



State of Data 2023

Data Clean Rooms & the Democratization of Data in the Privacy-Centric Ecosystem

SPONSORED BY:



January 24, 2023

Table of Contents

Foreword	3
Five Things You Need to Know	4
Executive Summary	5
Privacy-Preserving Technology: Adoption and Usage	7
Data Clean Rooms: Hurdles and Opportunities for Growth	17
Privacy-Preserving Technology: Considerations and Best Practices	27
Data Clean Rooms: Understanding the Benefits and Use Cases	33
Appendix	36
Data Clean Room Privacy Controls and Methods to Protect Consumer Data	
Evaluation Phase: Additional Factors for Consideration	
Methodology	
Respondent Profile	
About IAB	
About the IAB Measurement, Addressability, and Data Center	
About Ipsos	
About Our Sponsors	
A Perspective From Neustar	

Foreword

As the digital ad industry continues to suffer from signal loss and the evolution of state-level privacy legislation, the demand for privacy-preserving technology that enables critical, data-driven advertising has never been greater.

As part of our **sixth annual State of Data** initiative, **IAB** has commissioned Ipsos to examine how data clean rooms (DCRs) and other privacy-preserving technology, including customer data platforms (CDPs), consent management platforms (CMPs), data management platforms (DMPs), and identity solutions are being managed and activated. IAB sought to identify the challenges that ad buyers and sellers are facing when leveraging these technologies.

DCRs* specifically have risen as an essential technology by enabling privacy-compliant data matching and sophisticated cookie-agnostic measurement capabilities across the buy- and sell-sides, and therefore mitigating concerns that data decision-makers have had with other privacy-preserving technology.

The introduction of five new state-level, data privacy regulations in 2023 combined with the continued protection of consumer data by leading technology platforms only further raises the value of DCRs. Indeed, Gartner predicts that by 2023 80% of advertisers spending more than \$1 billion annually on media will use DCRs.

A survey of 200 data decision-makers at brands, agencies and publishers, and 20 in-depth interviews reveals that the industry is leveraging DCRs primarily for data privacy protection, especially when shared with external partners.

Although some companies leverage the capabilities that DCRs offer beyond privacy, most are not using the advanced measurement capabilities. **In fact, most data leaders are only scratching the surface with their current use of DCRs and are missing an opportunity to leverage the technology's most powerful advanced measurement capabilities.**

This report, the **IAB State of Data 2023: Data Clean Rooms and the Democratization of Data in the Privacy-Centric Ecosystem** provides ad buyers and sellers, as well as providers of privacy-preserving technology, actionable insights regarding onboarding and adoption, use cases, challenges, and opportunities moving forward with DCRs and other privacy-preserving technology.

The insights from this report will help determine the standards required to evolve the space by determining the data inputs and outputs, as well as the logistical and technical requirements that will ultimately inform the **IAB Tech Lab 2023 DCR initiative**.

This report reveals how we came to these conclusions and provides an action plan on how to prepare for and leverage DCRs.

*DCRs: Secure privacy environments that allow multiple parties to collaborate using proprietary data in compliance with privacy regulations, while allowing each participant to maintain privacy and control of its data.

Source: Gartner per Adweek, [3/16/22](#)

Five Things You Need to Know

1. In the world of privacy-preserving technology, data clean rooms (DCRs) have become an **essential collaboration tool for audience insights, measurement, and data activation in a privacy-centric ecosystem.**
2. While users are primarily leveraging DCRs to mitigate privacy risks and to activate audiences, they're not tapping the full potential of the **technology's advanced measurement capabilities.**
3. Although DCRs offer innovative, privacy-preserving use cases, they are not a turnkey technology—they **require significant investments** in talent, financial resources, and setup, including data infrastructure and connectivity as well as onboarding.
4. DCR requires investments that create a high barrier to entry which puts **smaller industry players including agencies, brands, and publishers at a disadvantage.**
5. It is incumbent upon all data providers, including walled gardens, **to make their data interoperable** so advertisers can measure full campaign effectiveness and ROI.

Executive Summary

1

The increased use of DCRs suggests clear marketplace value in an evolving privacy-centric portfolio. But the industry has not tapped into the technology's full potential.

- Two-thirds (64%) of companies leveraging privacy-preserving technology are using DCRs. This increases to 85% when including those that are considering the technology. Most companies use the technology for vital tasks including privacy protection and controls, match rates, and interoperability.
- Nearly half of DCR users are leveraging the technology for data privacy actions. However, each of the following advanced measurement functions are utilized by less than one-third of users: attribution, ROI/ROAS measurement, media or marketing mix modeling, propensity modeling, and predictive analysis.

2

DCR adoption is not turnkey. Onboarding and activation require significant investment in time, money, and human capital.

- Nearly half of DCR users (49%) have six or more employees dedicated to the technology—nearly one-third (30%) have a minimum of 11 people.
- Respondents cited time-frames of months to up to two years to get up and running with the technology.
- Investment requires six-figure annual budgets:
 - Nearly two-thirds (62%) of users spent a minimum of \$200K on the technology in 2022, with a quarter (23%) spending upwards of \$500K.
 - A 29% increase is expected in 2023.
- This creates an unfair market disadvantage for small agencies, brands, and publishers that don't have the resources to meet these investments.

Executive Summary

3 Although some companies are finding success using DCRs in innovative ways, most are citing significant challenges.

- Qualitative results showed that users are executing more complex tasks including lookalike and propensity model creation, shopper transaction pattern development, and closed-loop attribution.
- However, more than half of DCR users (52%) cite leveraging results/proving ROI as a challenge. About one-third of DCR users are also facing data interoperability / customization (39%), internal resource (38%), and privacy (32%) challenges when using DCRs.

4 Multiple factors are crucial for consideration when evaluating, implementing, and maintaining DCRs and other privacy-preserving technology.

- Data maturity, tracking capabilities, resource burden, interconnectivity, and complexity need to be considered when identifying technology use cases and developing a sequential data strategy.
- Companies must be agile and prepared for ongoing uncertainty caused by multiple state-level privacy legislation and continuous loss of data signals driven by actions from big tech companies and platforms.
- Companies should support, contribute to, and consider adopting industry privacy standards and privacy controls for risk mitigation, including re-identification and data leakage.

**Privacy-Preserving
Technology:
Adoption and Usage**

iab.

The privacy-preserving technology marketplace serves multiple functions

By using a combination of technologies, organizations can collect, analyze, measure, and activate data, as well as securely share data and insights to relevant internal and external parties.

Customer Data Platforms: CDPs

- Unifies customer data from disparate sources into one platform to provide a single customer view
- Combines internal and external customer demographic, behavioral, and historical data for real-time purchase analysis and prediction

Consent Management Platforms: CMPs

- Protects users' data privacy by allowing website owners to have total control over cookies, trackers, and user consent in one, fully automated solution
- Enables website owners to be compliant with global data privacy laws

Data Clean Rooms: DCRs

- Secure privacy environments that allow multiple parties to collaborate using proprietary data in compliance with privacy regulations, while allowing each participant to maintain privacy and control of its data

Data Management Platforms: DMPs

- Collects and stores large amounts of structured and unstructured data from online and offline sources, including first-party and third-party data
- Organizes and segments data into different customer types, such as location, income, and browsing behavior that can be used for marketing messaging

Identity Solutions

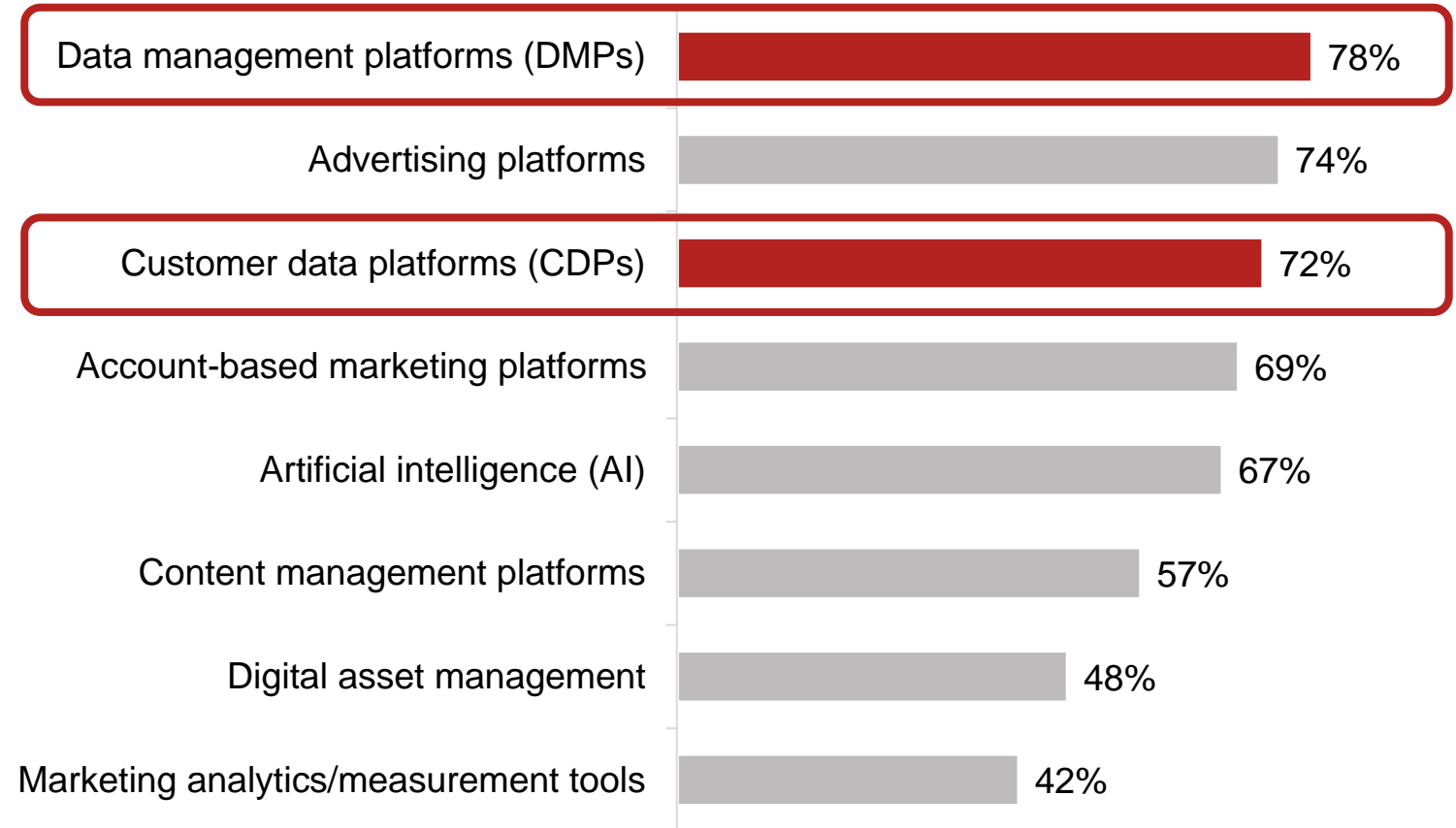
- Data management processes that link customer records across multiple devices and sites to a unique identity—providing companies with a cohesive approach to capturing, measuring, and drawing insights on individual users

Most privacy-preserving technologies have seen widespread adoption

Along with DMPs and CDPs (see right), nine in ten marketers are testing or considering at least one ID solution (data not shown).

