iab.

State Privacy Law Survey Results

March 2025

Sponsored by Ketch

Introduction

Participants in the digital advertising industry continue their efforts to comply with 19 comprehensive state privacy laws that are in effect or coming into effect, while also trying to enhance the scale of their compliance programs.

The IAB Legal Affairs Council seeks to improve clarity and consensus around how state privacy laws apply, in practice, to the digital advertising industry. It recently surveyed industry participants across publishers, sell-side and buy-side ad tech companies, agencies, brands, and law firms regarding the implementation of state privacy laws, as well as best practices. The survey posed questions on a wide range of critical topics and practices, including sensitive personal information, data clean rooms, data minimization, secondary use limitation, vendor due diligence, and data de-identification.

Amongst the respondents, 43% are publishers (and some may also provide ad tech services), 17% are advertisers, brands, and their agencies, 27% are ad tech providers, and the rest serve other roles (e.g., law firms, consultants).[1]

The survey results demonstrate that:

- When navigating varying state privacy laws, companies are more inclined to adopt a unified approach instead of a state-specific approach.
- Companies are still grappling with defining the boundaries of sensitive personal information, such as health data and minors' information, but the majority believe that non-sensitive data (e.g., browsing history, language preference) remains non-sensitive unless it is actively used to infer sensitive personal information.
- While the majority of respondents do not believe that data clean rooms can effectively de-identifiy all personal information, the myth that data clean rooms offer a privacy-proof solution that fully de-identifies personal information persists among a small percentage of the market participants.
- The majority of respondents believe that companies using DCRs can perfect a service provider relationship with the DCR. A "sale" occurs between parties leveraging the DCR for campaign planning and profile augmentation.
- For third-party due diligence, the industry primarily relies on questionnaires, favoring those tailored to the digital advertising sector.

[1] Total number of respondents=37.

Survey Results Highlights

SENSITIVE PERSONAL INFORMATION

The industry continues to grapple with defining the boundaries of sensitive personal information, such as health data and minors' information:

- For sensitive personal information under U.S. state laws in general, the majority (78%) believe that non-sensitive data remains non-sensitive unless it is actively used to infer sensitive information. In comparison, a smaller percentage (8%) view certain non-sensitive data (e.g., language preference, ethnic product affinity) as inherently sensitive because it serves as a proxy for sensitive information.[2] The majority (78%) think opt-in consent is needed (when applicable under U.S. state privacy laws) when inferring sensitive personal information from non-sensitive personal information.[3]

- For the Washington My Health My Data Act,[4] survey results reveal that 38% believe browsing history related to health topics is "Consumer Health Data," while 46% consider it so only if the data is used to generate or target consumer segments with health conditions.[5]

- Respondents who conduct targeted advertising based on minors' data (40%) tend to take a national approach (32%) that meets the highest age standard across all states instead of adopting a state-by-state approach (8%).[6]

DATA MINIMIZATION AND SECONDARY USE LIMITATION

The digital advertising industry remains uncertain about the types of digital advertising permitted under Maryland's Online Data Privacy Act (MODPA).[7] The law restricts the collection of personal data to what is reasonably necessary and proportionate for providing or maintaining a specific product or service requested by the consumer. Overall, respondents see a greater level of uncertainty around the types of advertising permitted under the MODPA. For example, 46% of the respondents stated that a publisher's and advertiser's collection of personal information can be used for first party advertising. A lower percentage of respondents stated that publisher's and advertiser's collection of personal information can be used for targeted advertising (i.e., 35% for publishers, and 27% for advertisers).[8]

[2] See survey result to Q5.

[3] See survey result to Q6.

[4] Wash. Rev. Code § 19.373 et seq.

[5] See survey result to Q7.

[6] See survey result to Q8.

[7] Md. Code, Com. § 14-4701 et seq.

[8] See survey result to Q4.

Regarding secondary use limitations for non-sensitive personal information, most respondents (68%) follow the U.S. state privacy law approach, requiring consent if the use was not disclosed in the privacy notice. A few respondents believe consent is needed if the use might surprise consumers, even if disclosed (22%).[9]

DE-IDENTIFICATION

43% of respondents use de-identification technologies such as perturbation (5%), differential privacy (27%), k-anonymity (19%), and synthetic data (22%).[10] However, 78% do not believe personal information can be de-identified for targeting, profile augmentation, measurement, and analytics use cases. Some respondents explained that, in measurement use cases, the output data may be aggregated and de-identified.[11]

DATA CLEAN ROOMS

The myth persists in a material portion of the market that data clean rooms offer a privacy-proof solution that fully de-identifies personal information. Some believe these platforms can de-identify data for audience profile augmentation (27%), generating measurement and analytics from purportedly de-identified inputs (16%), and campaign planning to enable subsequent targeting based on purportedly de-identified data (27%). The import of such views is that the information processed by these platforms for such use cases purportedly falls outside the scope of U.S. state privacy laws. On the other hand, 49% of respondents do not believe data clean rooms can effectively render personal information de-identified.[12]

The industry believes a DCR can act as a service provider for measurement, analytics (57%),[13] campaign planning, and profile augmentation (51%)[14] use cases and considers that personal information is "sold" between the collaborating parties. When asked slightly differently, respondents generally have more confidence that a service provider relationship can be perfected with the DCRs in measurement and analytics use cases (70%), but are less confident for profile augmentation (41%) and campaign planning (43%) use cases. 24% of the respondents consider data to be "sold" when shared with DCRs and treat them as "third parties" under state privacy laws.[15]

[9] See survey result to Q9.

[10] See survey result to Q11.

[11] See survey result to Q10.

[12] See survey result to Q12.

[13] See survey result to Q13.

[14] See survey result to Q14.

[15] See survey result to Q15.

THIRD-PARTY DUE DILIGENCE

Respondents stated they primarily rely on surveys and questionnaires that are either generic (35%) or tailored to the digital advertising industry (51%). Some engage assessors to understand outbound data flows (30%). Only a small percentage require additional technical proof to demonstrate data privacy promises are upheld.[16] When asked to assess how well their current approach meets third-party due diligence requirements under state privacy laws (e.g., Cal. Civ. Code 1798.135(g), 145(i), and C.R.S. § 6-1-1309), 81% of respondents rated it between 3 and 4 on a 5-point scale (5 means "high capacity.")[17]

OTHER AREAS

Companies continue to fend off rampant wiretapping lawsuits with a combination of varying tactics, including prominent disclosure in chatbots (59%), in search bars (30%), and deploying cookie consent banners (43%).[18]

Companies are also taking measures to avoid "dark patterns." Some have reviewed and revised all their consent-obtaining mechanisms for the collection of personal information (38%), some are in the process of doing so (27%), and certain are waiting on additional regulatory guidance (14%).[19]

Under the Oregon Consumer Privacy Act,[20] consumers can request a list of third parties that have received their personal data. Companies may choose to disclose either (1) all third parties receiving any consumer's data or (2) those receiving a specific consumer's data. Most opt for the first approach (70%).[21] Additionally, 81% of respondents limit disclosure to direct recipients (one-hop) rather than including indirect recipients (multi-hop).[22]

When asked to predict the future, considering the recent litigation, enforcement, and regulatory trends, the majority of the respondents (59%) believe the compliance landscape is going through seismic changes and the U.S. is essentially moving towards an opt-in regime even if the state privacy laws adopt an opt-out regime.[23]

[16] See survey result to Q6.

[17] See survey result to Q17.

