regulators to interpret the term "sale" in a manner consistent with how the California Attorney General's office has interpreted the term under the CCPA.

The MSPA Should Play an Important Role in Third-Party Compliance Programs

Respondents, including strong majorities of both buyers and sellers of ad inventory, respectively, indicated that the IAB's MSPA plays an important role in addressing compliance with the new CCPA provision that requires businesses to enter into contracts (containing certain privacy protective provisions) with third parties. This is a particular challenge in digital advertising because personal information is often sold and re-sold through the digital ad supply chain.

Two-thirds of respondents indicated that the MSPA—either alone or in combination with one-off, bespoke data protection agreements—offers the best means by which publishers, advertisers, pixel providers, and other third parties can comply with the CCPA's contractual requirements related to the sale or sharing of personal information with third parties, in particular when those sales and shares occur through the delivery of ad creative via third-party ad servers and through ad creative that may include third-party pixels.

[1] Complaint. *People of the State of California v. Sephora USA, Inc.*, San Francisco Superior Court Case No. CGC-22-601380, ¶ 3.



Combinations of Personal Information

Under the CCPA, service providers and contractors are prohibited from combining personal information received from or on behalf of the business they are servicing with personal information collected from or on behalf of another person or persons, or from its own interaction with the consumer, subject to certain exceptions.

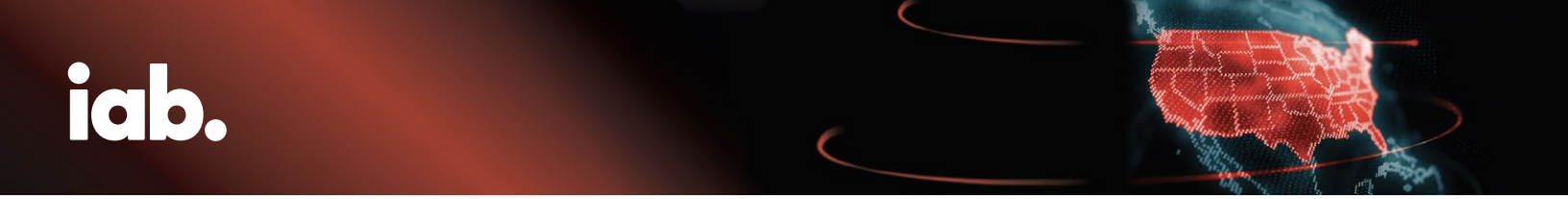
In general, a majority of respondents indicated that service providers and contractors can undertake ad measurement in compliance with this restriction, however, those respondents provided materially different reasons to justify that position.

For example, 33% of respondents indicated that a measurement company may lawfully conduct measurement using both advertiser and publisher data if the measurement company agrees to act as a joint service provider on behalf of publishers and advertisers who each agree to exercise joint control over measurement information. In practice, this is achieved by all parties signing the MSPA. Meanwhile, 10% of respondents indicated that there is simply no "combination" subject to the restriction that occurs when engaging in measurement, even though ad measurement often involves processing personal information collected from multiple sources by a measurement company (for example, collecting ad exposure data from a publisher and analyzing it together with conversion event data collected from an advertiser). This suggests that some respondents believe at least some methods for processing data across different data sets does not automatically result in a "combination" for CCPA purposes. Another 17% indicated that measurement companies may combine information for any business purpose enumerated by the CCPA—except for cross-context behavioral advertising—and remain in compliance with the CCPA's restrictions on service provider activities.

This range of responses highlights the need for additional regulatory clarity regarding how the service provider "combination" restriction applies to ad reporting and related activities (e.g., measurement by Mobile Measurement Platforms (MMPs) and other types of ad campaign measurement providers, anti-fraud activities, and viewability services), and the extent to which the CCPA business purpose being relied upon by a service provider/contractor may affect the analysis.

There is an Emerging Industry Consensus Regarding the Scope of Agency Liability

A majority of respondents—including at least half of respondents representing ad agencies—agree that an ad agency would likely be liable for continuing the frequent practice of including pixels in the ad creative they develop for advertisers in circumstances where the agency does not ensure adequate contracts and controls are in place with publishers who serve that ad creative, as required by law. For example, when an agency includes pixels in the ad creative on behalf of an advertiser, this causes the publisher to "sell" or "share" personal information, or engage in "targeted advertising," when the ad creative loads and pixels fire on the publisher's page. In this scenario, the survey asked to what extent *an agency* (or advertiser, if the agency is their service provider) would be liable if: (1) the agency does not ensure that *a publisher* has legally required contracts in place with the providers of pixels that fire in the ad creative—and to whom the publisher is "selling" or "sharing" personal information; and (2) the publisher fails to a honor consumer opt-out request with respect to pixels firing in the ad creative—which could result in the agency (or advertiser) controlling or processing personal information from an opted-out consumer.



Only 4% of respondents said that an agency would probably not have any liability for failing to ensure that publishers have the required contracts with the pixel providers. Similarly, a minority (18%) of respondents said that an agency would probably not have any liability for failing to ensure that publishers could effectuate an opt-out with respect to pixels in the ad creative. In contrast, the majority of respondents indicated that an agency likely has liability in those circumstances, but those respondents had differing views concerning the basis for such liability. For example, 53% of respondents agreed that the agency could have liability for failing to conduct adequate due diligence on the publisher when the publisher did not have any adequate means of effectuating opt-outs for pixels firing in the ad creative, and 37% believed that a lack of due diligence could be the basis for liability if a publisher failed to enter into legally required contracts governing "sales" and "sharing" of personal information caused by pixel fires in the ad creative. In addition, according to 35% of respondents, agency liability could be predicated on the scenario where the pixel provider was a service provider to the advertiser (and not an independent "controller" or "business" with respect to the personal information collected via pixels).

Addressing Sensitive Data and New Opt-Out Rights

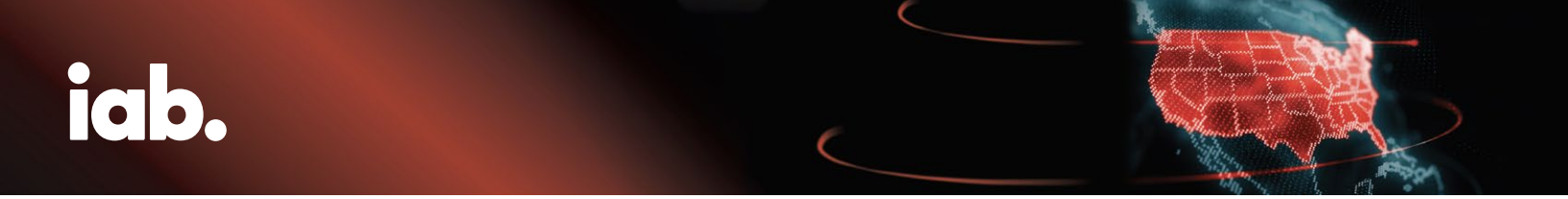
The state privacy laws covered by the survey generally impose new requirements on the processing of sensitive personal information and offer the right to opt-out of profiling and automated decision-making. The survey asked respondents how they understood the effects of these requirements on their businesses.

Sensitive Personal Information

Only 34% of respondents expected to process sensitive personal information in connection with digital advertising activities, while 13% remained unsure. In contrast, approximately half of respondents do not expect to process sensitive personal information. This could either represent a decision by market participants to avoid processing sensitive personal information altogether, or, alternatively, indicate that market participants are taking different positions on what constitutes sensitive personal information.