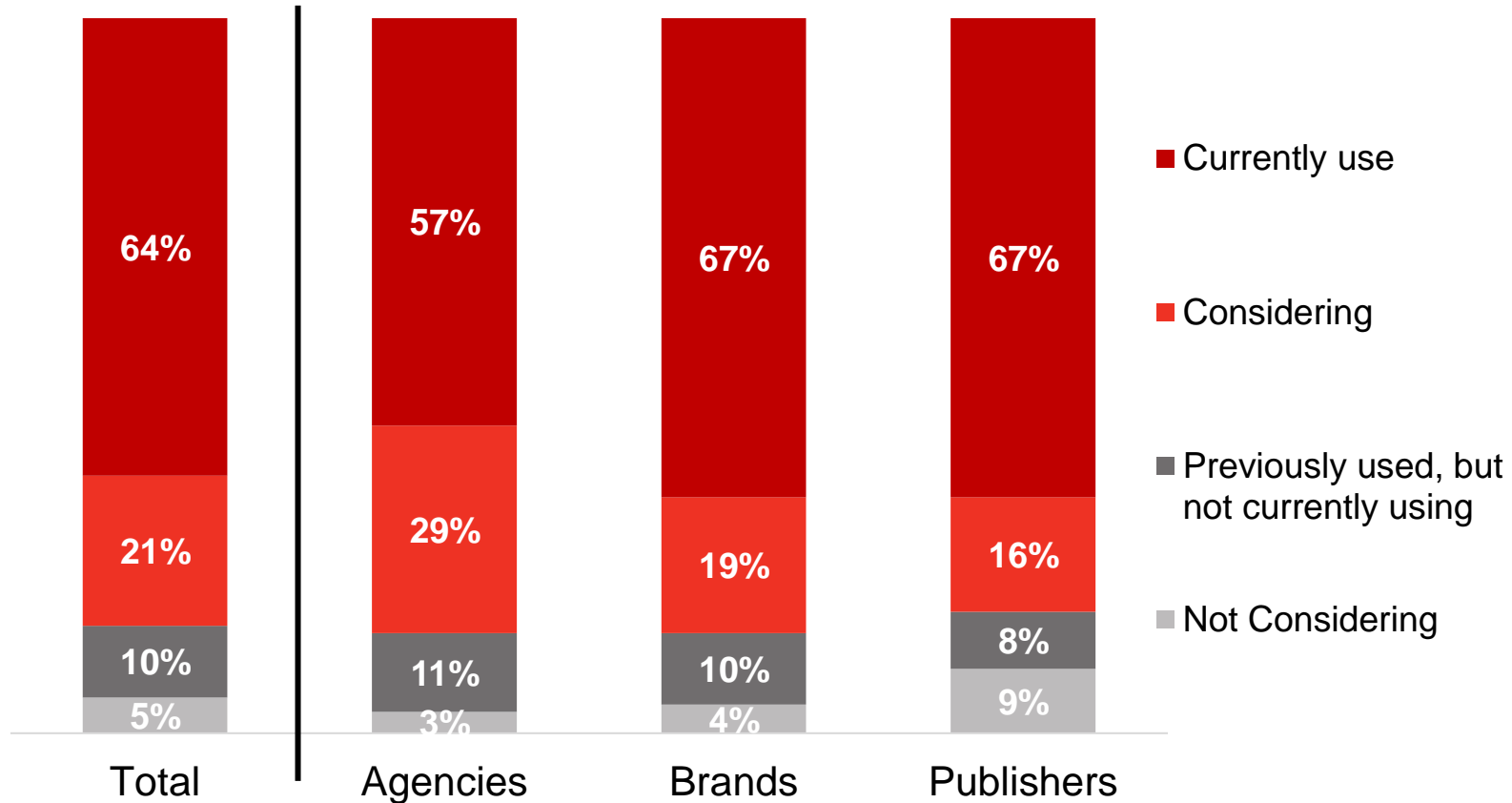
The changes in the privacy landscape have seen companies respond by investing in privacy-preserving technology that allow them to mitigate risk while being able to collaborate with partners.

Select Technology Used by U.S. Marketers



Among privacy-preserving technology users, two-thirds use data clean rooms (DCRs)

DCR Use by Company Type



DCR adoption has accelerated in the last two years

While the majority (61%) of DCR adoption has occurred in the last 2 years, DMP, CDP, CMP, and identity-solution adoption mostly occurred over three years ago.

“

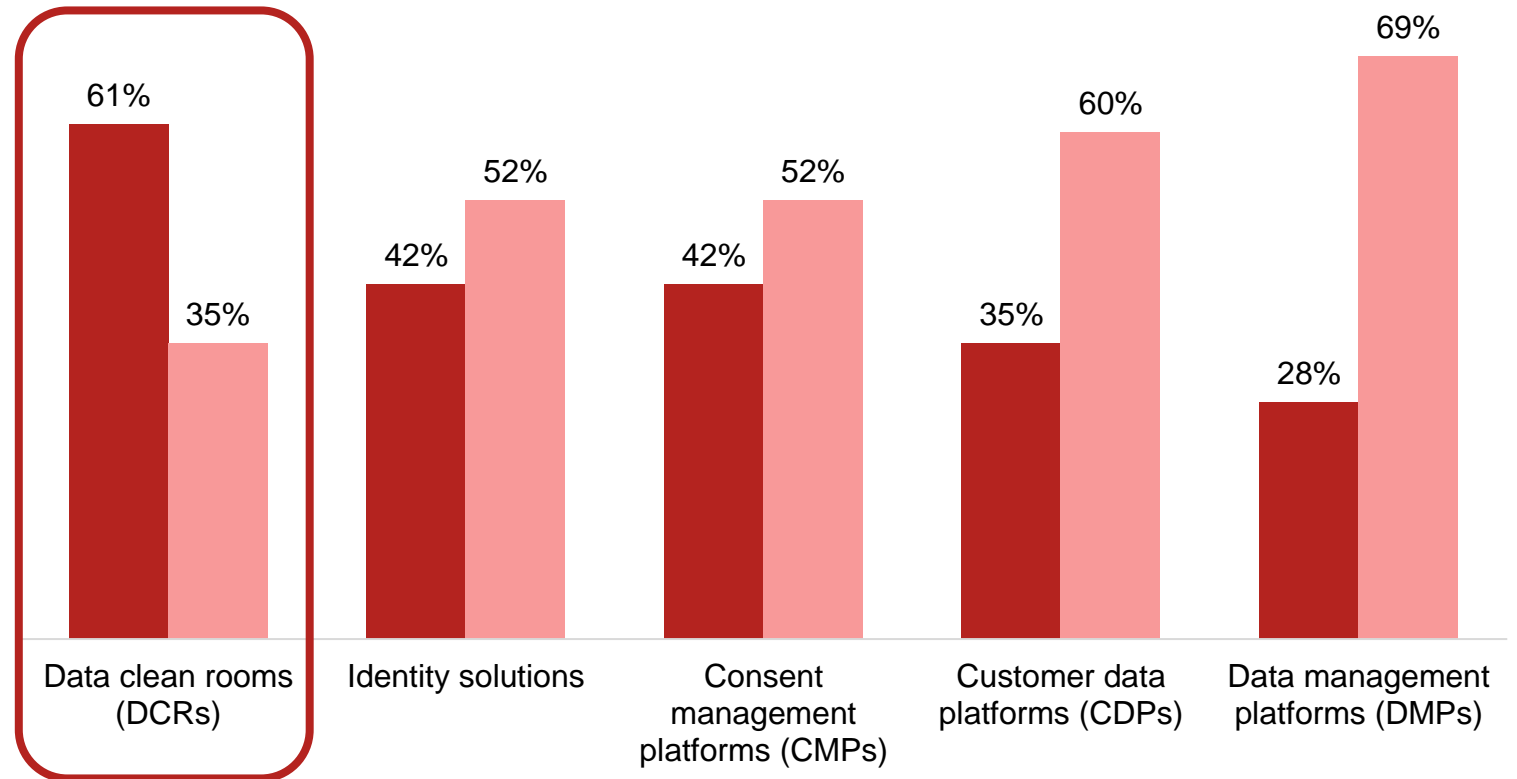
“We are going to accelerate [DCR investment], we are going to double down. With the increase in privacy, it’s going to be mandatory.”

– C-Suite, Agency

Length of Technology Use

(Sorted high to low by 2 years or less)

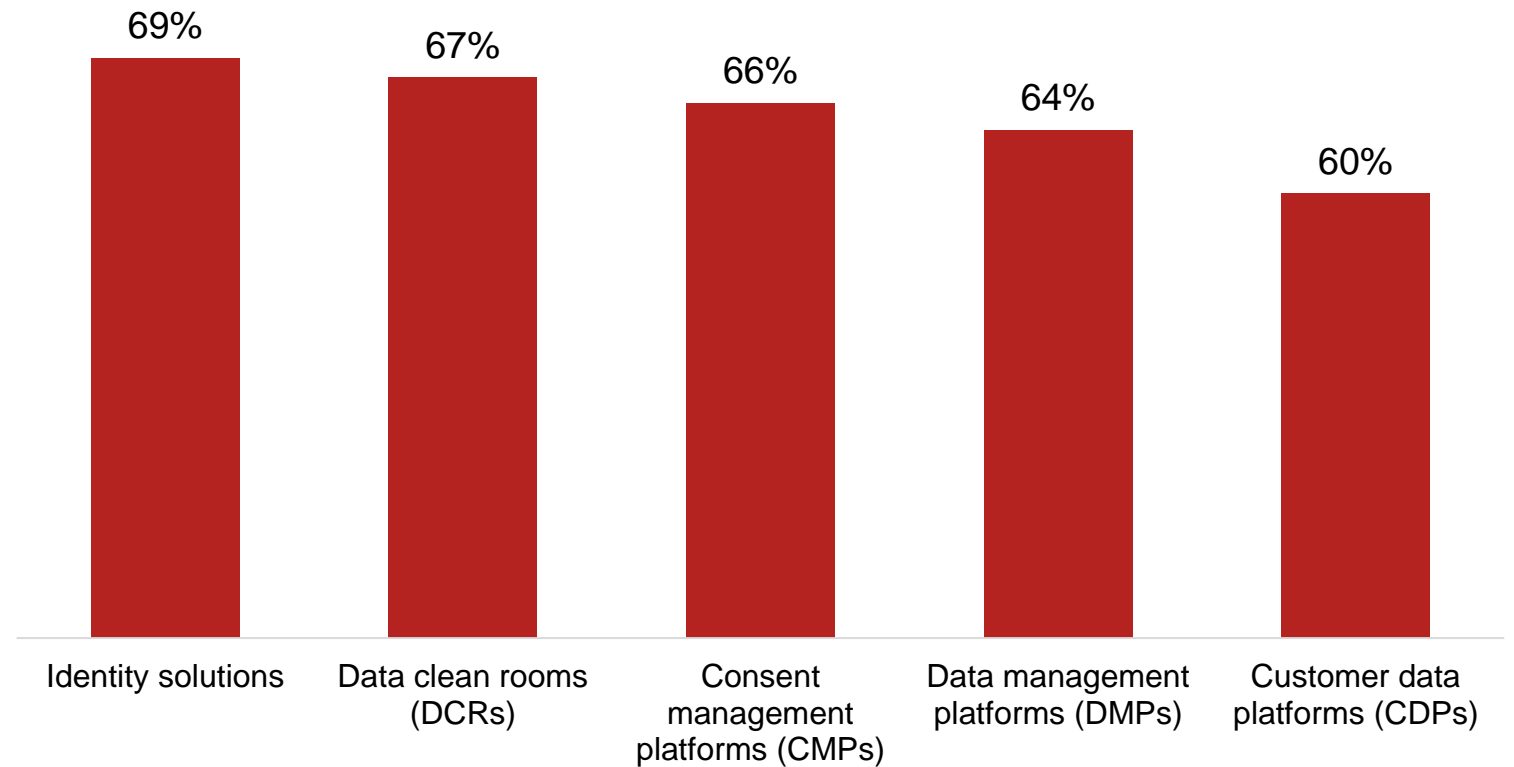
■ 2 years or less ■ 3+ years



Despite its relative nascency, satisfaction with DCRs is comparable to the more established technologies

Additionally, 60%+ of privacy-preserving technology users are satisfied with the technology across the board—suggesting a recognition of the overall marketplace’s value.