[18] See survey result to Q18.

[19] See survey result to Q19.

[20] ORS 646A.570 et seq.

[21] See survey result to Q1.

[22] See survey result to Q2.

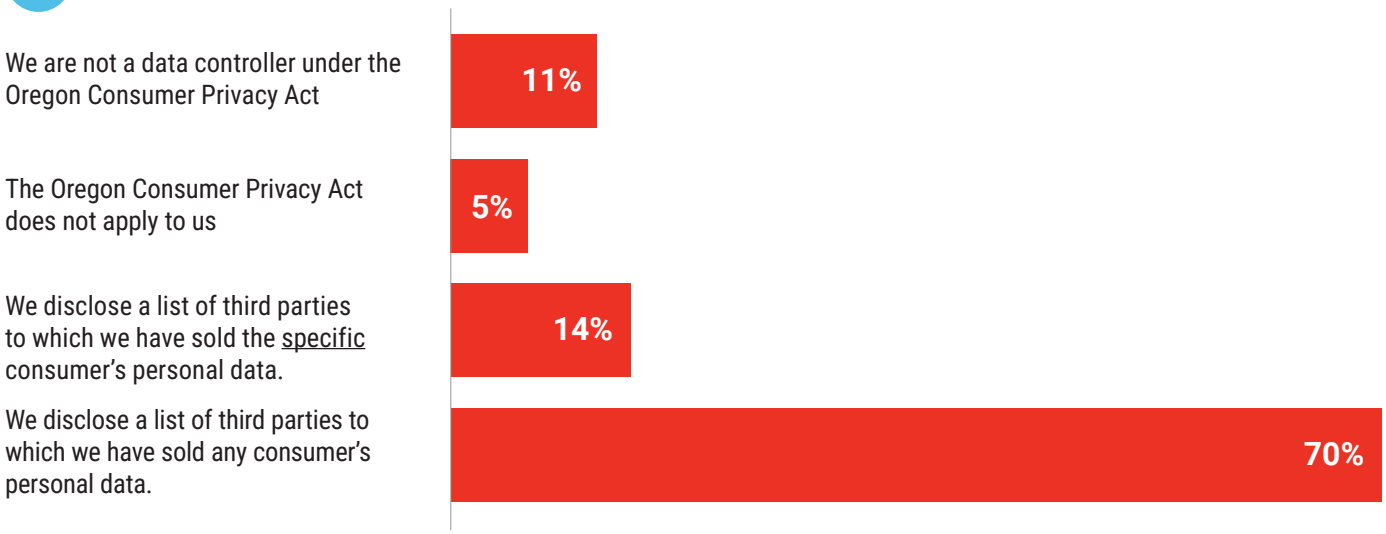
[23] See survey result to Q20.

Survey Results

STATE-SPECIFIC REQUIREMENTS

Under the **Oregon Consumer Privacy Act,** Consumers have the right to know, upon request, the specific third parties that have received their personal data or any personal data from a controller. *(See ORS 646A.574(1)(a)(B))*. Please choose answers to questions 1 and 2 that most closely align with your company's approach.

Q1 Upon consumer requests, which approach to disclosures do you take?



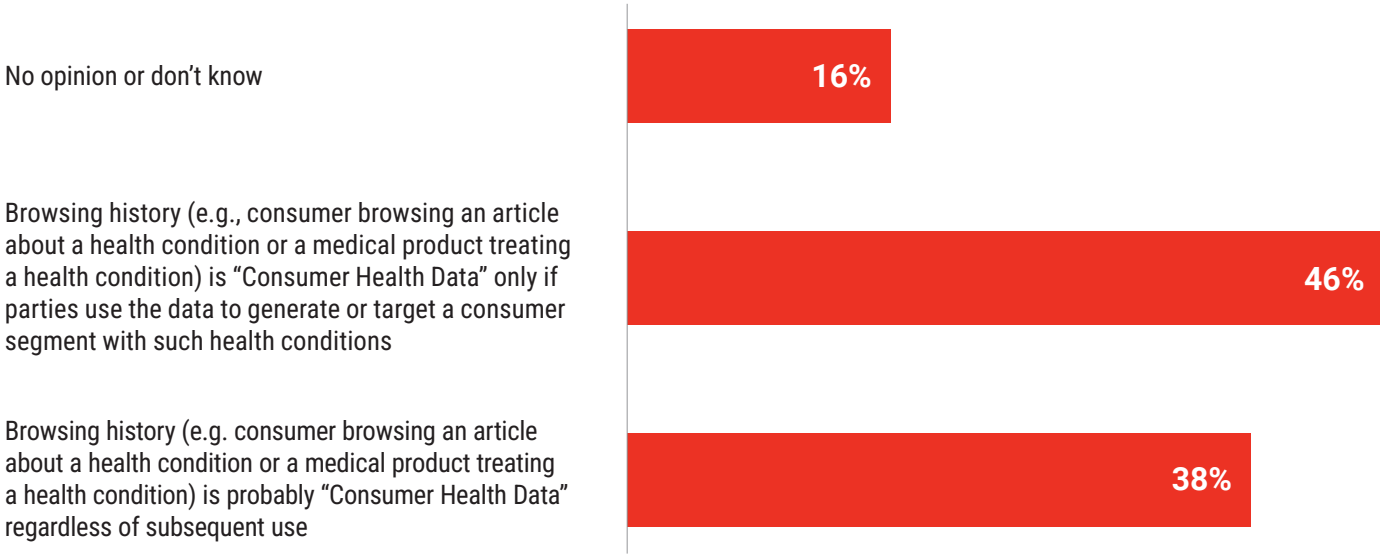
Single-select question: responses total 100%

Q2 In connection with Q1, what types of entities do you, or would you, include in the third-party list?

Single-select question: responses total 100%

Washington My Health My Data Act (WA MHMD) has a broad definition of "Consumer Health Data" that includes "personal data that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

Q3 Which statement below do you believe is true about the scope of "health data" under the WA MHMD?



Single-select question: responses total 100%

Maryland's Online Data Privacy Act (MODPA) prohibits selling personal data and limits the collection of personal data (as defined under MODPA) to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains. *(14-4607(B)(1))* The Act also requires the secondary use of personal data to be reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed. *(14-4607(A)(8))*