Opt-Out of Profiling or Automated Decision-Making

Several of the state privacy laws include a right to opt-out of profiling and/or automated decision-making that has a legal or similarly significant effect. Only 19% of respondents believe that audience segmentation and/or profiling for advertising purposes does or may constitute the kind of profiling and/or automated decision-making contemplated by state law, requiring a separate opt-out from the opt-out of sales or shares for targeted advertising. Another 33% of respondents stated that these practices may qualify as profiling and/or automated decision-making such that it necessitates a separate opt-out, but only in certain limited circumstances (e.g., when those profiles are used to select advertisements for housing, financial services, or other similar categories). 22% of respondents felt that audience segmentation and/or profiling for advertising purposes never qualify as the kind of profiling and/or automated decision-making contemplated under state law, in part likely because consumers can effectively opt-out of these practices through the opt-outs for sales, shares, or targeted advertising. Finally, while 26% were unsure. We hope regulators will provide further clarity on this topic over time.



Implementation and Readiness

General Compliance with the State Privacy Laws

Given the continued adoption of state-level privacy laws, the survey asked respondents how they plan to comply with this evolving privacy landscape. Most respondents indicated they are taking a "national" approach to privacy compliance, with 63% of respondents stating that they plan to provide consumers in all states with notice, choices, and rights intended to comply with each applicable state privacy laws, regardless of a given consumer's state residency.

Service Provider Due Diligence

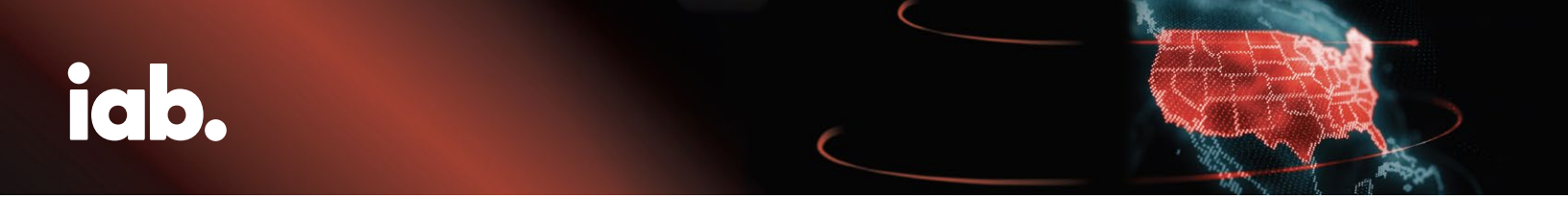
The state privacy laws covered by the survey impose varying due diligence obligations on businesses that use processors, service providers, or contractors to process personal information on their behalf. The survey results show that the industry lacks clarity concerning the necessary steps to implement these requirements. Moreover, nearly half of respondents (44%) do not feel prepared to comply with the vendor due diligence obligations required under the laws.

Opt-Out Preference Signals

Several state privacy laws require businesses to read and honor opt-out preference signals set at the browser level, such as the Global Privacy Control. Over half of respondents feel they are prepared for this requirement and currently read and honor opt-out preference signals for all consumers, while 14% read and honor opt-out signals only in jurisdictions where doing so is (or will be) required by law. The remaining respondents (13%) indicated that they do not yet read or honor opt-out preference signals or, alternatively, indicated that they do not believe they are required to do so because they do not "sell" or "share" personal information (21%). The widespread implementation of mechanisms to honor opt-out preference signals is encouraging, particularly in light of the office of the California Attorney General's focus on compliance in this area.

The updated CCPA regulations promulgated by the California Privacy Protection Agency (CPPA) also grant certain compliance exceptions for those businesses providing consumers with an opt-out of all "sales" and "shares" by the business in "frictionless" manner via an opt-out preference signal. For an opt-out to be "frictionless," it must meet the high standard set out in the regulations. Specifically, the business must not: (1) charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal; (2) change the consumer's experience with the product or service offered by the business; or (3) display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal.[2] Still, 44% of survey respondents that currently read and respond to opt-out preference signals believe that they meet the "frictionless" requirement. This suggests that those respondents are able to effectuate opt-outs for *all* of their "sales" and "sharing" after receiving an opt-out preference signal. However, the technical challenges posed by implementing this kind of thoroughgoing opt-out, in particular across both pseudonymous IDs (e.g. cookies or device IDs) and log-in information like email address, remain daunting.

[2] 11 C.C.R. § 7025(f).



Honoring Opt-Out Requests Generally

The State Law Survey asked respondents to select the types of advertising and methods of ad delivery that a publisher is still permitted to engage in after a consumer exercises an opt-out of sale, sharing, or targeted advertising.

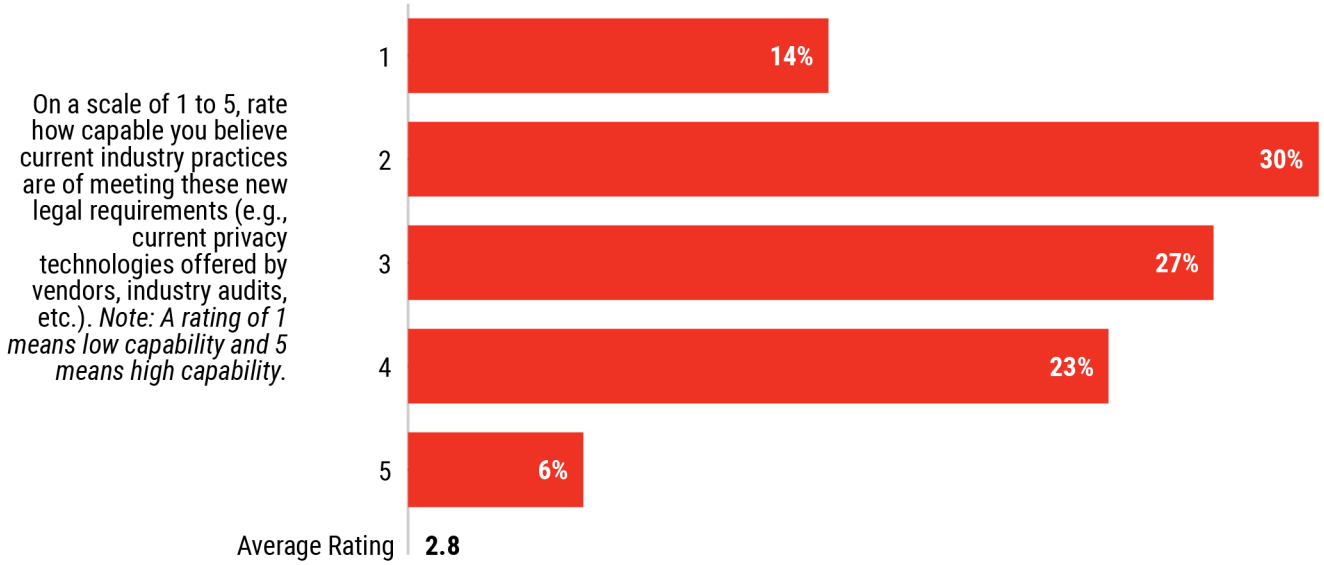
There was no broad consensus on the *methods of ad delivery* permitted after an opt-out request, indicating that additional industry education may be needed on this point. Specifically, 39% of respondents said that the publisher must use only its own first-party ad server to deliver advertising after an opt-out, and may not use third-party ad servers in this scenario. However, 35% said that the publisher may allow third-party ads to be delivered to its ad inventory after an opt-out. The remaining 26% of respondents either stated that the publisher should not deliver any advertising to the consumer after an opt-out (15%) or had no opinion on the topic (11%).