Avg. % Very/Somewhat Satisfied With Technology



DCRs are becoming essential for privacy-compliant data matching, activation, and measurement

“

“One of the main drivers of setting up DCRs is the idea that neither party, an advertiser or a third-party data provider, are able to see each other's data. Therefore, it's encrypted, anonymized, with a single key that's useful to activate but cannot be interrupted or decrypted.”

– SVP, Agency

“

“...We're looking at a long term [DCR] investment. Cookies are going away and marketers are going to have to get their data into platforms to be able to activate upon it...Connecting these dots now is going to lead to more investment in the future.”

– VP, Publisher

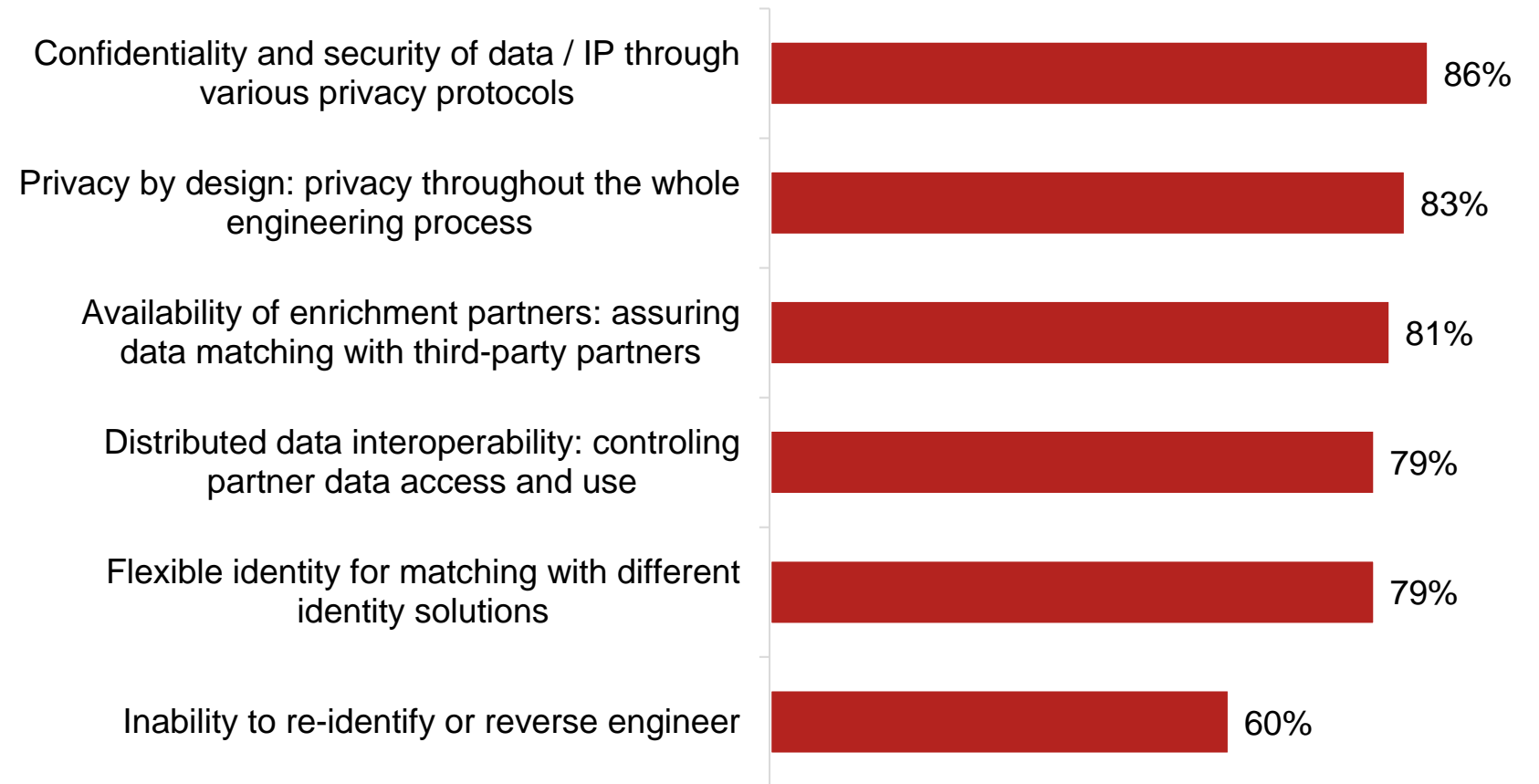
By 2023, 80% of advertisers spending more than \$1 billion annually on media will use DCRs.*

Current users expect to increase their DCR spend by 29% this year (2023).

Users are selecting DCRs for privacy protection, data controls, and interoperability

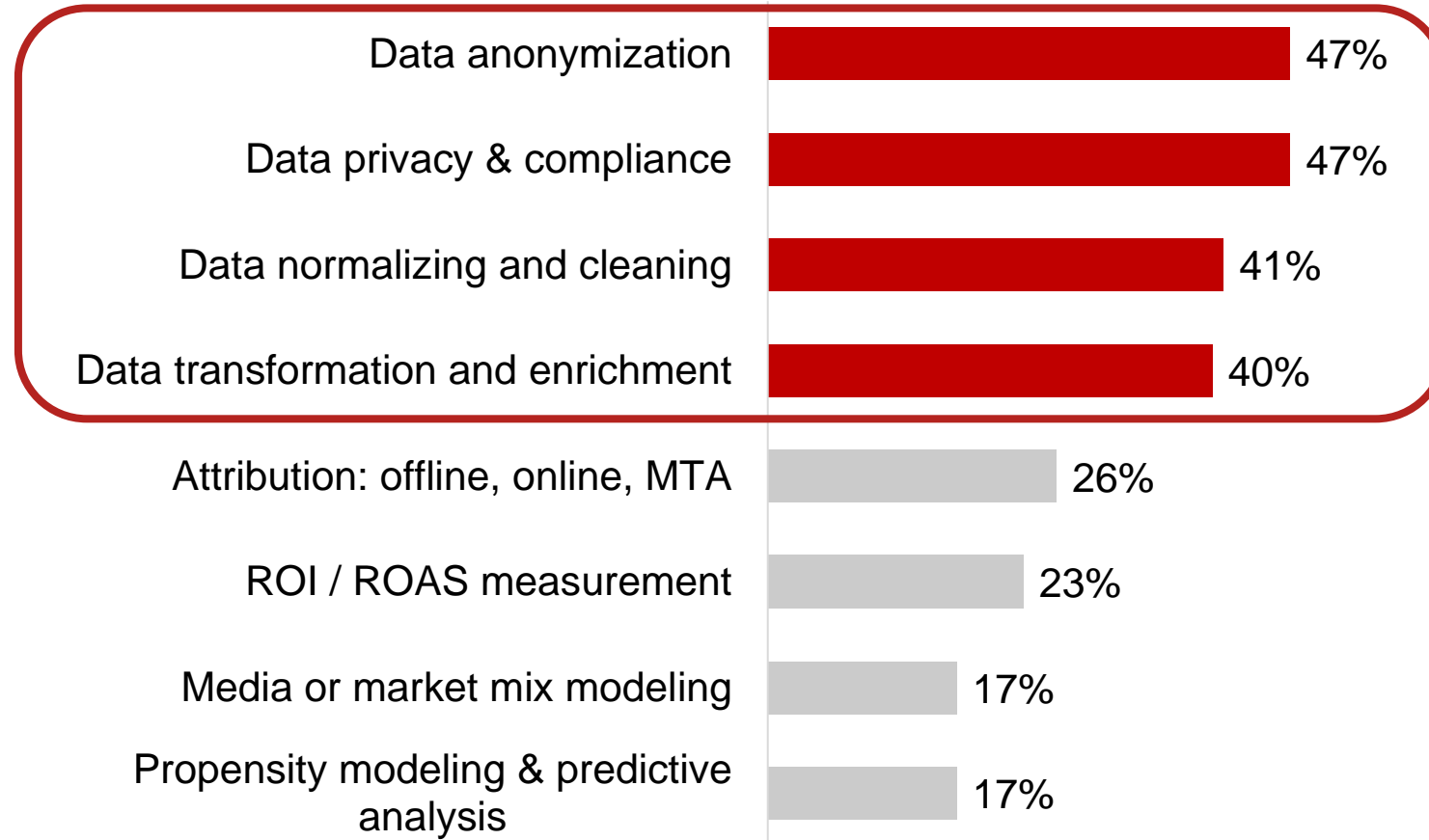
The vast majority (79-86%) of DCR users seek the technology for vital and complex functionality, including privacy protection and controls, match rates, and interoperability.

Importance of Key Criteria When Selecting a Third-Party DCR



Currently, DCR users are primarily leveraging the technology to address privacy concerns and activate audiences

DCR Use Cases



Missed opportunity: Less than one-third of DCR users are tapping into advanced measurement

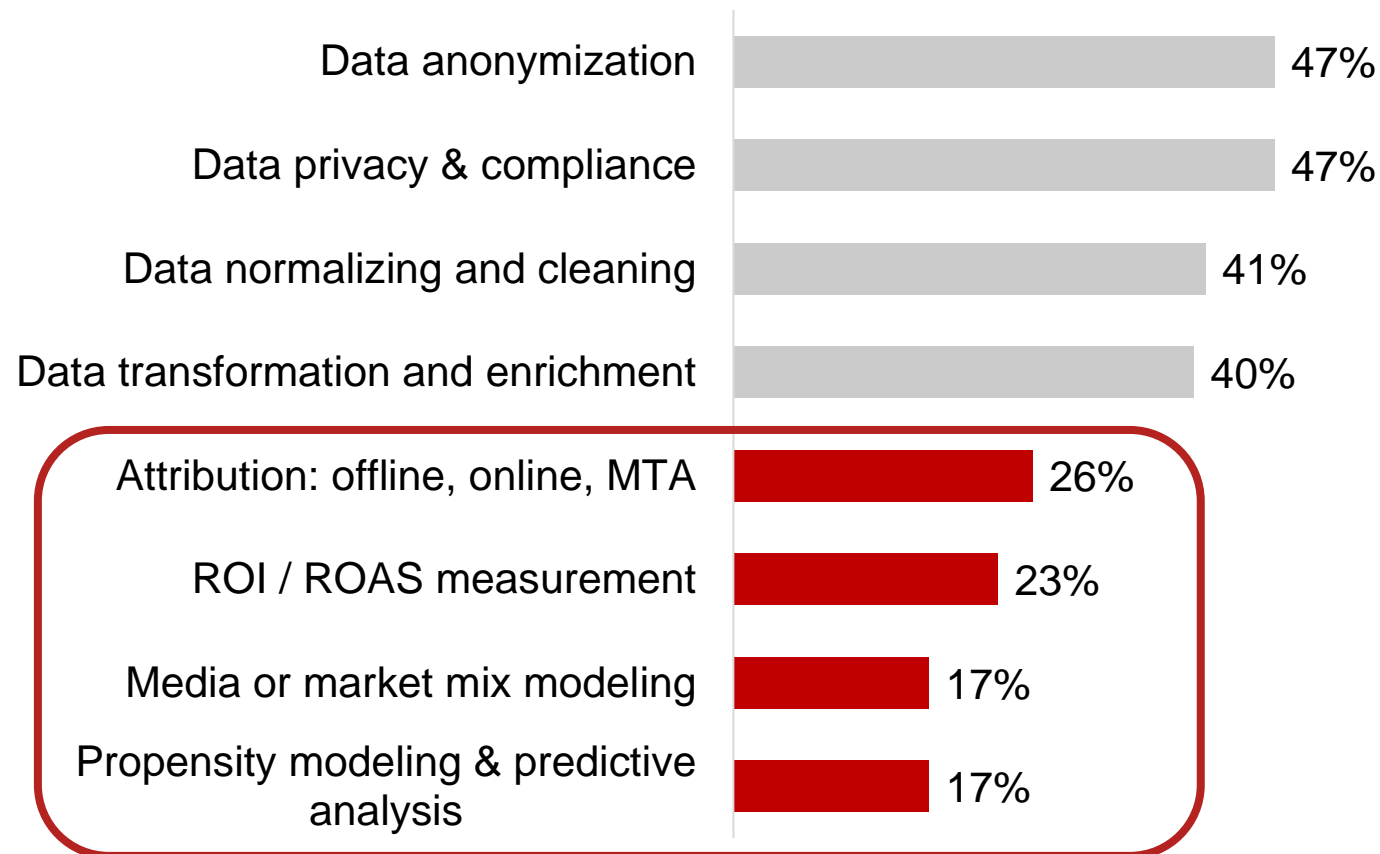
DCR users are likely not yet leveraging attribution, ROI/ROAS measurement, media or marketing mix modeling, and propensity modeling use cases as early-stage adoption has focused on privacy and audience activation. This represents an opportunity for DCR users to capitalize on the technology's most powerful capabilities critical for operating in the evolving data landscape.