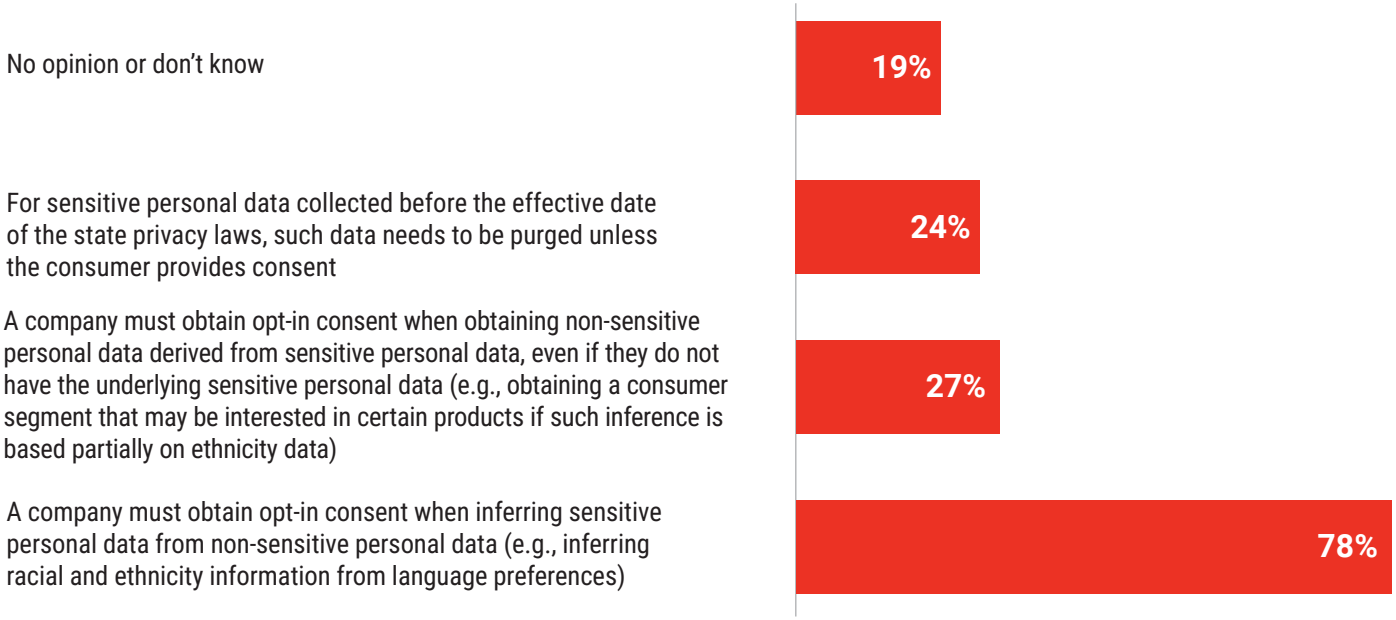
Q4 MODPA: Which statement(s) below are aligned with your view if only non-sensitive personal data is involved? Select all that apply.

Multi-select question: % out of total # of responses, %s cannot be added together.

SENSITIVE PERSONAL DATA

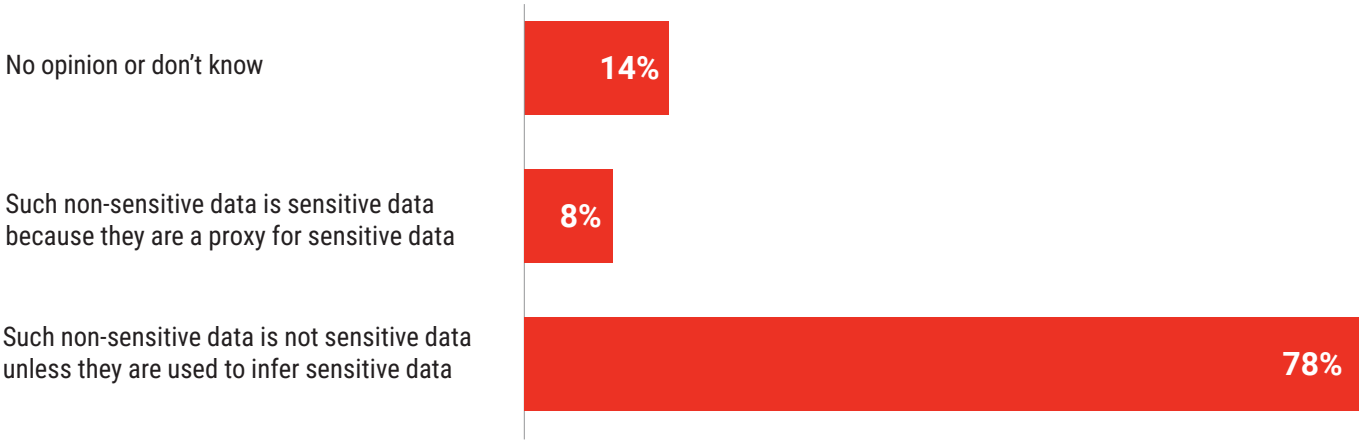
Sensitive personal data are subject to heightened requirements under the state privacy laws.

Q5 If an individual is a resident of a state that requires opt-in consent for collective sensitive personal data, which statement(s) align with your view? Select all that apply.



Multi-select question: % out of total # of responses, %s cannot be added together.

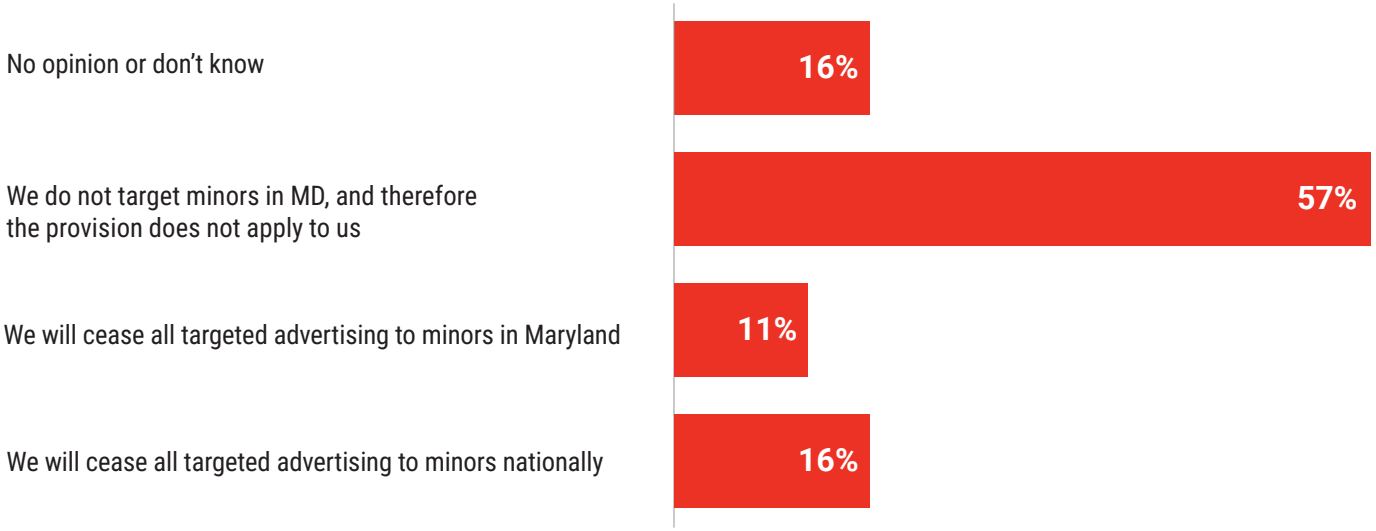
Q6 For certain non-sensitive data (e.g., language preference, ethnic product affinity) that can be used to infer sensitive personal data, which statement is true based on your view?