On the question of the *type* of advertising that may be delivered to a consumer after an opt-out, approximately 70% of respondents stated that the publisher may deliver "house" advertising for their own products and services, and may also deliver contextual advertising. This result suggests that a portion of the market may not be considering how an IP address is personal information that is leveraged in contextual ad bids, which necessitates a string of service provider relationships across the sell-side and buy-side vendors (e.g., the MSPA). Additional industry education is likely needed on this topic in light of the survey responses.

Survey Results

Q1: The CPRA and its implementing regulations require businesses to conduct due diligence of their service providers and contractors, as well as third parties to whom they sell or share personal information, in order to avoid potential liability for the acts of those entities *(see Cal. Civ. Code 1798.135(g), 145(i))*.

On a scale of 1 to 5, rate how capable you believe current industry practices are of meeting these new legal requirements (e.g., current privacy technologies offered by vendors, industry audits, etc.).

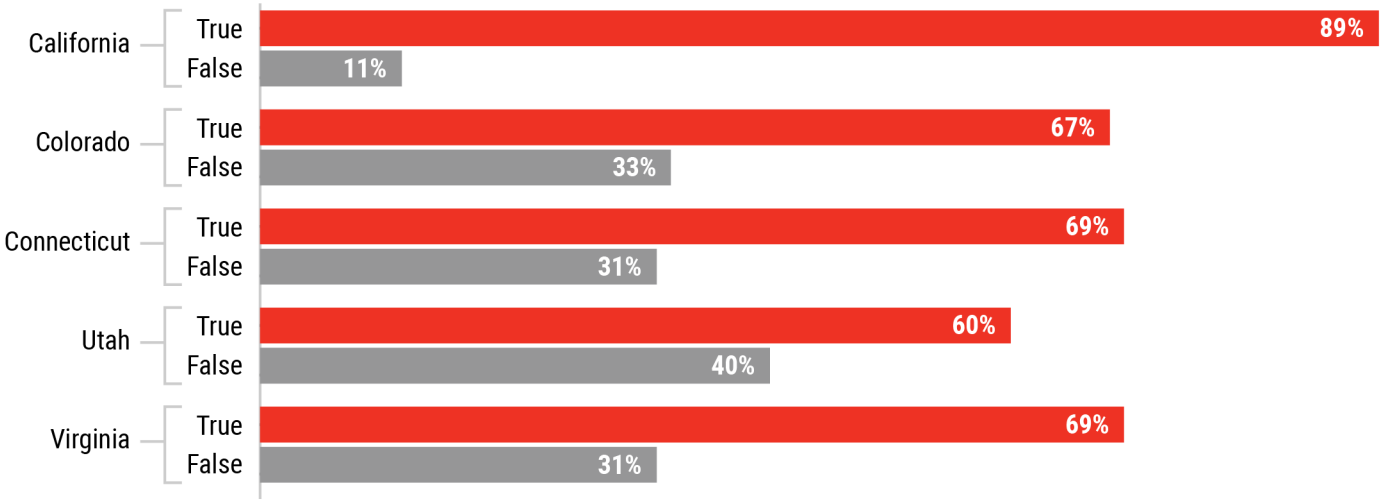


Base: Percent of Responses 100%

Q2: Regarding the relationship between the concepts of "sale" and "share" under the CPRA *(see Cal. Civ. Code Sections 1798.140(ad),(ah))* **which do you think most accurately describes disclosures of personal information for Cross-Context Behavioral Advertising** *(CCBA, see Cal. Civ. Code 1798.140(k))***?**

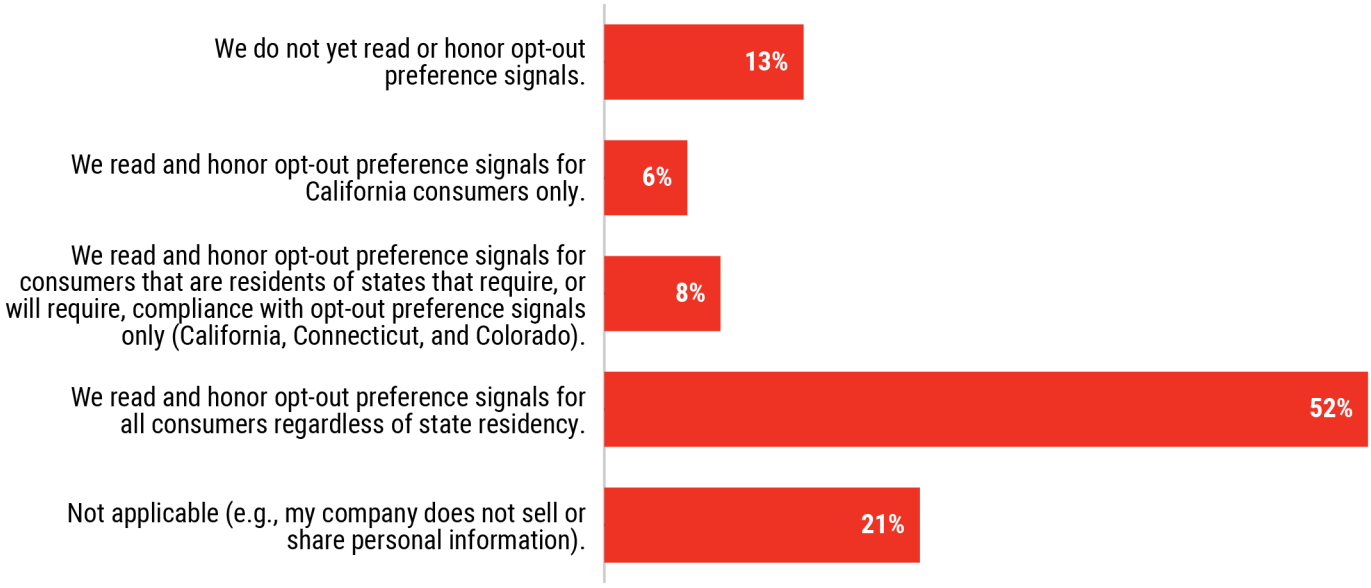
Base: Percent of Responses 100%

Q3: True or false: All disclosures of personal information from a business or controller to a third party *(i.e., not a service provider or processor)*, **whether for targeting a consumer, for measurement or ad delivery purposes, are subject to a consumer opt-out choice** *(i.e., are a "sale" "sharing," or "targeted advertising").*