"Number one [use case] is planning, where your high-value audience over-indexes, because it's the easiest. Because it's the easiest, you get there first. The next question is activation and then the third is measurement."

– SVP, Publisher

DCR Use Cases



**Data Clean Rooms:
Hurdles and
Opportunities for Growth**

iab.

DCRs offer opportunities for innovative, privacy-preserving use cases

Select DCR Innovative Use Cases

- ❑ Privacy-compliant audience and transactional data activation
- ❑ Advanced attribution and cross-channel measurement
- ❑ Predictive modeling and market mix modeling
- ❑ Enrichment of transactional data with behavioral signals
- ❑ Audience insights and propensity models

“

“The DCR allows you to reach people in a way that is fully privacy compliant, [driving] 5 or 10 times the uplift in user engagement because we’ve had the right message, to the right person, at the right time—something cookies don’t do.”

– C-Suite, Publisher

“

“We combine ad impressions with transactions, look at interaction patterns... send the transaction data completely anonymized at the aggregated level and then get the same from our partners, and mix this together.”

– Director, Retailer

“

“...we made log files available for closed-loop attribution and for reach and frequency.”

– SVP, Publisher

“

“We use [DCR] for activation purposes, creating lookalikes and propensity models”

– SVP, Agency

However, DCRs require significant investment in human talent

Half of DCR users (49%) have six or more employees at their companies who are users, builders, facilitators, or purchasers of DCRs, with nearly one-third (30%) leveraging a minimum of 11 people.

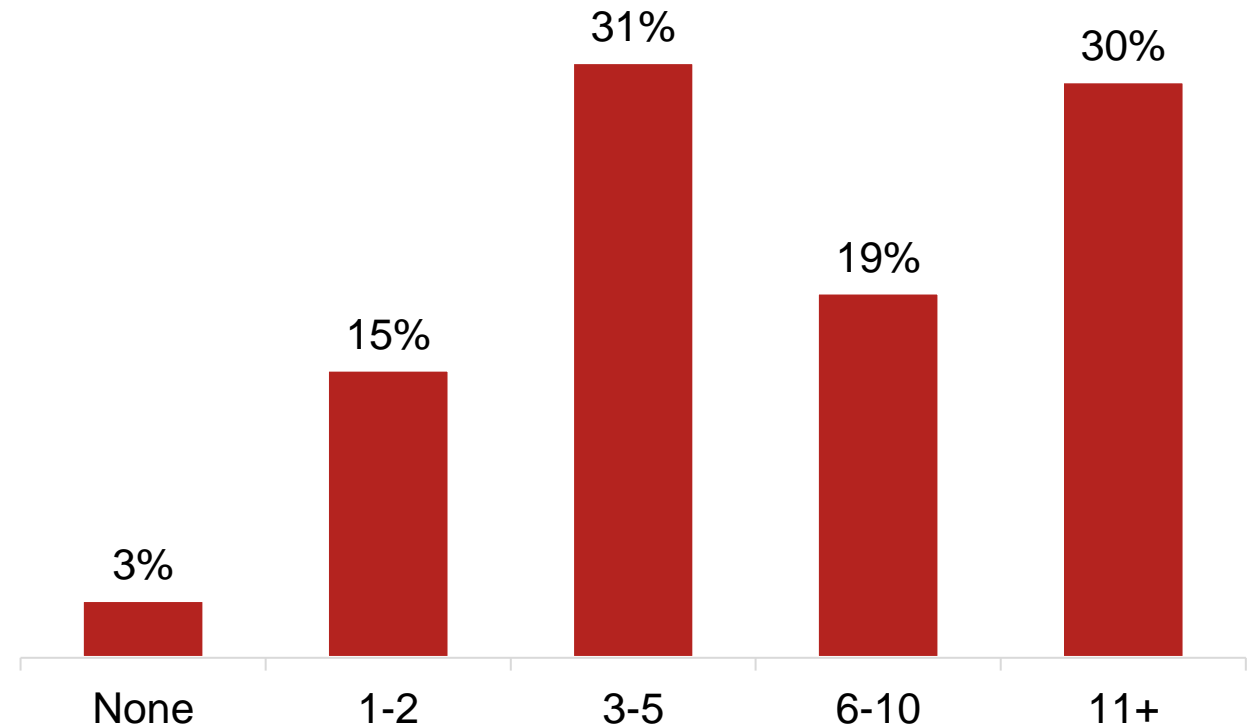
It is crucial that DCR talent have privacy expertise, including encryption technology, data security, and other privacy-enhancing technologies such as differential privacy*, k-anonymity*, etc.

“

“You need data architects, data engineers, QA, DevOps, and infrastructure. You’re talking about 5 different roles so ~5 FTEs at a minimum.”

– C-Suite, Agency

of Employees Using / Building / Facilitating / Purchasing DCRs



DCR setup is lengthy and complex

Complex DCR Setup Process

- ❑ Review privacy and governance settings internally and with external partners
- ❑ Evaluation of data use cases and ownership rights
- ❑ Setup data onboarding procedures
- ❑ Establish connections with multiple external and internal partners
- ❑ Configure and maintain dataset filtering and queries

“

“The bulk of the work is before using DCR...in the contracting and setting up to make sure that the relationships are privacy compliant...Then, on the other side it’s the justification of what data you are getting, where it is going, what is the use case.”

– Director, Retail

“

“It took us longer to set it up be running with [DCRs] than we had anticipated...we had major skill and knowledge gaps in our organization.”

– Senior Director, Brand

“

“We had to work with product and tech teams on deeper privacy, security and compliance requirements to set up the ad-hoc environment, set up audiences and sales data, and how we look at data in the sandbox environment, targeting, match reporting and measurement. That takes a lot of time.”

– VP, Retailer

“

“DCR setup challenge: you need DCR connectivity with publishers. If the DCR has a relationship, the setup is faster. But if not, then you have to get every publisher to look at their IT.”

– SVP, Agency

DCR costs create a high barrier to entry—a challenge for smaller industry players

Nearly two-thirds (62%) of DCR users spent a minimum of \$200K on the technology, with a quarter (23%) spending \$500K+.

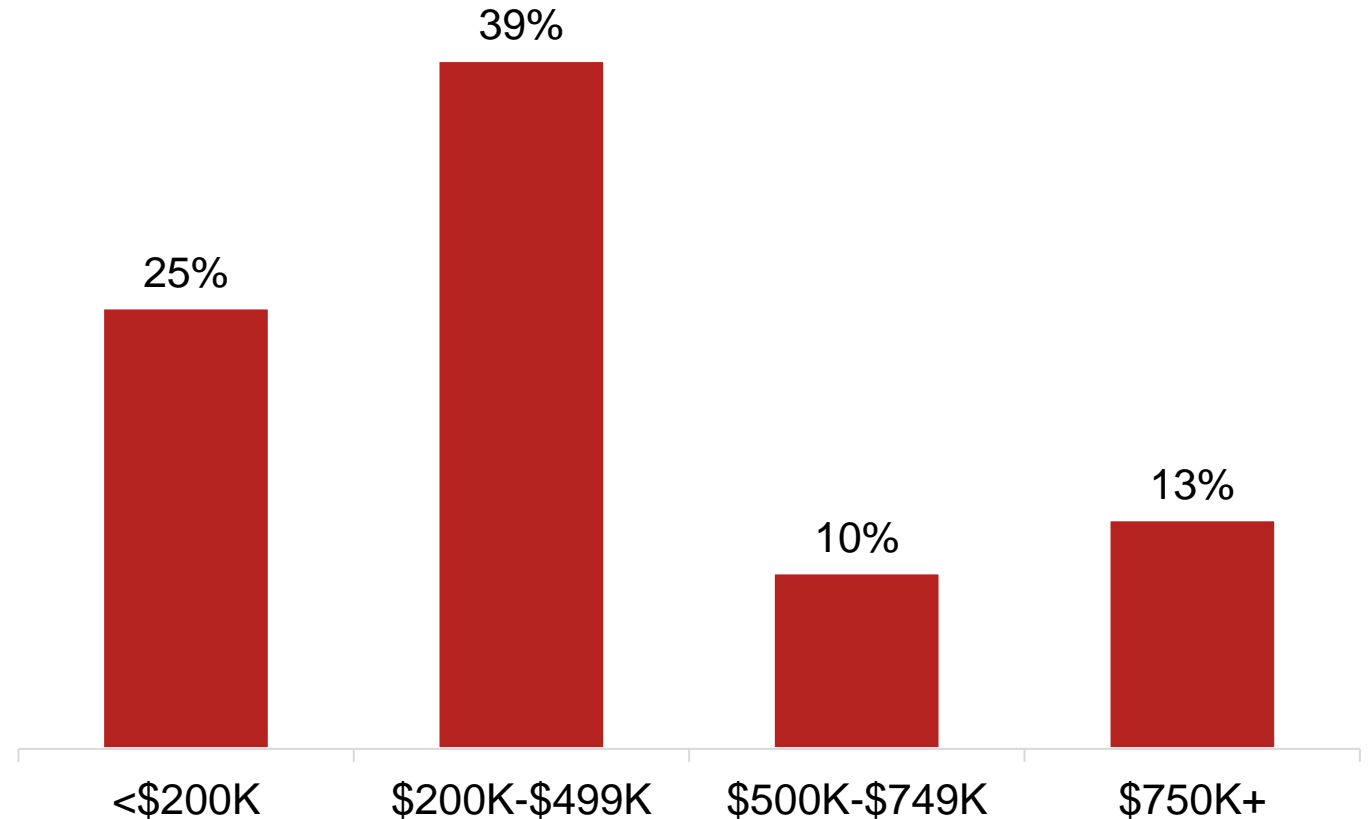
Those spending \$100M+ annually in media are 29% more likely to be DCR users than those spending <\$100M (data not shown).