Single-select question: responses total 100%

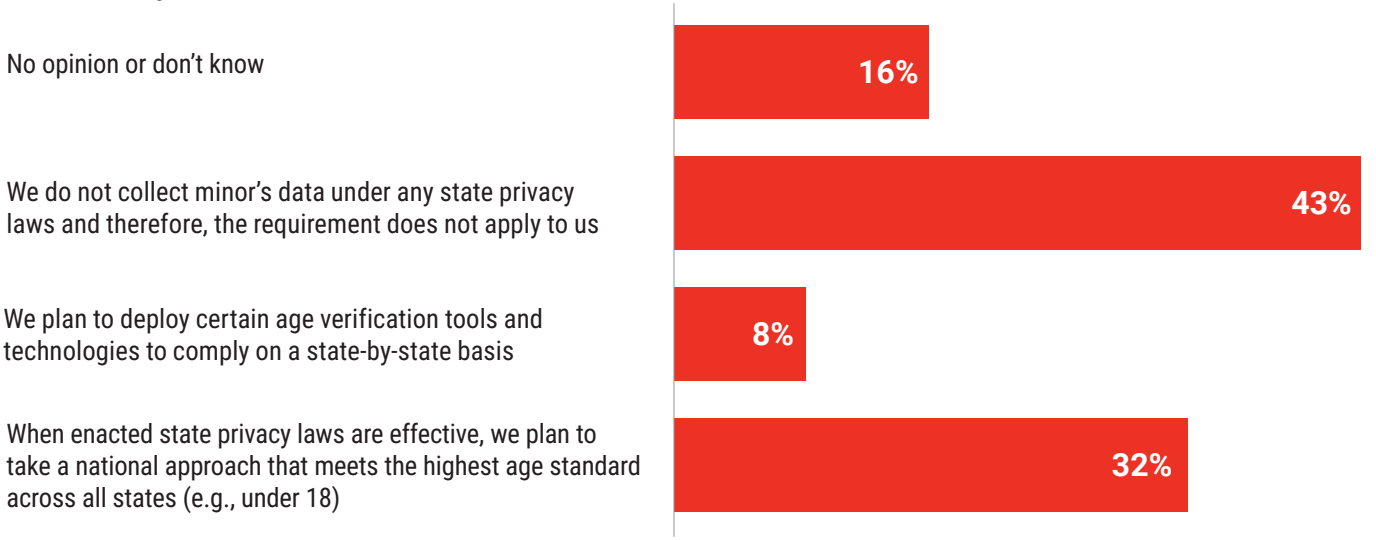
MINOR'S DATA

Q7 Maryland's Online Data Protection Act (MODPA) prohibits controllers from processing or selling minor's data for the purpose of targeted advertising when the controller knows, or should have known, that the personal information pertains to a minor. Which statement below is aligned with your view on complying with MODPA?



Single-select question: responses total 100%

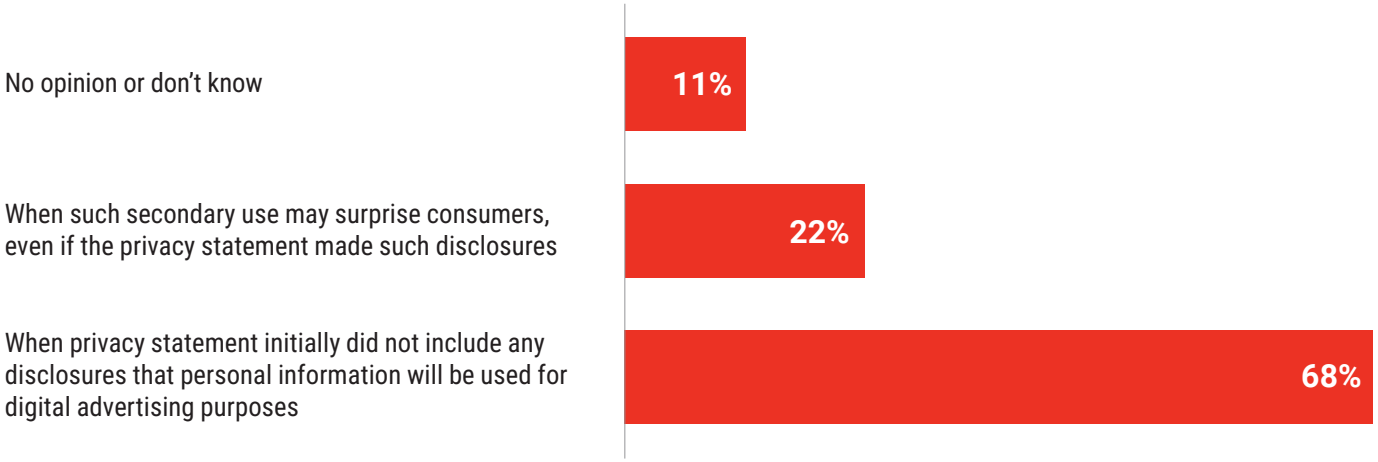
Q8 Minor's data are often treated as sensitive personal data under state privacy laws and are subject to different levels of protection. Different states adopt varying definitions of minor's data, whereby certain states adopt a definition aligned with that of COPPA, while other states extend it to up to 18 years of age. Which statement below is aligned with your view?



Single-select question: responses total 100%

SECONDARY USE LIMITATION REQUIREMENT

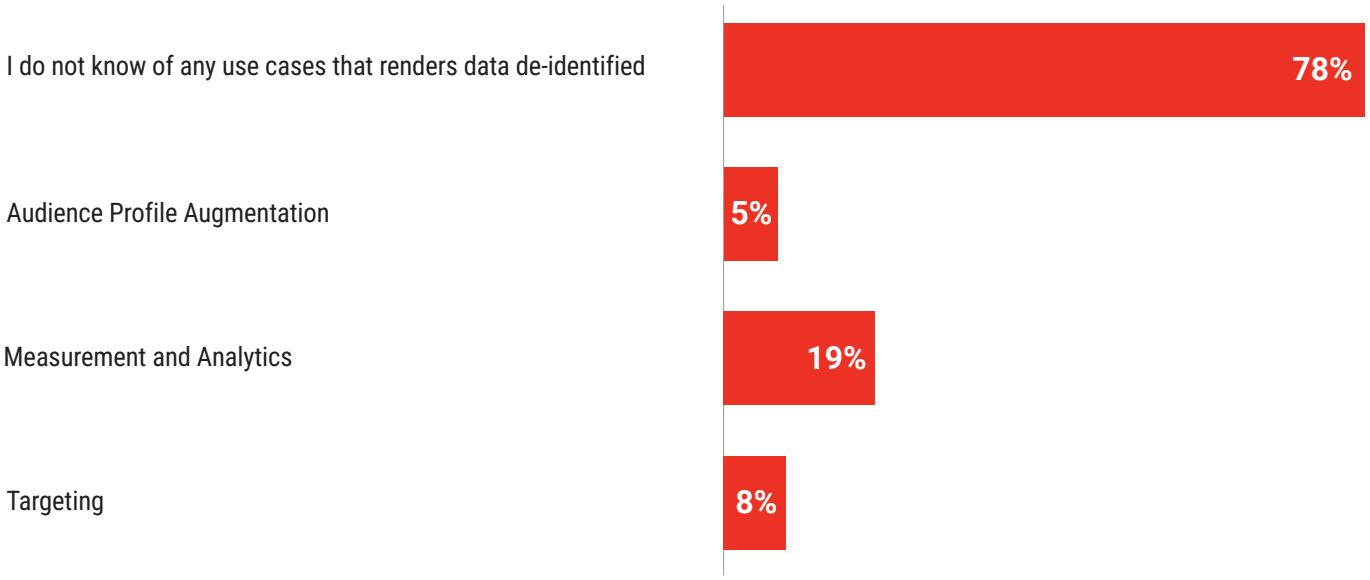
Q9 **The majority of the U.S. state privacy laws state a controller is only permitted to process personal data for purposes that are reasonably necessary to or compatible with the specified purposes for which the personal data are processed as disclosed unless the controller first obtains the consumer's consent** *(see, e.g., C.R.S. § 6-1-1308(3)).* **When do you believe such consent is necessary in situations where sensitive personal data is not involved?**



Single-select question: responses total 100%

DATA DE-IDENTIFICATION

Q10 Aside from the disclosure of information in an aggregated report, do you believe that deidentifying personal data is reasonably achievable and practical in the following use case among today's digital industry practices?