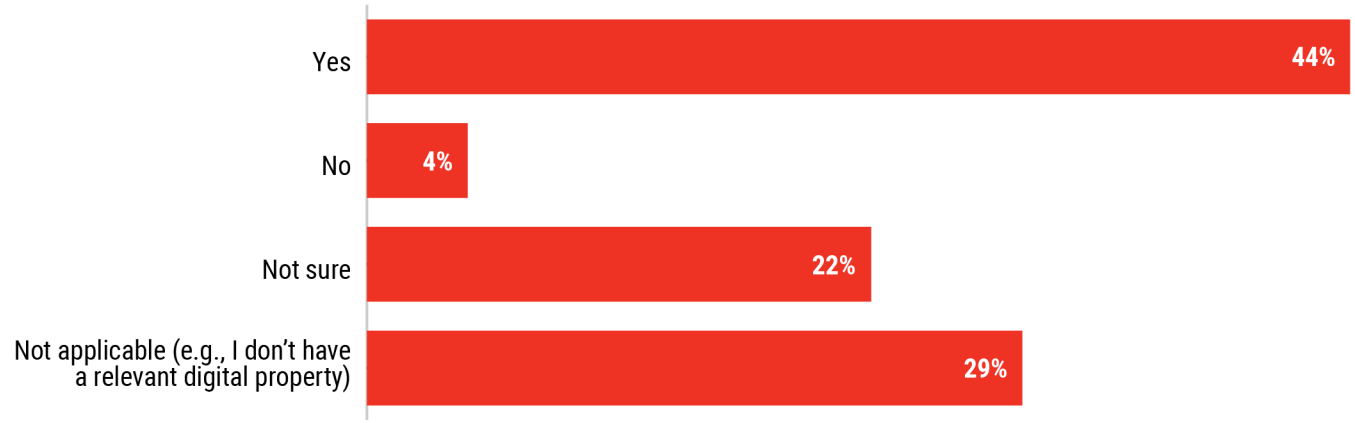
Base: Percent of Responses 100%

Q4: Some state privacy laws require, or will require, businesses to read and honor opt-out preference signals *(such as Global Privacy Control)*. **Which betst describes your company's implementation of opt-out preference signals?**



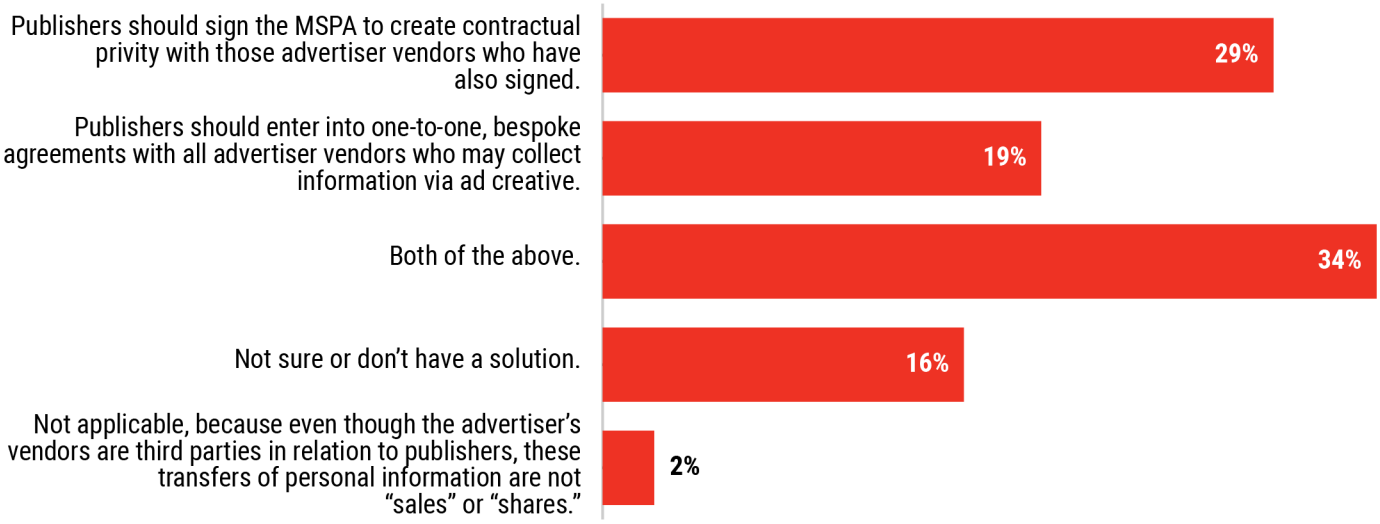
Base: Percent of Responses 100%

Q5: If you have implemented the technology needed to read and respond to opt-out preference signals for one or more of your digital properties, do you allow consumers to opt out in a "frictionless" manner as contemplated by the CPRA regulations *(see e.g. CPRA regulation 7013(d))***?**



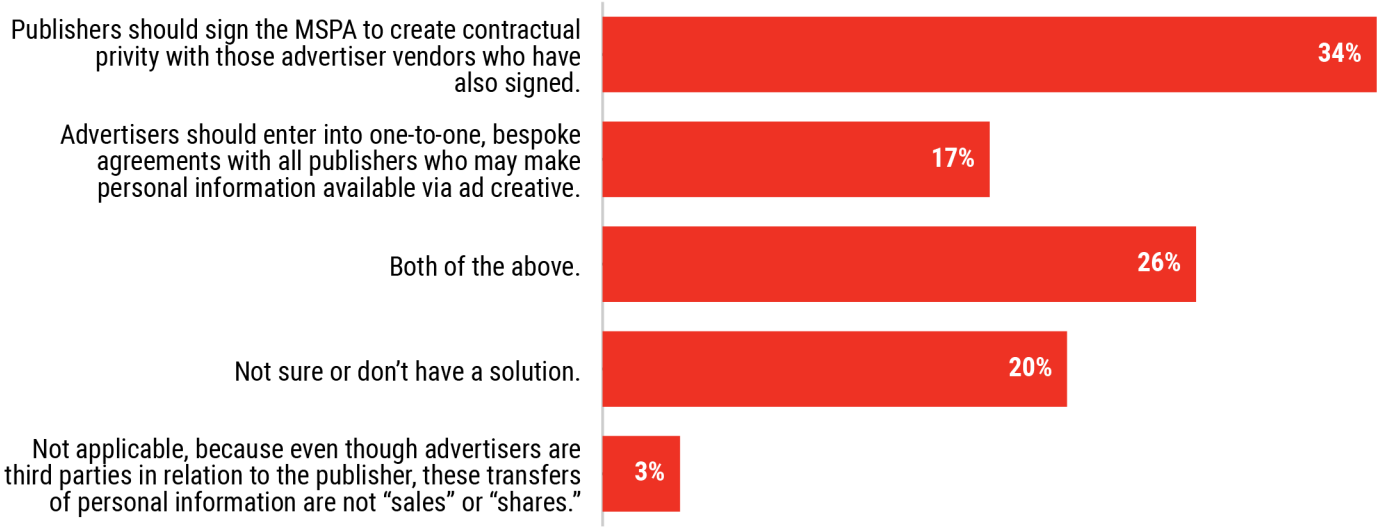
Base: Percent of Responses 100%

Q6: The CPRA requires a contract with certain privacy protective provisions to be in place between a business and a third party for all "sales" and "shares" of personal information. In practice, this means that whenever an advertiser's ad creative is delivered to an ad inventory slot, the publisher "sells" or "shares" personal information to the advertiser or its vendors involved in selecting, delivering, and measuring the ad *(such as third party ad servers, DSPs, measurement companies, and/or agencies)***. In your view, what is the best way for a publisher to comply with the requirement to have a contract in place with those third parties to whom it may "sell" or "share" personal information via ad creative?**