“

“From an investment perspective, the licensing is very expensive. You’re paying \$200K or even upwards of \$500K just to build out one. There’s not a lot of media partners or brands who can spend that kind of cash on a tech.”

– C-Suite, Agency

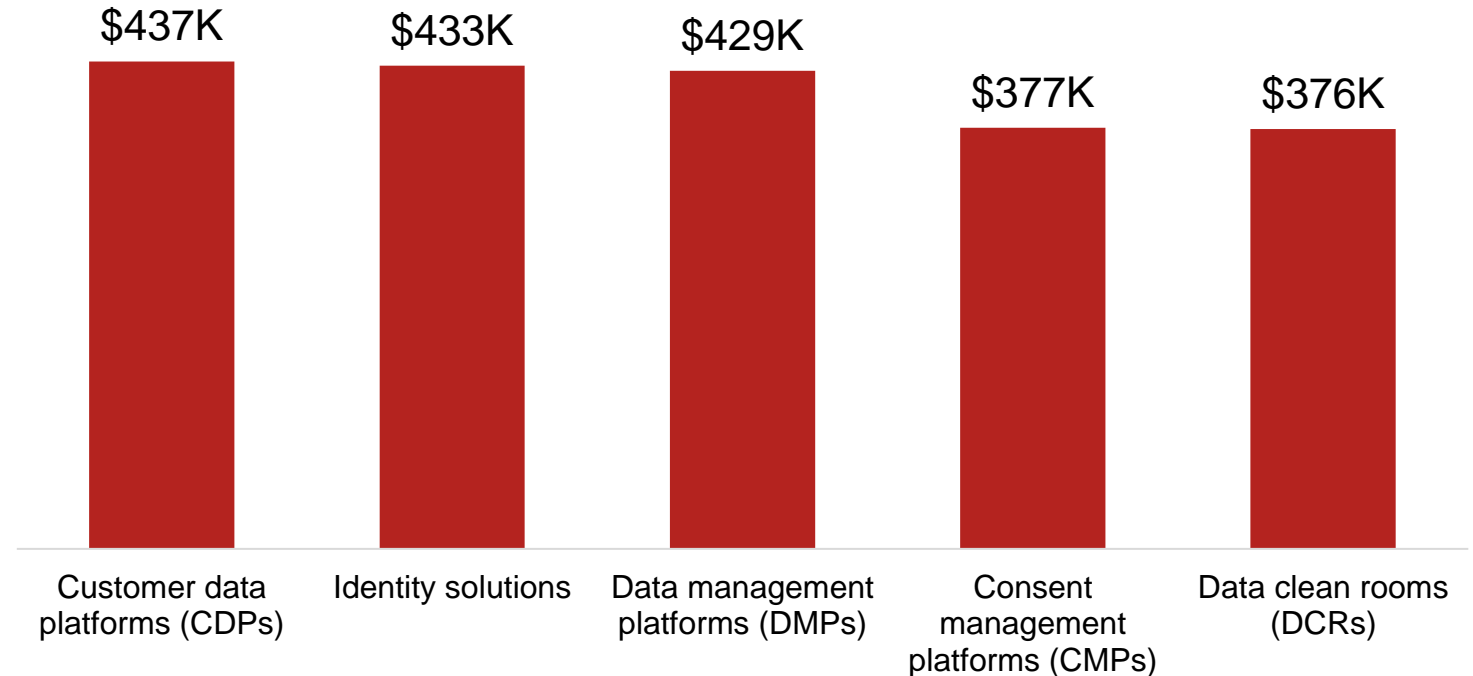
2022 DCR Spend



Additionally, using DCRs with other privacy-preserving technology can drive annual costs above \$2M

Companies recognize the importance of using DCRs in conjunction with other privacy-preserving technology. For example, eight in ten DCR users are using CDPs (84%) and DMPs (81%), and half are using identity solutions (55%) and CMPs (45%). Thus, DCR users are likely experiencing compounded costs.

Average 2022 Costs by Technology (\$K)



And, sub-par match rates threaten the overall efficacy of DCRs

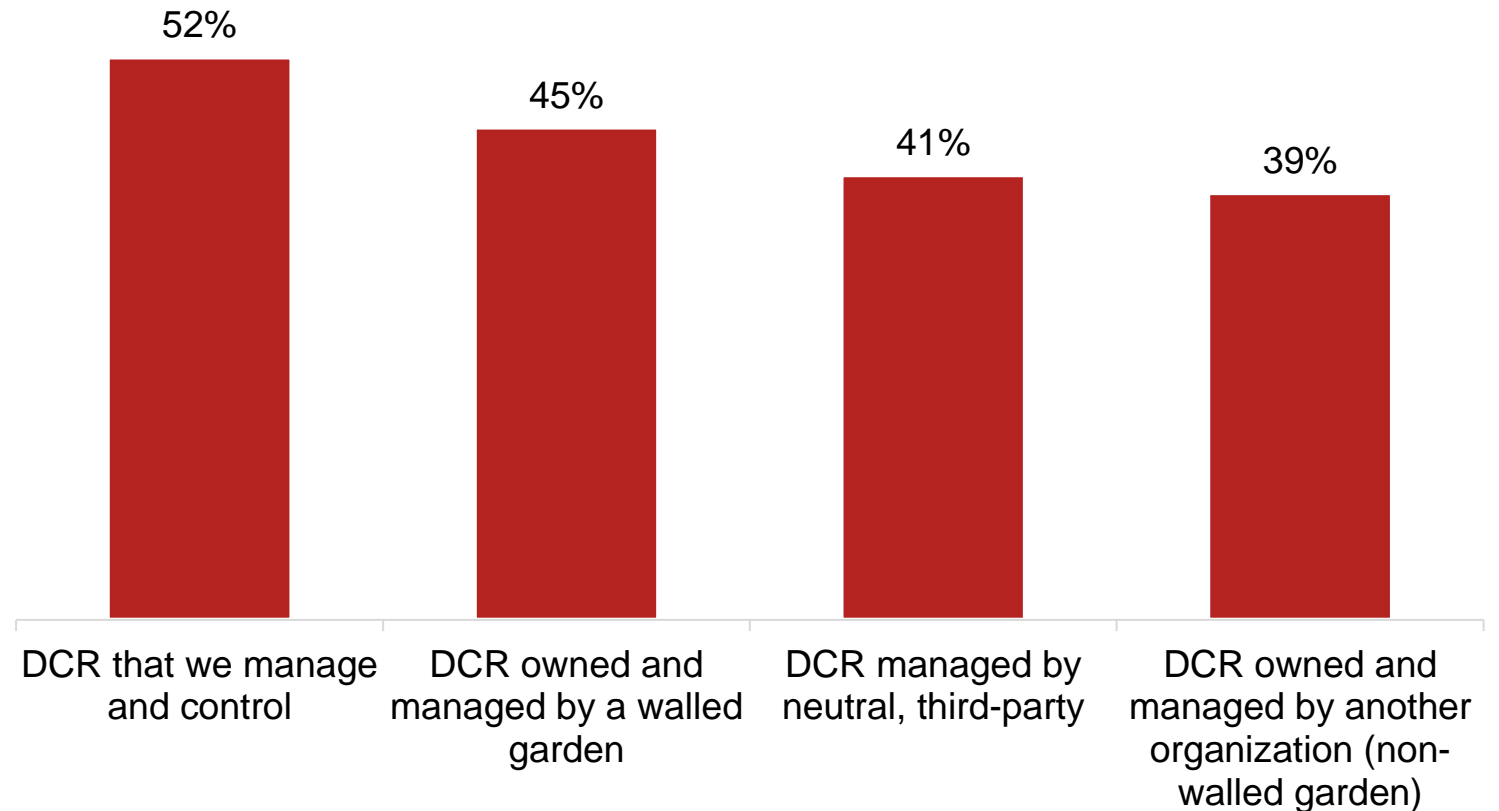
Ongoing signal loss and the evolution of state-level privacy legislation will likely further challenge match rates—putting additional pressure on the DCR marketplace to improve.

“

“We have a target for match rate which is at least 50% so when we send out our audience segment we want to make sure that the vendor here is actually able to match 50% of their audience.”

– Director, Retailer

Average Match Rates by DCR Type



Sub-par match rates are driven by a multitude of factors

Sub-Par Match Rate Drivers

- ❑ Identity fragmentation
- ❑ Platform bifurcation
- ❑ Inconsistent data inputs
- ❑ Data obfuscation

“

“Whenever I'm matching, I need to make sure that my ID is recognized out in the ecosystem, and there are a lot of IDs in the ecosystem today.”

– C-Suite, Agency

“

“There is definitely a challenge with respect to the identifiers that we can potentially work with [for matching]...Not every client is going to share their IP addresses and may instead want to use email addresses so we need to have a similar identifier on our side.”

– Senior Director, Publisher

“

“Different platforms have varying degrees of data capture capabilities, so transforming it and normalizing it is difficult... [The effort is] getting the data into a format that works for the DCR to be able to make matches.”

– SVP, Agency

“

“If email address is the thing being matched on, a lot of people subscribing to a publication might be using a work email address vs. personal email addresses for the advertiser. So [with B2B clients], the match has that extra hurdle of different email addresses.”

– SVP, Publisher

Due to the complexities, a significant percentage of DCR users cite ongoing challenges

“

“In testing we learned that we have to realign our data assets to what is needed. And there were a number of things that didn't work. We did an overlap test and found that deep insights were really hard to do and activation was challenging.”