Multi-select question: % out of total # of responses, %s cannot be added together.

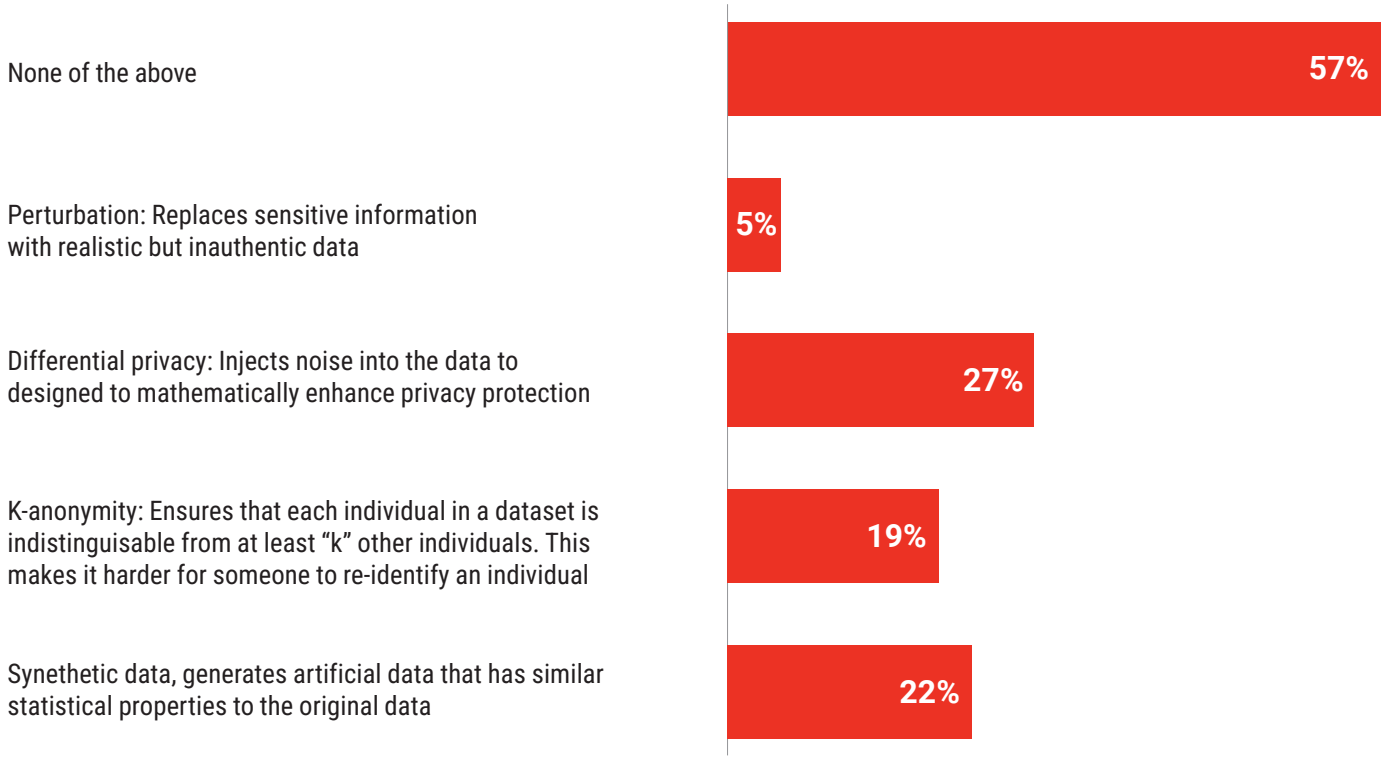
The survey question offers options to provide free text responses to provide more context for their choices.

Respondents selecting "targeting" believe personal data could be deidentified for such use case because: (1) "deident[i]fying data here would not allow for targeting of specific devices. Pseudonymous data is a close second. The end result here would likely be contextual targeting;" (2) "if an audience is built by a third party with no knowledge of individuals and no information is attributed to such individuals as part of the building process," and (3) "internal solution."

Respondents choosing "measurement" believe personal data could be deidentified for such use case because (1) "for high volume traffic, you could slice this data a number of ways and still get very valuable insights, including what customer behavior patterns most often correlate to engagement and conversion;" (2) "tokens;" (3) "when aggregated reports are created for measurement and analytics;" (4) "internal solution;" and (5) "targeting based on cohorts/differential privacy."

The respondent choosing "profile augmentation," however, doesn't appear to believe personal data could be deidentified for such use because the response stated: "deidentified data may not provide the value and insights needed for profile augmentation."

Q11 What technologies do you current use or in the near future plan to use to de-identify data under the U.S. State Privacy Laws?



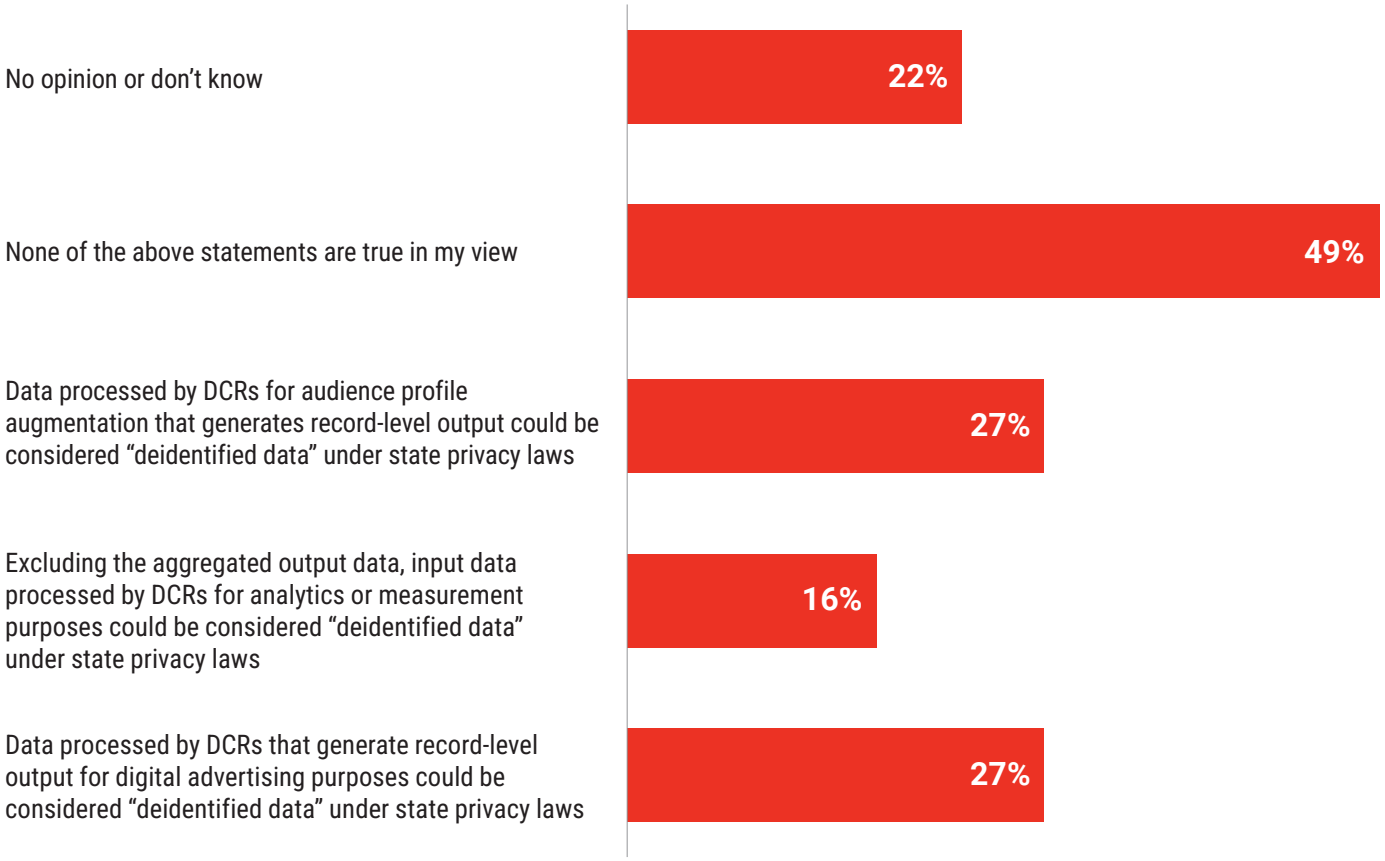
Multi-select question: % out of total # of responses, %s cannot be added together.