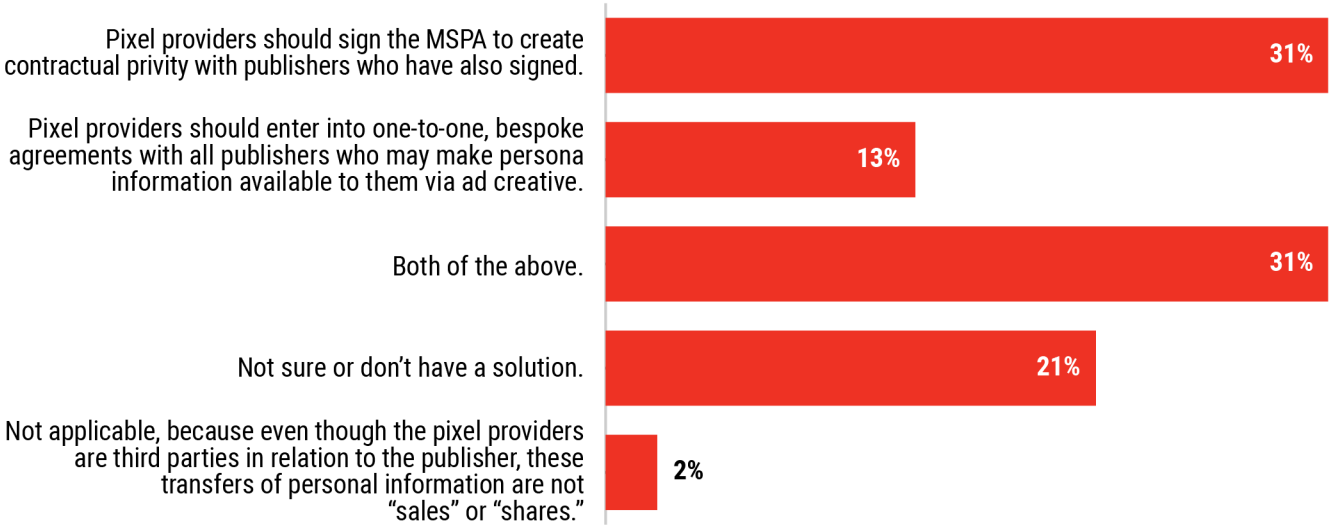
Base: Percent of Responses 100%

Q7: When an advertiser *(or agency acting on its behalf)* **includes pixels in ad creative for a digital ad campaign using pixel providers who act as the advertiser's service providers or contractors for CPRA purposes, those pixels cause a "sale" or "share" of personal information from the publisher to the advertiser because the advertiser is then the third party business that controls the personal information sold or shared via the pixel** *(the vendor is only a service provider)***. In those circumstances, what do you view as the best path for advertisers to comply with the requirement to have a contract in place with those publisher "businesses" who "sell" or "share" personal information to them as "third parties" via ad creative delivered to the publisher page?**



Base: Percent of Responses 100%

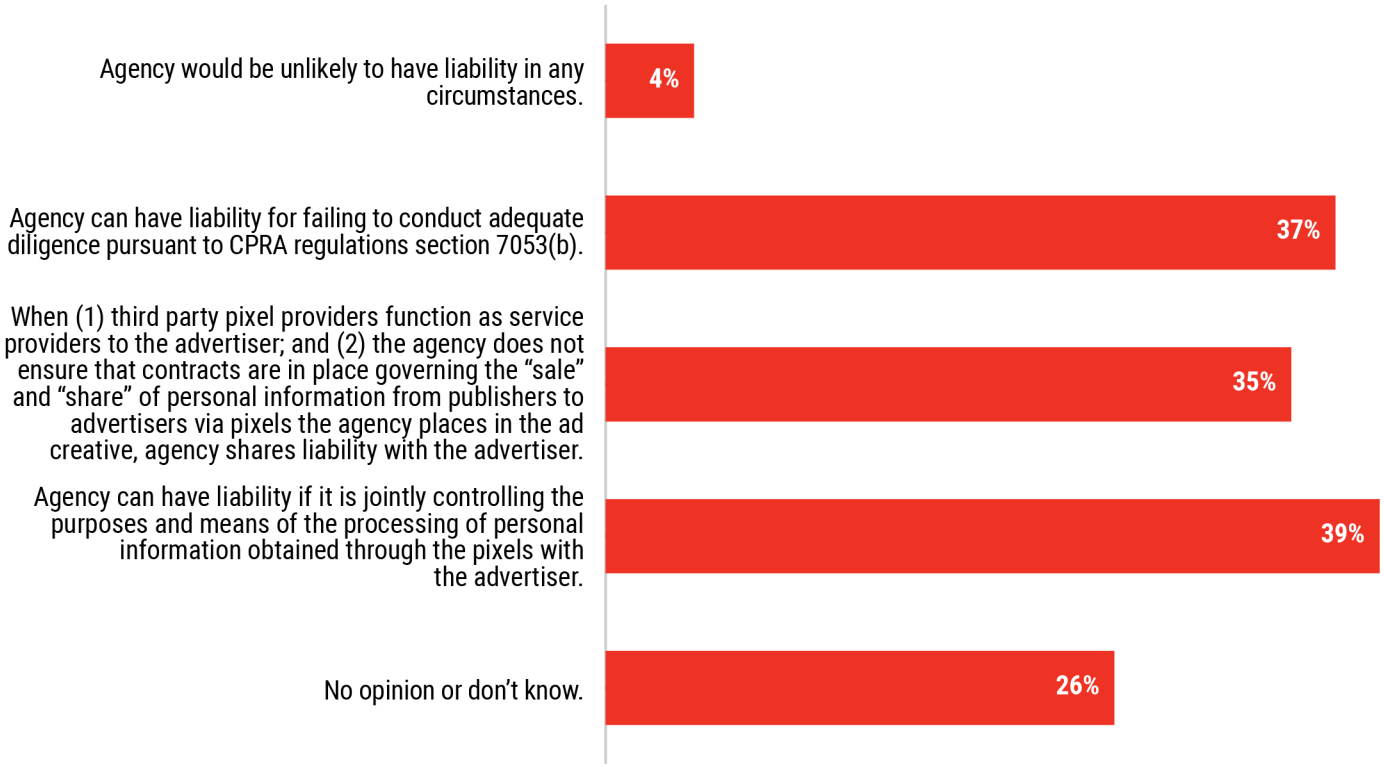
Q8: When an advertiser *(or agency acting on its behalf)* **includes pixels in ad creative for a digital ad campaign using vendors who are not acting as the advertiser's "service provider" or "contractor" under CPRA, those pixels cause a "sale" or "share" of personal information from the publisher to the pixel provider because the pixel provider is the third-party business that controls the personal information sold or shared via the pixel** *(even if the pixel provider is acting on behalf of the advertiser or agency as a third-party vendor)***. In those circumstances, what do you view as the best path for pixel providers to comply with the requirement to have a contract in place with those publisher "businesses" who "sell" or "share" personal information to them as "third parties" via ad creative delivered to the publisher page?**



Base: Percent of Responses 100%

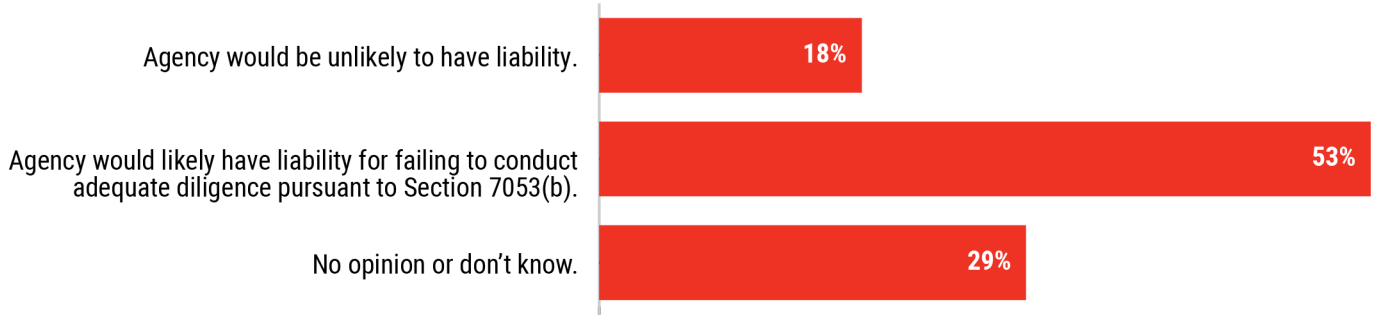
Q9: Publishers are obligated to effectuate consumer opt-outs under each state privacy law. This includes effectuating opt outs with respect to pixels that fire in the ad creative when they cause a "sale," "share," or "targeted advertising." The CPRA also requires a contract with certain privacy protective provisions to be in place between publishers and third-party pixel providers when publishers "sell" or "share" personal information to them through the ad creative.