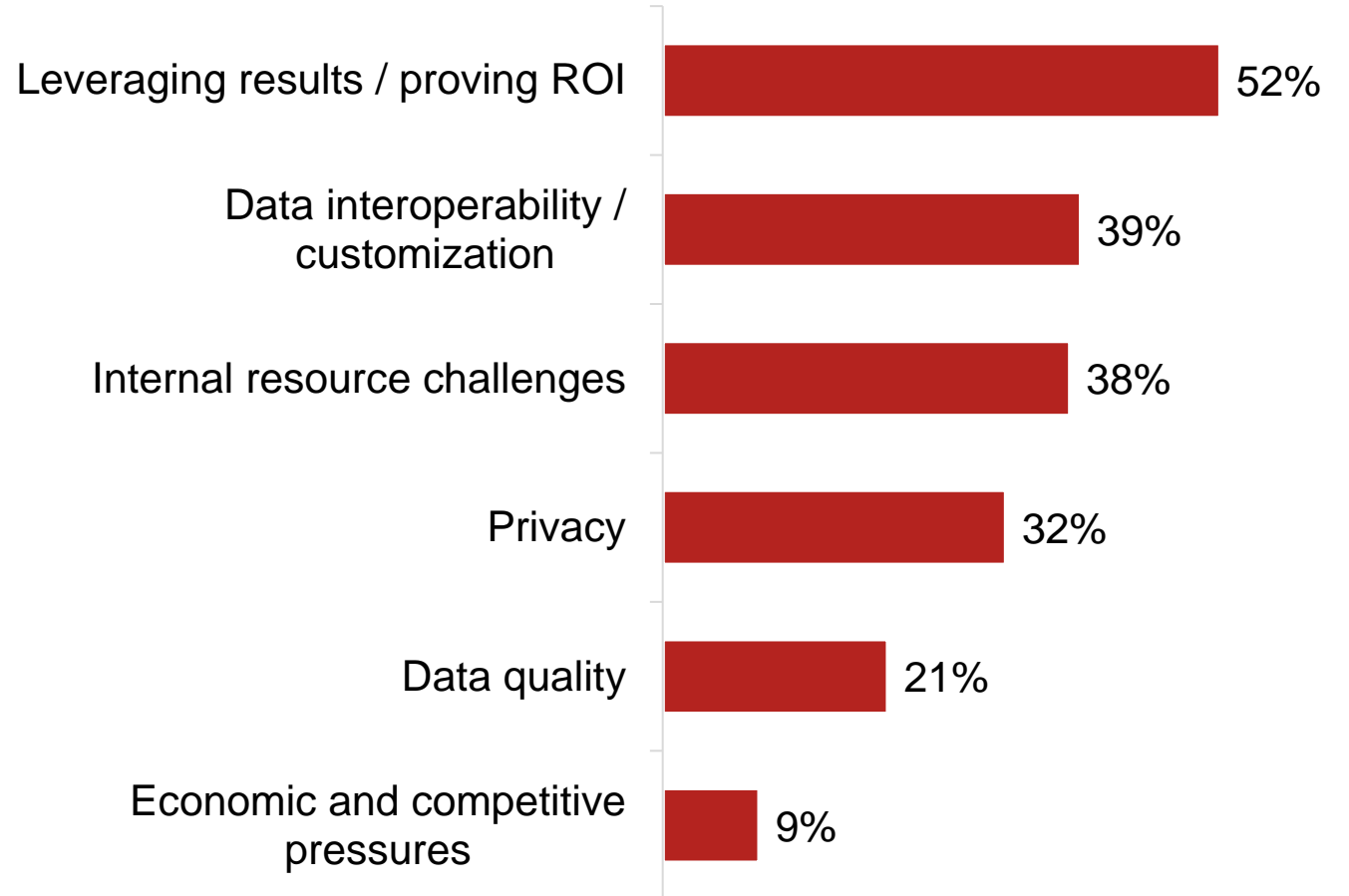
– VP, Publisher

“

“[DCR] is in a nascent stage...it's not a fully matured tech with everything you need [yet]...There is a lot of complexity with volume and types of data, and also the organizational structure.”

– Product Lead, Brand

DCR Challenges



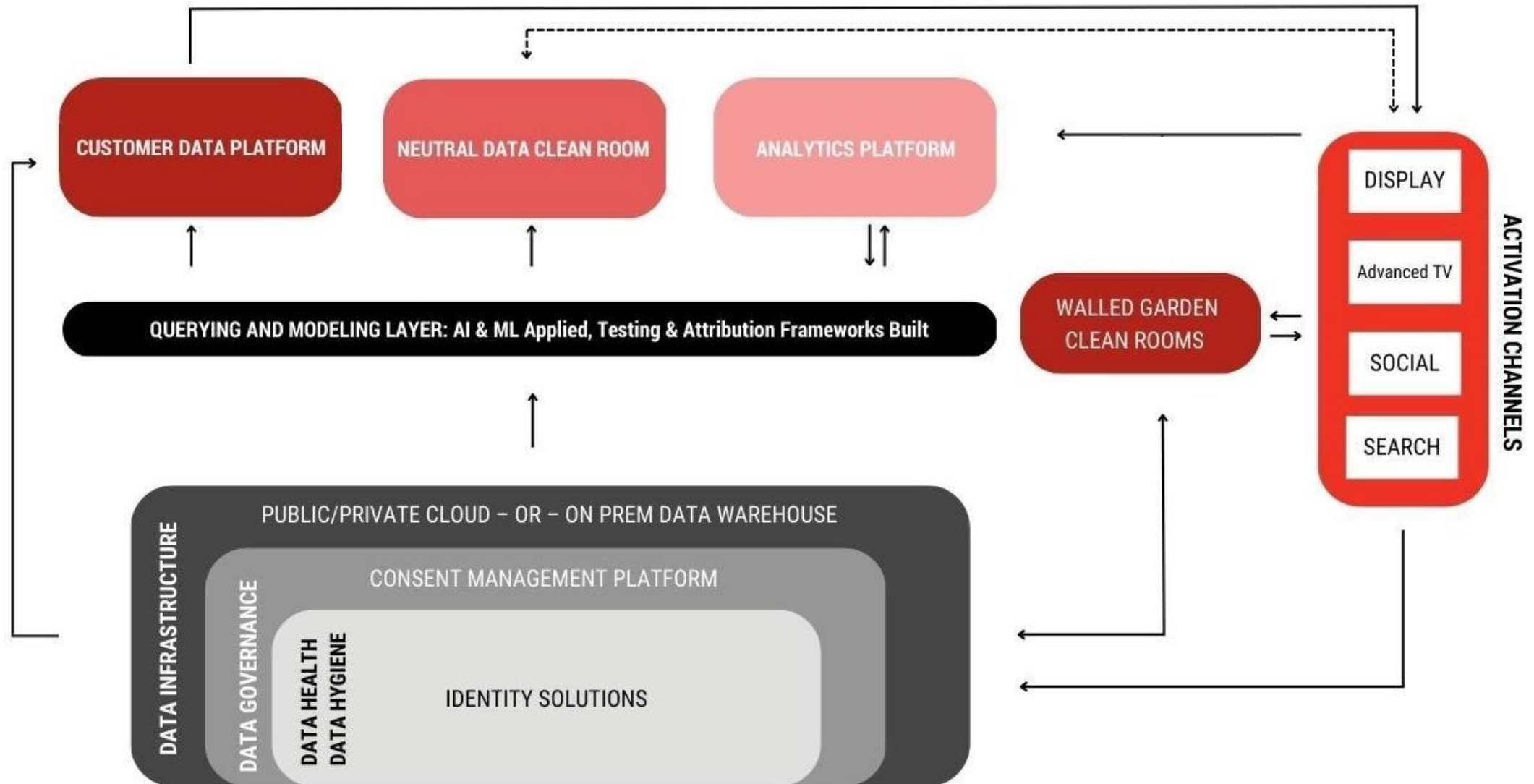
Recap: Five Things You Need to Know

1. DCRs have become an **essential technology in the privacy-centric ecosystem.**
2. DCR users have yet to tap the full potential of **technology's advanced measurement capabilities.**
3. DCRs are not turnkey technology, **requiring significant investments** in talent, cost, and setup, including data infrastructure and connectivity as well as onboarding.
4. High DCR investments **disadvantage smaller industry players.**
5. All data providers, including walled gardens, need to **make their data interoperable for measurement and ROI.**

**Privacy-Preserving
Technology:
Considerations and
Best Practices**

iab.

Privacy-Preserving Technology: Interconnectivity Map



Evaluation Phase: Key considerations

- 1. Cost and Time:** It can take significant time, effort, and cost to set up and maintain a DCR or other privacy-preserving technology. Timing is dependent on (but not limited to) the following factors:
 - a. The number of data points
 - b. The number of data sources
 - c. How complex the data assets are
 - d. The desired level of security
 - e. The infrastructure and resources needed to support it
- 2. Accessibility and Security:** Data access and analysis requires strict protocols and procedures to ensure security and privacy. Data cleanup can be time consuming—especially if companies need to access the data frequently or have large volumes of data to analyze. Additionally, there can be multiple levels of approval, as well as detailed documentation required for implementation.
- 3. Data Accuracy and Scalability:** Prior to implementation, it is essential to ensure that the data intended for use is accurate, reliable, and scalable. This helps mitigate the risks of potential financial loss and performance gaps.
- 4. Human Capital and Talent:** Implementation and maintenance requires a wide talent pool with subject-matter expertise including data privacy, security, governance, analytics, and marketing. Long-term success requires hiring and retaining top talent in these areas with the skills and capabilities to adapt and evolve over time.

See pages 38-39 of the appendix for lists of detailed factors for each of these four considerations.

Implementation and Maintenance Phase(s): Best practices

- 1. Define clear scope and purpose:** Establish and prioritize use cases based on technology and business needs, financial impact, data maturity, and operational complexity.
- 2. Establish strict access controls:** Determine and maintain access technology controls to ensure only authorized personnel can access the data being processed. Physical access controls, login credentials, and background checks may be included.
- 3. Follow strict data handling procedures:** Ensure that data is kept secure and confidential in the technology by establishing protocols for encryption and secured data transfers.
- 4. Regularly review and audit:** Perform regular reviews and audits to ensure that the technology is operating effectively and is compliant with all laws and regulations.
- 5. Consider data accuracy and maturity:** Choose partners with track records that accurately and comprehensively resolve identities.
- 6. Review partner data privacy and security practices:** Investigate and understand platform partners' data privacy and security protocols.
- 7. Consider the level of customer support offered:** Partners should offer documentation, training resources, and responsive customer service.
- 8. Clean and standardize your data:** Make sure to clean and standardize your data *before* integrating it into any platform to ensure that it is accurate and consistent.
- 9. Establish KPIs/success criteria:** Determine measurable, desired outcomes to evaluate the performance of the technology for your use cases.
- 10. Stay up to date on evolving privacy compliance requirements:** Work with legal and compliance professionals internally and externally to understand the potential impact of the changes on your technology practices.

Continued Maintenance: Risks from evolving privacy legislation and platform changes

The data landscape is facing ongoing privacy challenges, from five new state-level laws coming into effect in 2023, to actions from platforms resulting in industry signal loss, to pressure from consumer privacy-preserving advocates forcing companies to evaluate their practices to ensure they respect individuals' rights to their personal data.

There are two main risks to the advertising industry that are crucial regarding the privacy-preserving technology landscape:

1. Restrictions on the collection and use of personal data:

Privacy regulations such as the five new state-level laws in California, Virginia, Colorado, Connecticut, and Utah, Apple's App Tracking Transparency (ATT) initiatives, and the impending roll-out of Google's Privacy Sandbox places limits on the types of data that companies can collect, as well as how they can use and share that data. This will continue to change the way that companies target ads, as they can no longer rely on certain types of data to do so.

2. Increased transparency and choice for consumers:

Companies will need to be more transparent about their data collection and practices while giving consumers more control over their personal data. This includes the right to opt out of the collection and use of their data for advertising purposes. High opt-out rates can potentially threaten the efficacy and effectiveness of companies' advertising and marketing efforts.

Overall, companies need to be prepared for evolving changes to data activation, collection, and measurement as the data and privacy landscape continues to evolve. It is crucial to ensure that all data handling activities in DCRs and other privacy-preserving technologies comply with relevant privacy regulations and adapt to data loss—otherwise companies risk significant fines or reputational damage. It is imperative that companies collaborate with both internal and external partners across functions and develop strategies for mitigating risk.