DATA CLEAN ROOM

A data clean room (DCR) is a controlled environment that enables multiple companies or divisions of a company to bring data together for various purposes, such as retargeting, analytics, measurement, or audience profile augmentation. Privacy-enhancing technologies, such as encryption or hashing, are often applied during data processing.

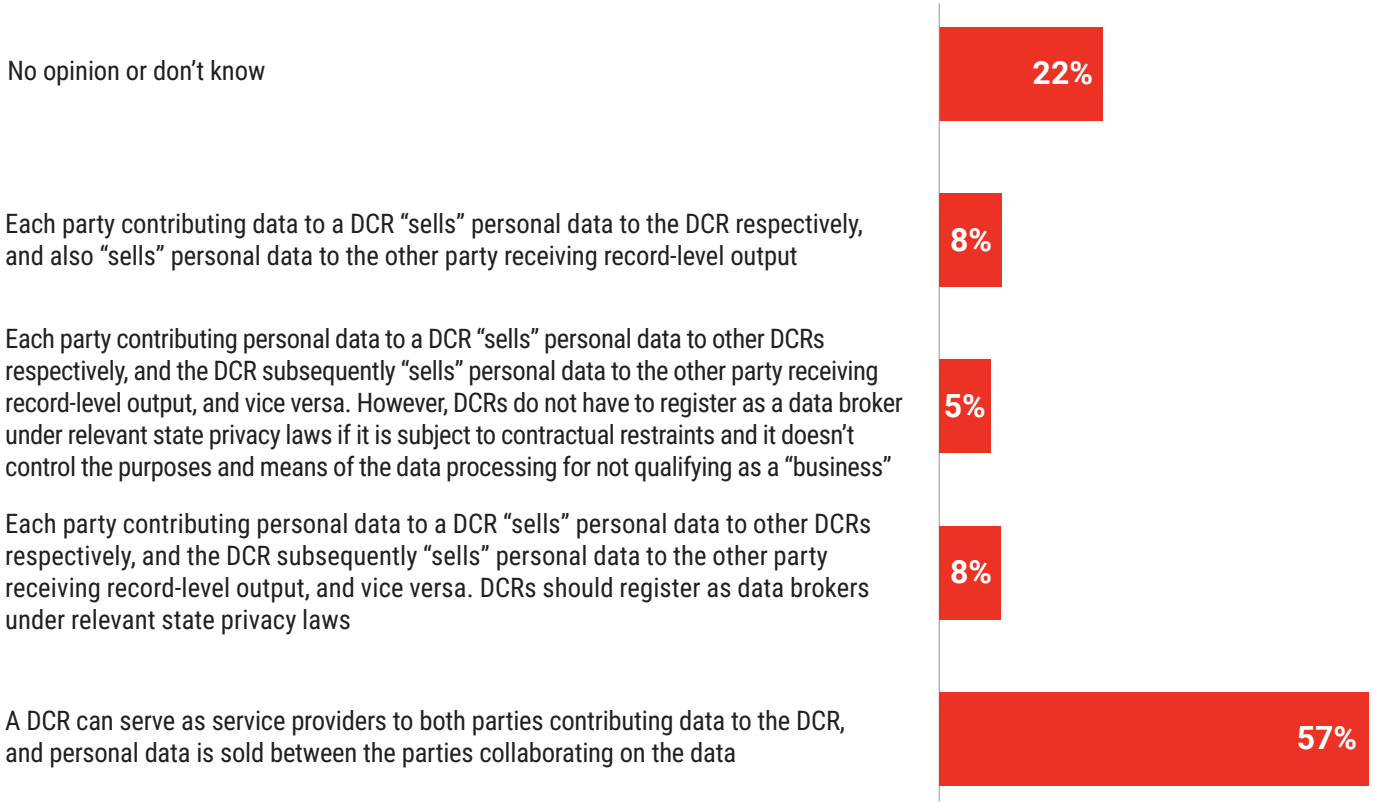
For instance, DCRs can be used for one or more use cases below: (1) **Analytics**. Parties may get aggregated report output such as customer overlapping analysis. A party may use the analytics to determine whether to collaborate with the other party for subsequent advertising purposes; (2) **Campaign Planning and Retargeting.** Parties may use the individual record level output for retargeting purposes; (3) **Audience Augmentation and Profile Enrichment.** Parties may obtain enhanced customer profile information, such as record level output regarding customer affinity group (e.g., record X is a sports.com reader), and (4) **Measurement.** A party may obtain measurement data, such as frequency/lift analysis.

Q12 What statements are aligned with your understanding of data clean rooms? Select all that apply.



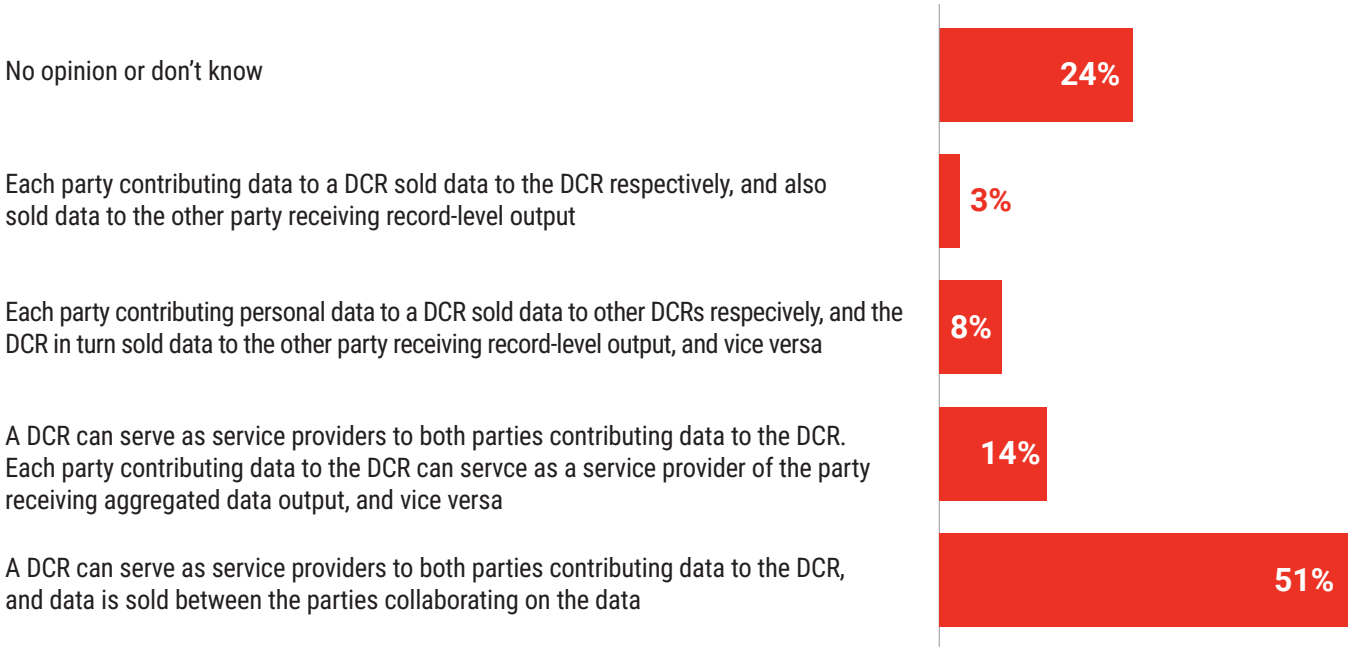
Multi-select question: % out of total # of responses, %s cannot be added together.