What liability, if any, could agencies have when including those pixels in the ad creative on behalf of advertisers and not ensuring that publishers have contracts with the pixel providers? *(Select all that apply.)*



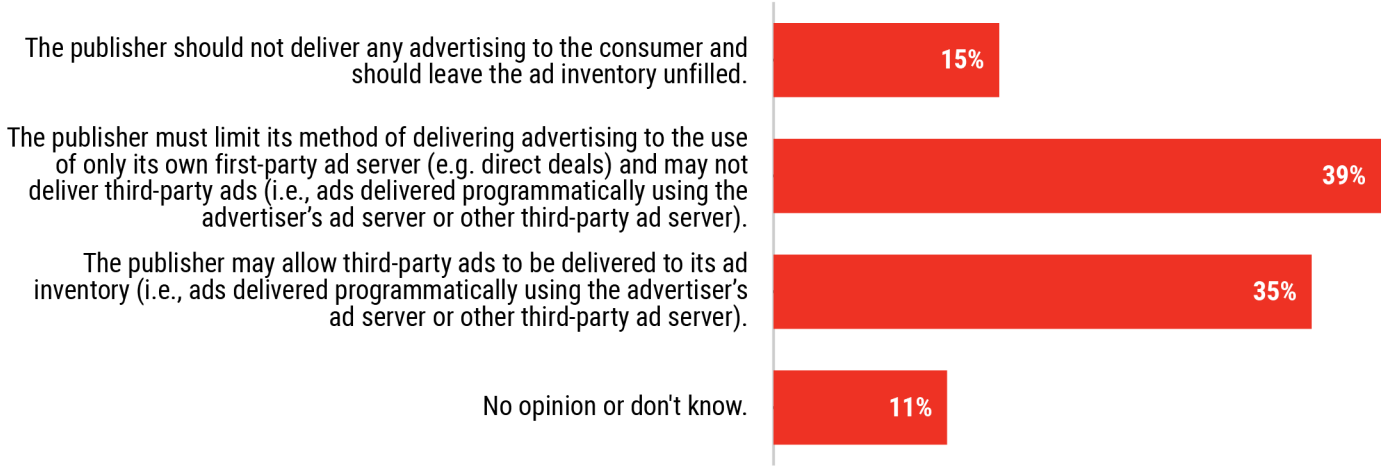
Base: Percent of Responses >100%

Q10: Publishers are obligated to effectuate consumer opt-outs under each state privacy law. This includes effectuating opt outs with respect to pixels that fire in the ad creative when they cause a "sale," "share," or "targeted advertising." The CPRA also requires a contract with certain privacy protective provisions to be in place between publishers and third-party pixel providers when publishers "sell" or "share" personal information to them through the ad creative. What liability, if any, could agencies have when including those pixels in the ad creative on behalf of advertisers and not ensuring that publishers have means of effectuating opt-outs in the ad creative?



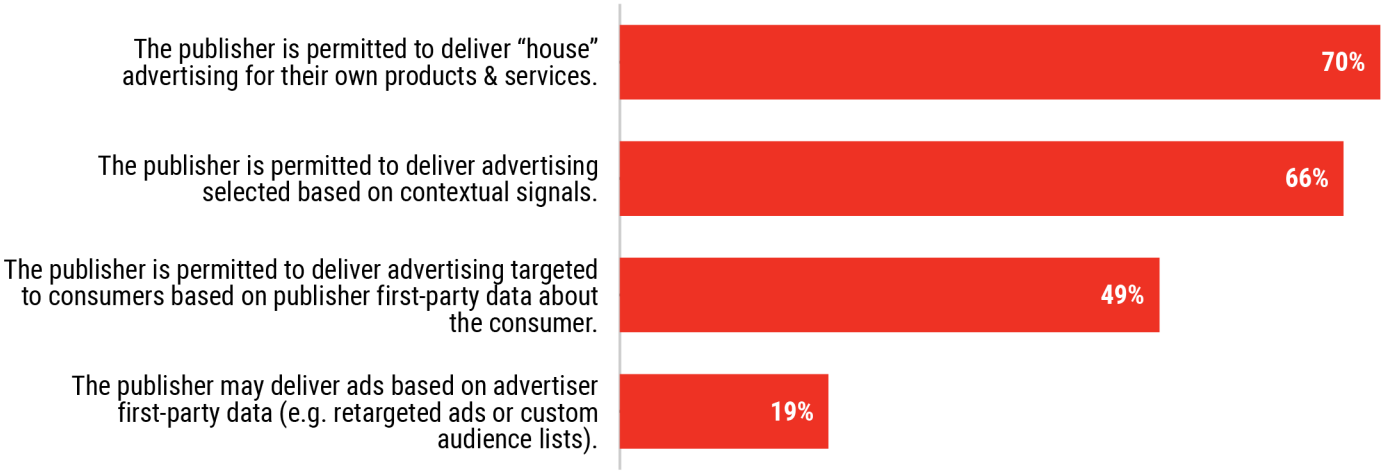
Base: Percent of Responses 100%

Q11: After a publisher receives a valid consumer request to opt out of "sales" and "sharing"/"targeted advertising," that publisher generally must not deliver ads based on information collected across contexts *(e.g. "targeted advertising" or "cross-context behavioral advertising" under applicable state privacy laws)***. Which of the following best describes the types of ad delivery methods you believe that publishers can still lawfully use to deliver ads to the opted-out consumer, assuming the ad is selected without using cross-context data?**