Continued Maintenance: Key industry standards for risk mitigation

Standards can be extremely beneficial for companies by ensuring the consistency and reliability of products, processes, and services—resulting in improved quality and reduced costs. They can also facilitate interoperability that allows for seamless integration of various systems and devices. Standards can aid a company in complying with regulations and industry standards, as well as enhancing its reputation and credibility. IAB and IAB Tech Lab advise the industry to prepare for new U.S. state-level privacy signaling changes, and encourage companies to support, contribute to, and consider adopting the following standards. **Moreover, if your company hasn't started solving the privacy challenges coming this year, it's time to start ringing the alarm bells.**

- 1. [Global Privacy Platform \(GPP\)](#)** The Global Privacy Platform helps the industry solve for the challenges that come with the need to address differing and evolving privacy regulations worldwide. The GPP enables user consent signals to be communicated throughout the digital ad supply chain and provides the protocol to help consolidate the management of different consent signals from multiple global privacy jurisdictions. It has the capabilities to read GPP signals—TCF, U.S. State signals, Global Privacy Control (GPC)—and apply to identities.
- 2. [IAB Multi-State Privacy Agreement \(MSPA\)](#)** The IAB Multi-State Privacy Agreement is an industry contractual framework intended to aid advertisers, publishers, agencies, and ad tech intermediaries in complying with five state privacy laws that are becoming effective in 2023 (California, Virginia, Colorado, Connecticut, Utah). Note: 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.
- 3. [Taxonomies](#):** As part of ongoing efforts to put privacy-by-design principles into practice, IAB and the IAB Tech Lab introduced and continuously update the following taxonomies to provide the industry with common nomenclature for audience segment names and content labels to improve comparability of data across different providers: [Transparency Center](#), [Content Taxonomy](#), and [Audience Taxonomy](#).
- 4. [Privacy Enhancing Technologies \(PETs\)](#):** Deploy privacy guaranteeing technologies like differential privacy* and multi-party computation to keep DCR transactions private and to avoid sharing/transferring sensitive information. IAB Tech Lab's PETs initiative focuses on use case definitions, API standards for PETs between pairs/groups of digital ads ecosystem participants and stewarding open-source initiatives.

For more information about how to get involved or learn more about IAB and IAB Tech Lab initiatives, please email data@iab.com.

Data Clean Rooms: Understanding the Benefits and Use Cases

iab.

IAB Perspective: The benefits of DCRs in the privacy-preserving technology landscape

The primary benefit of a data clean room (DCR) is that it enables data to be shared anonymously with other parties without the risk of breaching that data's privacy or exposing it to potential external breaches. This makes DCRs a particularly valuable technology for companies across the advertising ecosystem given the increased industry sensitivity on how companies are collecting and using consumer data.

This report shows that DCRs' anonymization capabilities enable companies to derive advanced consumer insights and conduct segmentation analyses without concern over the potential risks to data that may be considered sensitive, such as PII, device IDs, and other geographic, behavioral, audience, or contextual data. Companies can also further enrich their data with other sources for audience insights and measurement through use of a DCR.

It is incumbent upon DCR owners to determine the level of differential privacy mechanisms and controls needed to secure the data and mitigate re-identification of PII. For details on DCR privacy controls and methods to protect consumer data, see page 37 of the appendix.

As illuminated in [IAB's State of Data 2022 \(Part II\): Preparing For The New Addressability Landscape](#) report, consumer trust is vital to providing companies the access data they need to monetize their businesses and create better consumer experiences, products, and services. DCRs can help companies be accountable by demonstrating their commitment to protecting consumers' sensitive information.

When considering a DCR, it is imperative to carefully evaluate and weigh the pros and cons of the technology implementation and maintenance, and then select partner(s) best suited to meet your needs.

Since DCR investment requires six-figure annual budgets, DCRs may not be opportune approach for all companies. Companies can protect sensitive data using other methods such as de-identification or aggregation; however, while these methods can be less expensive, they are ultimately more time-consuming.

In summation, while DCRs may not be suitable for all companies, they can be an effective solution for those that need to share data with external parties on a regular basis.

Use Case Framework: Develop a conditional sequence data approach

When evaluating DCR use cases, it is optimal to take a **conditional sequence data approach**.* Outline the various use cases sequences based on your hypothesis which will branch out based on the business needs, operational lift, cost, and data maturity. By doing so, companies can identify how to achieve both short-term and long-term success and achieve incremental value from their DCR adoptions.

Data monetization in a privacy-preserving environment is a core capability for retailers in DCRs. This allows for the democratization of data to improve personalization, enhance audience insights, and offers a comprehensive view of measurement and outcomes.

In the future, as DCRs evolve and become more sophisticated, additional use cases will be unlocked and offer companies across the ecosystem more flexible, sophisticated, interoperable, and scalable opportunities.

Overarching Use Cases

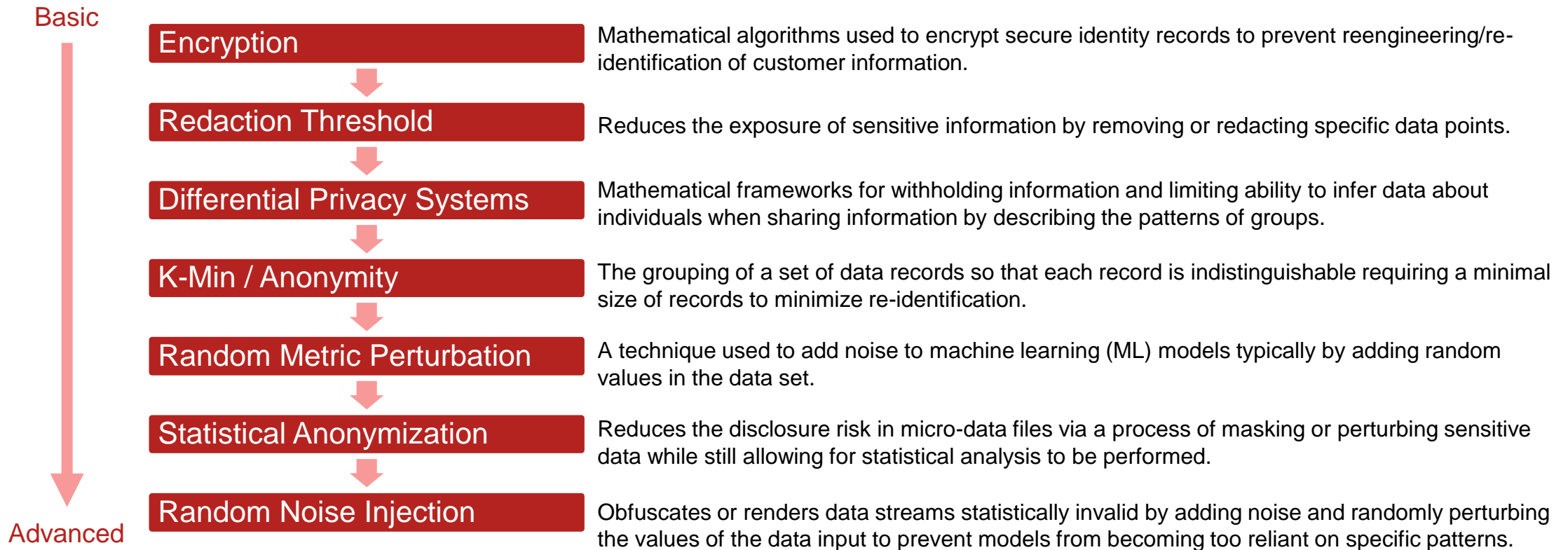
- 1. Audience insights and segmentation:** Collaboration in a DCR between the buy- and sell-sides of the digital advertising industry allows both parties to comingle their first-party data and improve data enrichment to understand advanced consumer insights, such as behavioral and contextual signals, in a privacy-compliant way.
- 2. Media campaign measurement and attribution:** By matching customer and performance data, DCRs enable companies to measure cross-media performance and develop attribution and measurement models for optimization. DCR users can conduct a variety of analyses: consumer journey, audience overlap, and reach and frequency, as well as mix modeling and scenario planning with the use of artificial intelligence (AI) and machine learning (ML).
- 3. Audience modeling and activation:** Advertisers can use DCRs for scalable audience activation by creating probabilistic or look-a-like audiences for targeting in a privacy-first ecosystem. Publishers and retailers can uncover and create audiences that ad buyers may find more appealing. DCR collaboration capabilities open the possibilities for improved data enrichment to understand consumer insights such and behavioral and contextual signals.

Appendix

iab.

DCR Privacy Controls and Methods to Protect Consumer Data

It is incumbent upon DCR owners to determine the level of differential privacy mechanisms and controls needed to secure the data and mitigate re-identification of PII.



Evaluation Phase: Additional factors for consideration (1 of 2)

Cost and Time

1. **Initial setup and deployment:** Upfront costs associated with getting the technology up and running.
2. **Ongoing maintenance:** Costs needed to keep the technology running smoothly including updates, patches, and technical support.
3. **Licensing:** Upfront costs associated with licensing the technology.
4. **Hosting:** Costs to consider if the technology is hosted on a third-party server.
5. **Customization:** Costs to consider if the technology is needed to be customized to fit the specific needs of your business.
6. **Integration:** Costs to consider if the technology needs to be integrated with other systems or software.
7. **Training:** Costs to consider if employees need to be trained on how to use the technology.
8. **Scalability:** Costs to consider if the technology needs to be scaled up as your company's business grows.
9. **Service fees:** Additional costs for services provided with the purchasing, licensing, or additional support personnel by platform company.

Accessibility and Security

1. **Location-specific features:** If your business operates in multiple locations, the technology should support location-specific features such as localized customer management.
2. **Access control:** Consider the technology's access control measures such as authentication and authorization protocols.
3. **Data security:** Make sure each technology has strong data security measures in place including encryption of sensitive data and secure servers.
4. **Compliance:** Make sure the technology is compliant with relevant regulations such as GDPR, CPRA, COPPA, HIPPA, etc.
5. **Security updates and patches:** Confirm that each technology regularly releases security updates and patches to address new threats.
6. **Data backup and recovery:** Technologies should have robust data backup and recovery process in place to protect against data loss.
7. **Support:** Technologies should provide timely and reliable support in the event of a security breach or other issue.

Evaluation Phase: Additional factors for consideration (2 of 2)

Data Accuracy and Scalability (Technology Requirements)

1. **Data quality:** Data quality tools and processes should be in place to ensure that the data is accurate, complete, and consistent, including tools for data cleansing, deduplication, and data validation.
2. **Data governance:** The presence of a data governance framework is vital to ensure that data is properly managed, secured, and compliant with relevant regulations and standards.
3. **Scalability:** Technologies need to scale up or down to support companies' changing needs, including the ability to handle large amounts of data and a high volume of concurrent users or transactions.
4. **Performance:** Fast query and data processing times are important to ensure that users can access the data they need quickly and efficiently.
5. **Integration:** The ability to easily integrate with other systems and tools such as extract, transform, and load (ETL) tools, analytics platforms, and data visualization tools.
6. **Support:** Documentation, training resources, and customer support are crucial to help users effectively use and maintain the technology.

Human Capital and Talent

1. **Skills and expertise:** Bring together leaders with varying skillsets (data, technology, marketing, and privacy). Ensure your company is also hiring and retaining people with privacy technology expertise.
2. **Training and development:** Provide ongoing training and development opportunities to ensure that the team has the necessary skills to support the technology. This may include formal training programs, as well as opportunities for on-the-job learning and professional development.
3. **Team size and structure:** The size and structure of the team supporting the technology should be appropriate for the scale and complexity of the technology. This may involve having a dedicated team or a hybrid team that supports multiple platforms.
4. **Staff retention:** High staff turnover can be disruptive and costly, so it is important to have strategies in place to retain key team members. This may include competitive salaries, benefits, and opportunities for career advancement.
5. **Collaboration and communication:** The team should have strong collaboration and communication skills to work effectively together and with other stakeholders, such as users, vendors, and senior management.
6. **Culture and values:** The team's culture and values should align with those of the company and support the overall goals and objectives of the platform. This can help create a positive and productive work environment.

Methodology

Partnered With Ipsos

IAB commissioned Ipsos to co-create and execute a quantitative and qualitative analysis to examine how data clean rooms (DCRs) and other privacy-preserving technology including customer data platforms (CDPs), consent management platforms (CMPs), data management platforms (DMPs), and identity solutions are being managed and activated.