Q13 If data processed by a DCR is considered "personal information" or "personal data" for digital advertising or audience profile augmentation purposes that generate record-level output, what statement mostly aligns with your understanding of parties' roles under the state privacy laws?



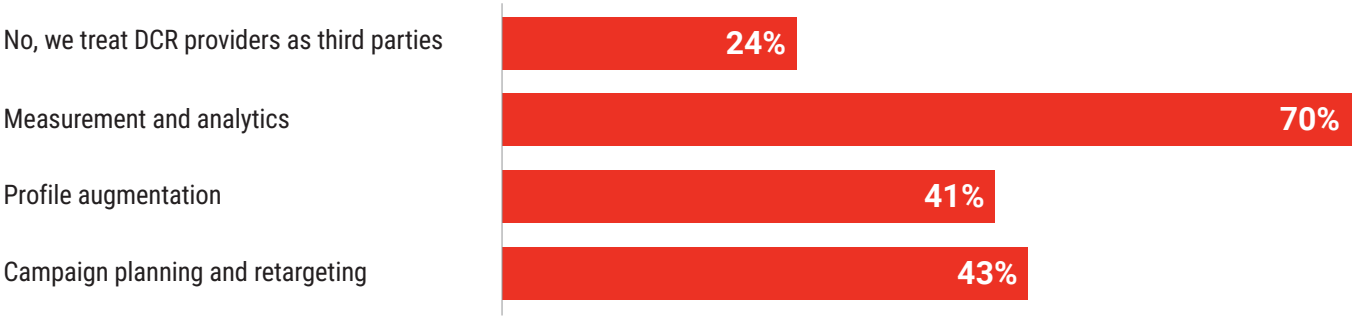
Single-select question: responses total 100%

Q14 If data processed by DCR is considered "personal information" or "personal data" for measurement and analytics purposes that generate aggregated results, what statement is mostly aligned with your understanding of parties' roles under the state privacy laws?



Single-select question: responses total 100%

Q15 What use cases, if any, do you believe parties collaborating on their data may perfect a Service Provider relationship with the DCR provider? Select all that apply.

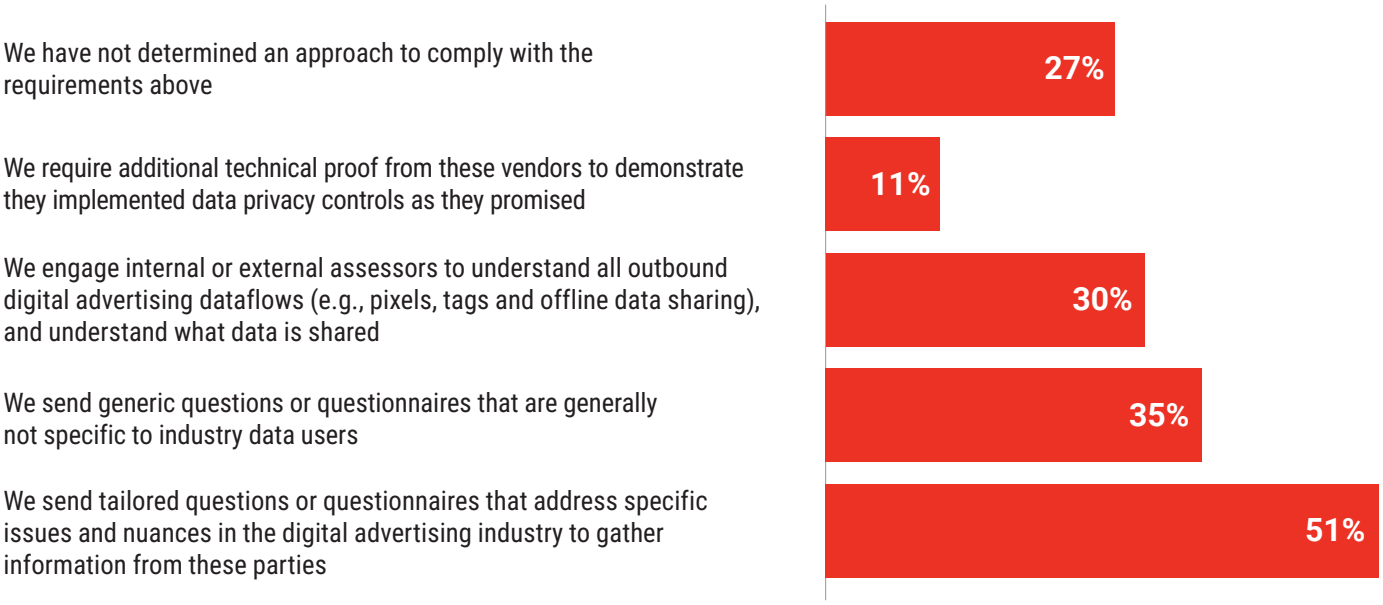


Multi-select question: % out of total # of responses, %s cannot be added together.

VENDOR DUE DILIGENCE

The CCPA and its implementing regulations require businesses to conduct due diligence of their service providers, contractors and third parties to avoid potential liability for the acts of those entities *(see Cal. Civ. Code 1798.135(g), 145(i))*. Most other state privacy laws require similar diligence of processors. Additionally, most state privacy laws require covered companies to conduct data protection impact assessment for digital advertising. *(See, for example, C.R.S. § 6-1-1309).*

Q16 Which of the following is most closely aligned with your company's current approach to conducting third party due diligence to obtain information to comply with the requirements? Select all that apply.



Multi-select question: % out of total # of responses, %s cannot be added together.