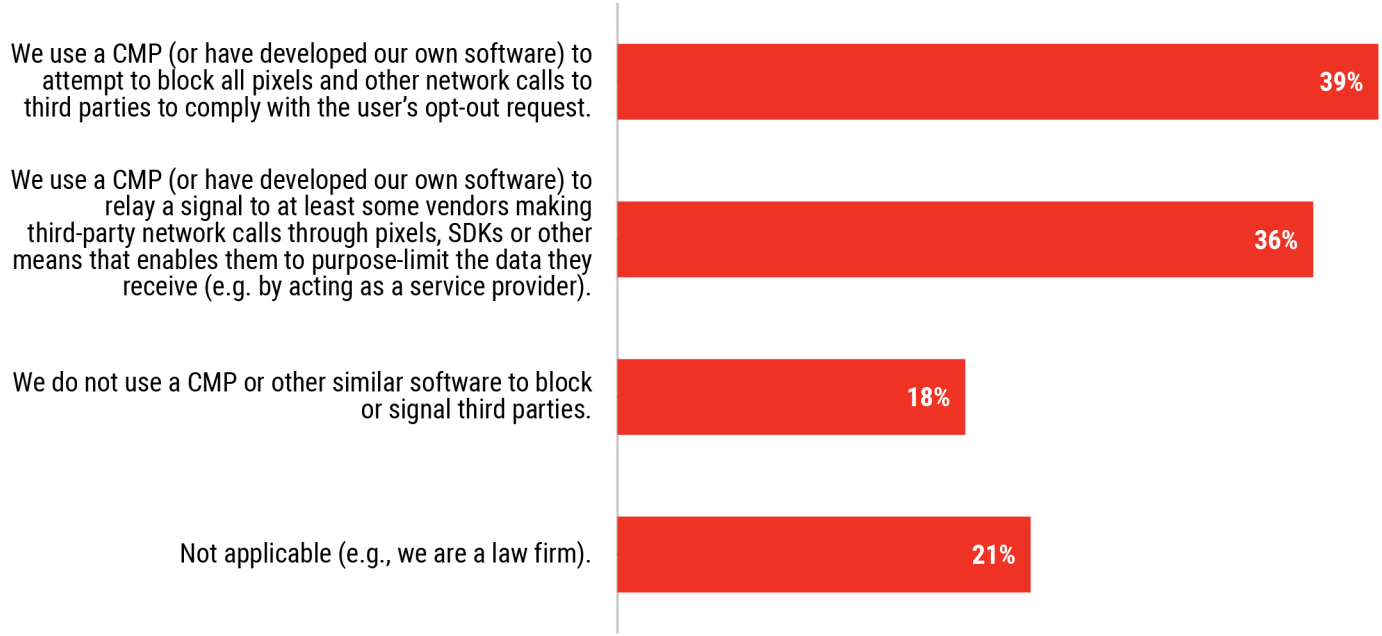
Base: Percent of Responses 100%

Q12: After a publisher receives a valid consumer request to opt out of "sales" and "sharing"/"targeted advertising," that publisher generally must not deliver ads based on information collected across contexts *(e.g. "targeted advertising" or "cross-context behavioral advertising" under applicable state privacy laws)***.What types of advertising do you believe that publishers can still lawfully deliver to the opted-out consumer? Select all that apply in terms of ad selection:**



Base: Percent of Responses >100%

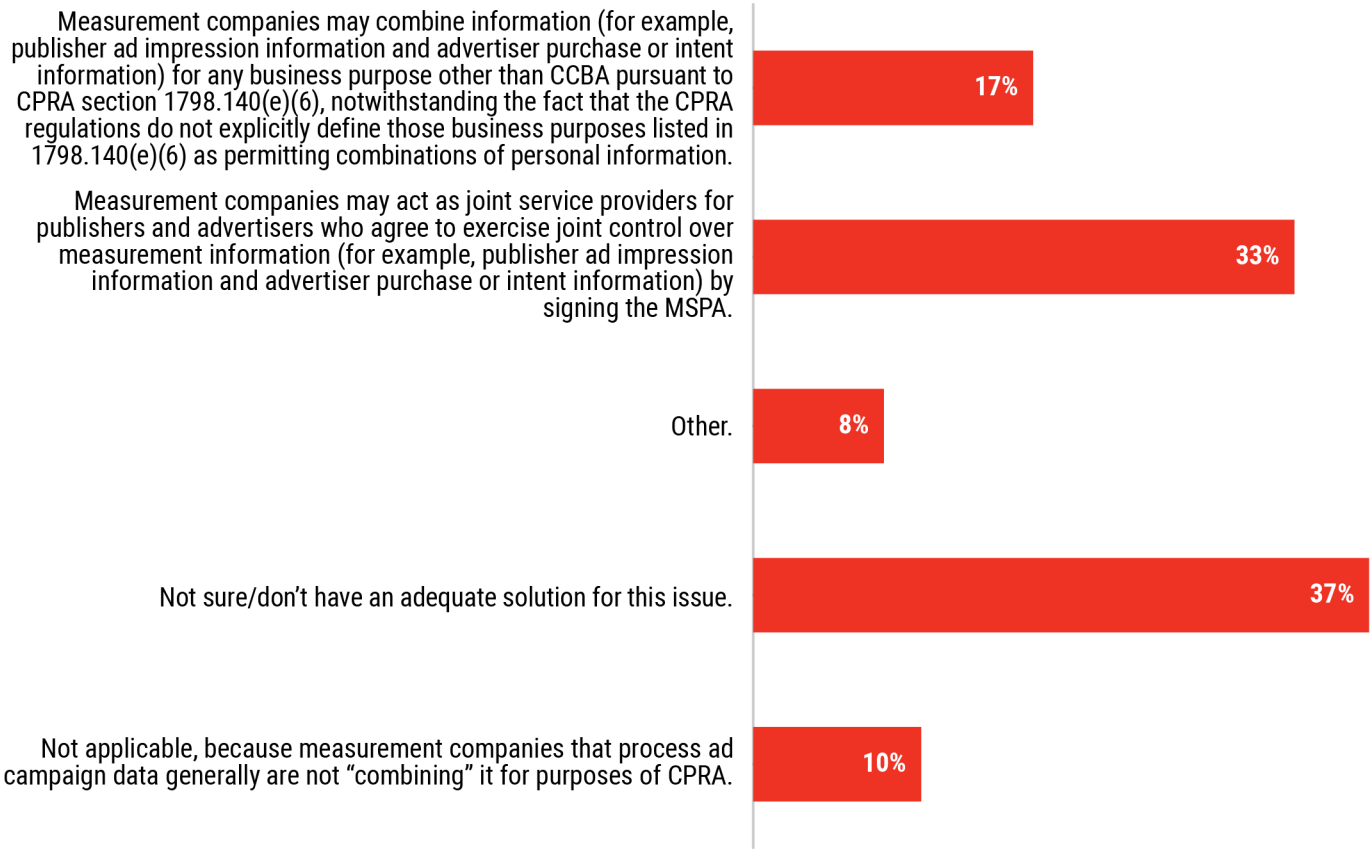
Q13: With respect to network requests sent after a user opts out of sales/share/targeted advertising: *(Select all that apply.)*



Base: Percent of Responses >100%

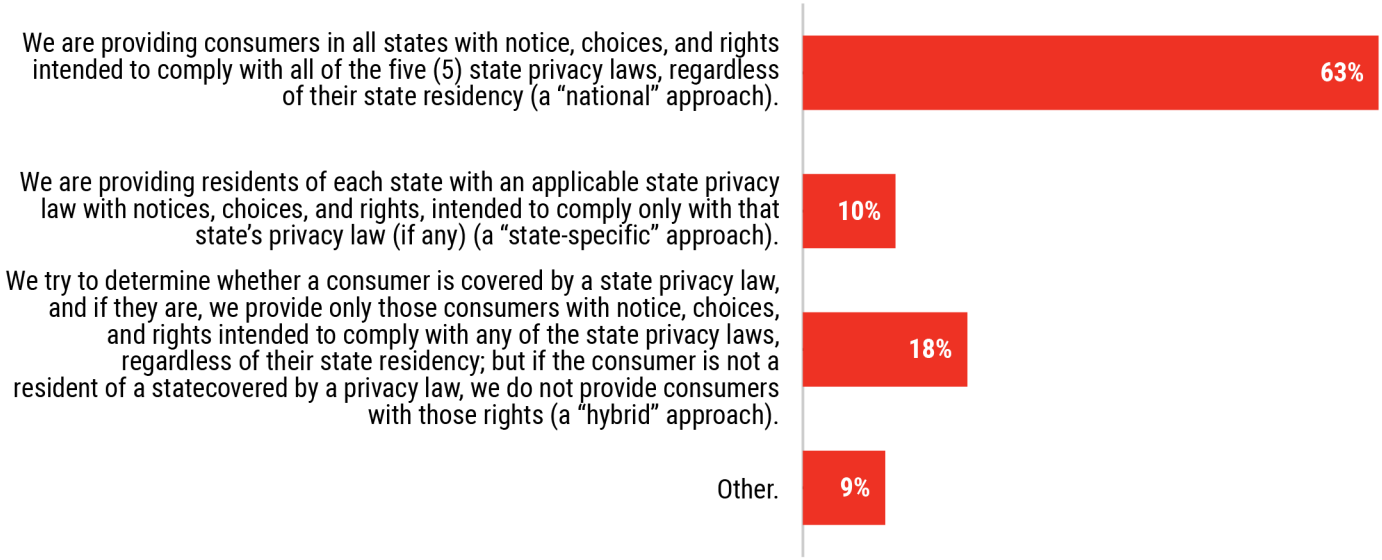
Q14: The CPRA prohibits a service provider or contractor from "combining" personal information that it receives from or on behalf of the business it is servicing with personal information collected from or on behalf of another person or persons, or from its own interaction with the consumer, except to perform any business purpose as defined the in the CPRA regulations.

In the context of measuring digital ad campaigns, which of the following in your view describes a compliant approach to this restriction? *(Select all that apply.)* **- Selected Choice**



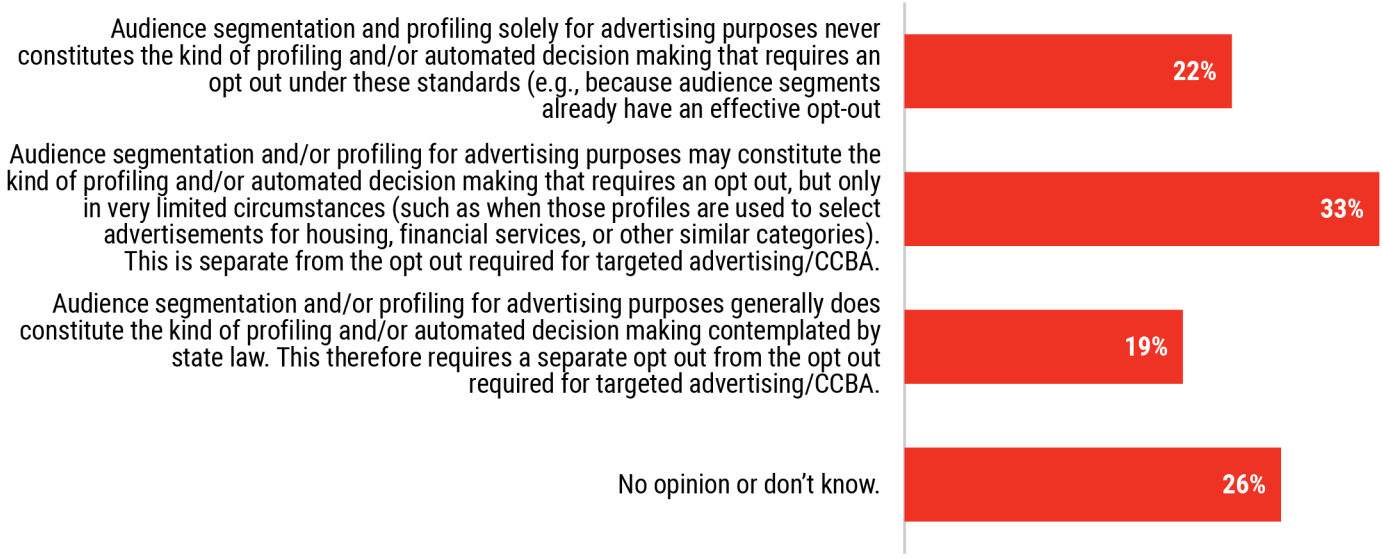
Base: Percent of Responses >100%

Q15: There are 5 state privacy laws coming into effect in 2023 *(California, Virginia, Connecticut, Colorado, and Utah)***. With respect to your creation of a multi-state compliance program, what best describes your approach** *(or if you are a law firm, what do you see your clients typically choosing)***: - Selected Choice**



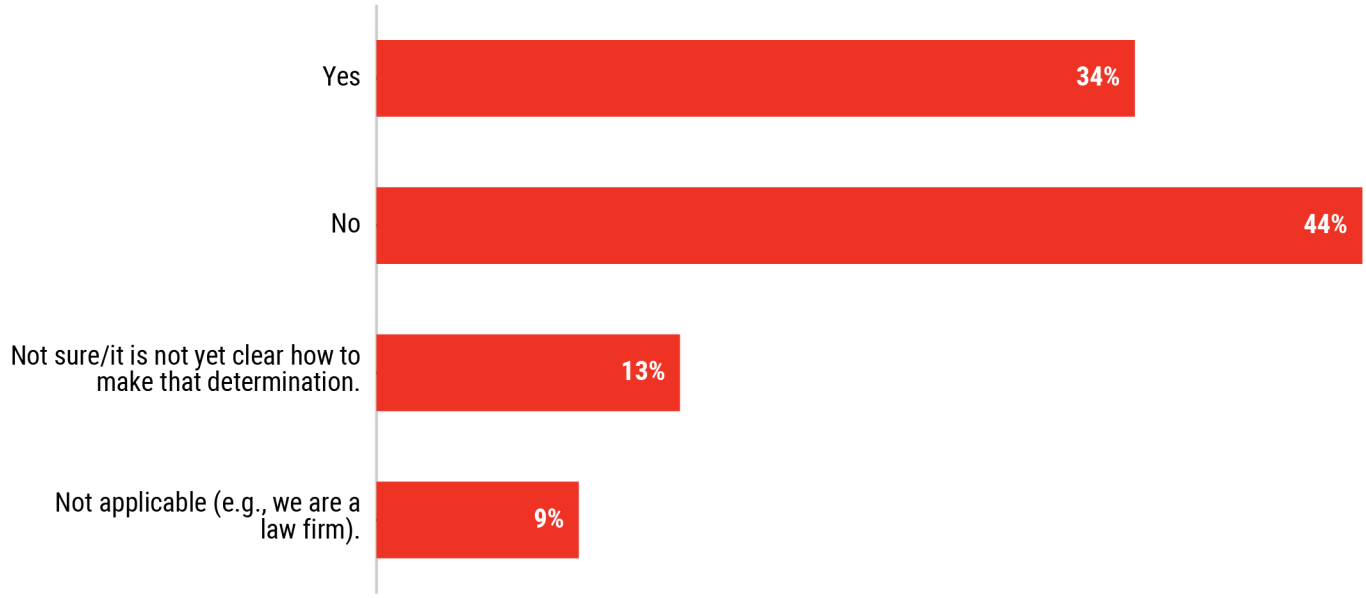
Base: Percent of Responses 100%

Q16: Some state laws include a right to opt out of profiling and/or automated decision-making that has a legal or similarly significant effect. What statement best describes your company's position *(or if you are a law firm, the advice you typically provide)* **regarding profiles used for advertising?**



Base: Percent of Responses 100%

Q17: Do you anticipate your company does or will process sensitive personal information, as defined in any of the 5 state privacy laws, in connection with digital advertising activities?



Base: Percent of Responses 100%