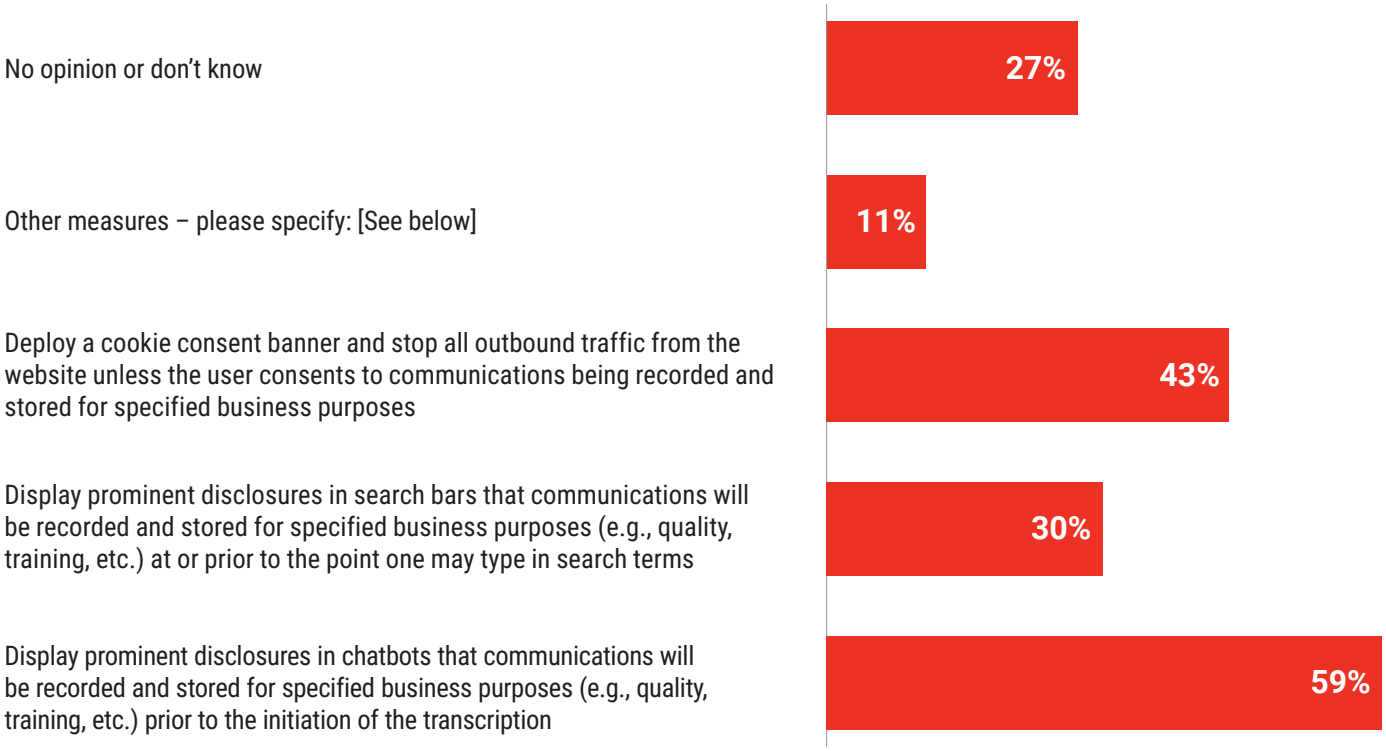
Q17 On a scale of 1 to 5, rate how capable you believe your approach above would meet the aforementioned third party due diligence requirements. *See e.g., Cal. Civ. Code 1798.135(g), 145(i) and C.R.S. § 6-1-1309).* (Note: A rating of 1 means low capability and 5 means high capability):

Single-select question: responses total 100%

STATE WIRETAPPING LITIGATION

The last several years have brought a wave of lawsuits alleging that the use of session cookies, certain tracking pixels, AI assisted call centers, and chatbots result in the interception of communications in violation of federal and state wiretapping laws.

Q18 Which measures below do you believe are effective and practice strategies to deter these litigations? Select all that apply.



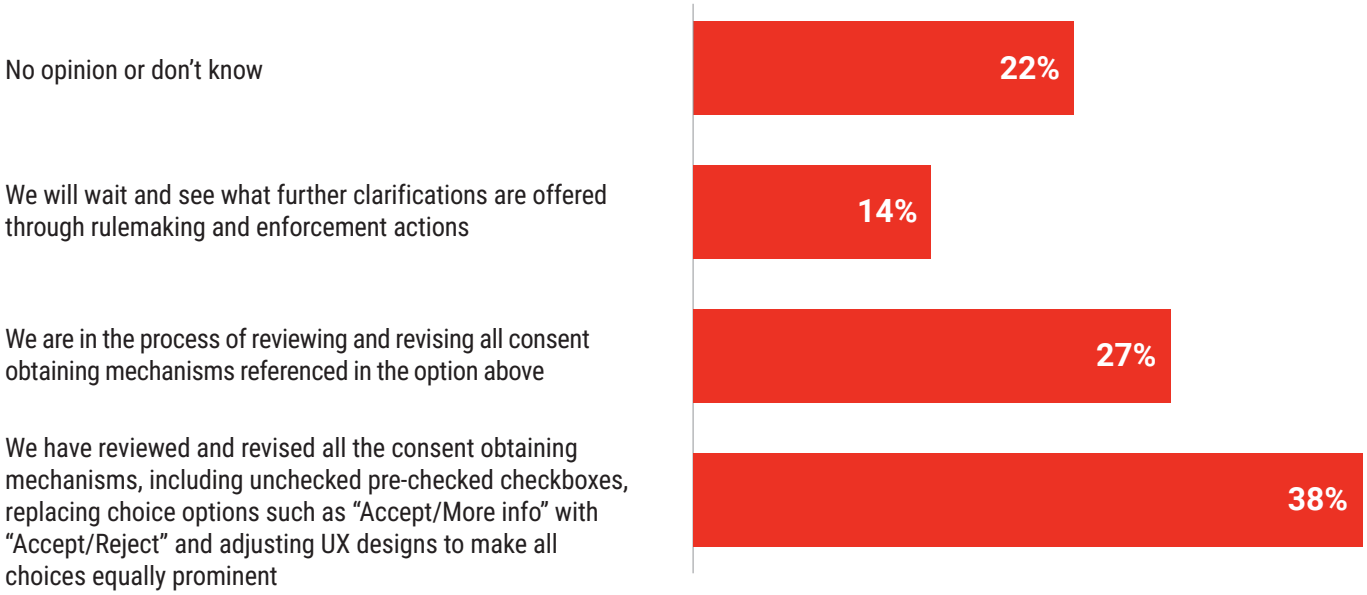
Multi-select question: % out of total # of responses, %s cannot be added together.

The survey question offers options to provide free text responses if they adopt other measures not listed in the existing options. These respondents stated: (1) "clear and explicit disclosures in privacy policies; clear and enforceable forced arbitration clause in terms of service;" (2) "cookie banner - without opt-in consent - may still be an effective measure to deter plaintiff's lawyers. Also effective arbitration provisions in the website terms of use can make sites a less attractive target;" (3) "display general cookie notice banner;" and (4) "ideally, the data collector would obtain affirmative consent."

DARK PATTERNS

Many state privacy laws explicitly prohibit controllers from obtaining consent to collect, use or share personal information through dark patterns, including CCPA in California, the Colorado Privacy Act and the Connecticut Data Privacy Act.

Q19 Many state privacy laws explicitly prohibit controllers from obtaining consent to collect, use or share personal information through dark patterns, including CCPA in California, the Colorado Privacy Act and the Connecticut Data Privacy Act. Which statement is aligned with your current company's approach?



Single-select question: responses total 100%

Q20 Do you believe the U.S. is essentially moving towards an opt-in regime even if the state privacy laws adopt an opt-out regime?

Single-select question: responses total 100%