Quantitative Sample Generated and Execution

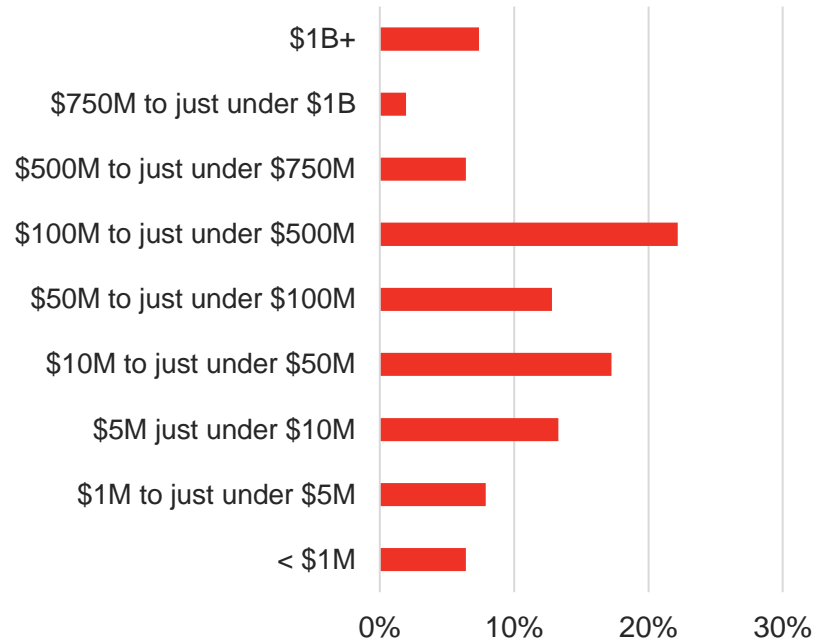
- 15-minute anonymous online survey, n=203
- Ipsos leveraged NewtonX B2B sample methodology to recruit verified data decision-makers who are engaged with privacy-preserving technology across the following company types:
 - Brands
 - Publishers/Retailers
 - Agencies
- Fielded: November 11 to 23, 2022

Qualitative Sample Generated and Execution

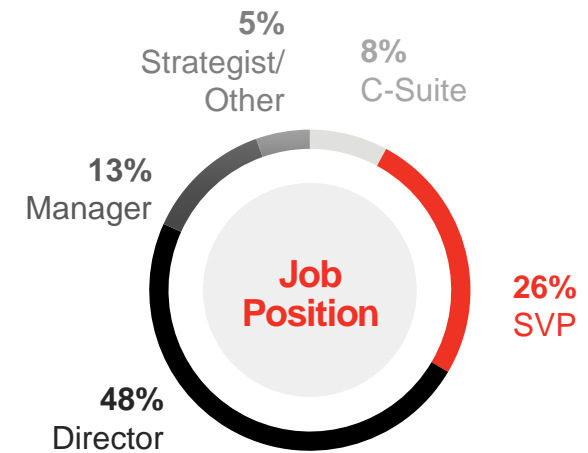
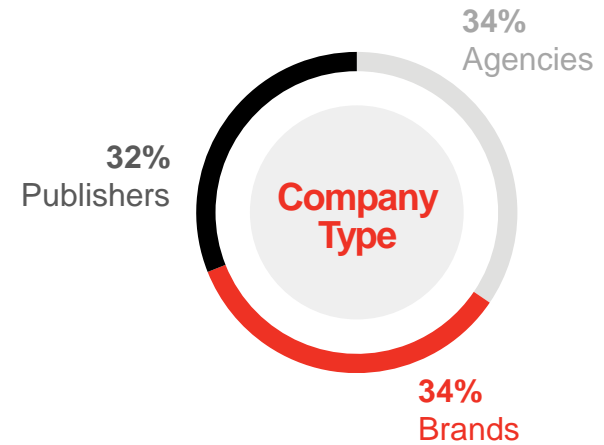
- 30-minute interviews with 20 industry leaders, with representatives across the following company types: brands, agencies, publishers, and retailers/retail media networks
- Fielded: November-December 2022

Respondent Profile

2022 Ad Spend



● 2022 ad spend for primary brand / account



About IAB

The [Interactive Advertising Bureau](#) empowers the media and marketing industries to thrive in the digital economy. Its membership comprises more than 700 leading media companies, brands, agencies, and the technology firms responsible for selling, delivering, and optimizing digital ad marketing campaigns. The trade group fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. In affiliation with the IAB Tech Lab, IAB develops technical standards and solutions. IAB is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of its public policy office in Washington, D.C., the trade association advocates for its members and promotes the value of the interactive advertising industry to legislators and policymakers. Founded in 1996, IAB is headquartered in New York City.



About the IAB Measurement, Addressability & Data Center

The collection and use of data to reach audiences and measure online advertising campaigns is central to powering the digital advertising ecosystem. IAB's [Measurement, Addressability & Data Center](#) aims to provide essential industry guidance and education on solutions amid changes in underlying technology, privacy regulations in a constantly evolving ecosystem.

- Develop measurement and addressability standards, best practices, and guidelines for digital media.
- Identify requirements for improving data assets for brand suitability, brand safety, transparency, and trust.
- Provide updated standard IAB Terms & Conditions to allow companies to transact more efficiently.
- Deliver guidance on new addressability and measurement solutions of known and unknown audiences and/or changes in the marketplace.
- Accelerate the development of effective emerging markets, such as retail media networks, data clean rooms, etc.



IAB Measurement, Addressability & Data Center Board Member Companies:



About Ipsos

Ipsos is the third largest market research company in the world, present in 90 markets and employing more than 18,000 people.

Our research professionals, analysts, and scientists have built unique multi-specialist capabilities that provide powerful insights into the actions, opinions, and motivations of citizens, consumers, patients, customers or employees. Our 75 business solutions are based on primary data coming from our surveys, social media monitoring, and qualitative or observational techniques.

“Game Changers” – our tagline – summarises our ambition to help our 5,000 clients to navigate more easily our deeply changing world.

Founded in France in 1975, Ipsos is listed on the Euronext Paris since July 1st, 1999. The company is part of the SBF 120 and the Mid-60 index and is eligible for the Deferred Settlement Service (SRD).

ISIN code FR0000073298, Reuters ISOS.PA, Bloomberg IPS:FP
www.ipsos.com



Game Changers

In our world of rapid change, the need for reliable information to make confident decisions has never been greater.

At Ipsos we believe our clients need more than a data supplier, they need a partner who can produce accurate and relevant information and turn it into actionable truth.

This is why our passionately curious experts not only provide the most precise measurement, but shape it to provide True Understanding of Society, Markets and People.

To do this, we use the best of science, technology and know-how and apply the principles of security, simplicity, speed and substance to everything we do.

So that our clients can act faster, smarter, and bolder.

Ultimately, success comes down to a simple truth:

You act better when you are sure.

About our Sponsors



Principal Sponsor

The Marketing Solutions business at Neustar, Inc., a TransUnion company, powers the next generation of privacy-enhanced identity data enrichment, omnichannel audience targeting, and advanced analytics to transform marketing and media performance.

Additionally, Neustar offers industry-leading solutions in risk and communications that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Learn how your company can benefit from the power of trusted connections. home.neustar

Platinum Sponsor

[Dstillery](http://dstillery.com), the custom audience solutions company, empowers brands and agencies to reach their best customers across the programmatic web. Backed by our award-winning data science, Dstillery has earned 16 patents (and counting) for the AI technology that powers our precise, scalable solutions. Our newest innovation, ID-free Custom AI, is a privacy-by-design behavioral targeting solution that performs on par with cookies — without user tracking. Our ID-based premier product, Custom AI Audiences, is a just-for-your-brand targeting solution that continuously scores hundreds of millions of users to deliver the best audiences for your brand.

To learn more, visit us at www.dstillery.com or follow us on [LinkedIn](https://www.linkedin.com/company/dstillery).

Premier Sponsor

Adstra is the new model for the data-driven enterprise. Adstra comprises a comprehensive suite of transparent identity and data solutions that are portable, futureproofed, and offered via a subscription-based model that liberates brands to realize the maximum value from their data. As the first Enterprise Identity Platform, Adstra enables the flexibility to activate identity management and data capabilities within your existing technology environments. In addition, Adstra connects brands with authenticated audiences tailored to specific business objectives. No other data provider bridges the gaps between PII and anonymized data with the same speed, flexibility, cost-effectiveness, and frictionless portability across all media.

Title Sponsor

Comscore is a trusted partner for planning, transacting, and evaluating media across platforms. With a data footprint that combines digital, linear TV, over-the-top, and theatrical viewership intelligence with advanced audience insights, Comscore allows media buyers and sellers to quantify their multiscreen behavior and make business decisions with confidence. A proven leader in measuring digital and TV audiences and advertising at scale, Comscore is the industry's emerging, third-party source for reliable and comprehensive cross-platform measurement.



A Perspective from Neustar, a TransUnion Company: Becoming a Data Leader

Sponsored Content

In 2023, marketers face the difficult question of how to shore up their consumer engagement and acquisition strategies in the face of privacy regulation and data deprecation. The need for improved privacy controls has driven the rise of data clean rooms (DCRs). The loss of data signals associated with cookies and mobile ad IDs has forced us to re-evaluate how we collect, enrich, activate, and measure consumer data. So how should we adapt to these new and developing paradigms in the data-driven marketing world?

Our clients are addressing the consumer privacy and data loss challenges in a few different ways like leveraging back-to-basics contextual targeting, developing partnerships across the rapidly growing connected TV and retail media spaces, or unlocking new sources of second-party data by collaborating with trade and ecosystem partners.

Those that seize the opportunity to test, learn, and adapt to the consumer data challenges we all face will become the data leaders of tomorrow. These leaders will be busy in 2023 building and executing an addressable marketing strategy rooted in privacy, with clearly defined use cases and data requirements at its core.

As many marketers have learned, technology is only as valuable as what you put into it. Clear use cases must precede investments in next-generation marketing technology like DCRs. First, take inventory and define the challenges you face, such as increasing customer acquisition costs, decreasing addressable audience reach, and/or the inability to measure incremental ROI across channels. Linking these pain points to a specific action and a potential set of outcomes will help provide a path.

Second, identify the data types and sources that you need to fulfill your key outcomes. As an example, if optimizing marketing contribution to revenue is the goal of a large consumer goods company, the marketing team will need to consider a variety of owned and partner media and sales channel data sources, both offline and online.

The team should start by thoroughly evaluating the consumer data it has—or can access—across its first-, second-, and third-party data sources spanning these channels. By beginning its journey with a multi-faceted data strategy (across multiple potential data partners) at its core, the team greatly increases its chance of success of not only measuring across channels, but also seeing the incremental contribution of each. This is key to effective marketing optimization.

Finally, it's time to apply consumer data to use cases in a privacy-focused way, and that means implementing the right infrastructure and a clear data taxonomy. Too often, evaluating privacy technology before identifying use cases and data leads to unnecessary work. Data leaders, and data and technology partners should walk through a clear set of requirements and concerns that data owners and users have, such as the risk of re-identification. Additionally, data controllers can help their partners use only the data they need, for example by running a travel-oriented campaign based on an anonymized cohort of consumers with similar destination interest. Trusted partners will candidly discuss how to mitigate and manage their concerns.

Successful data leaders in our privacy-focused and increasingly data deprived world will navigate these intertwined parameters of privacy requirements, use cases, and data, and bring the strength of their organizations to bear.

Written by
Brett House
Global Vice President,
Marketing Solutions,
TransUnion



Written by
Sam Shapiro-Kline
Director of Growth,
TransUnion



Thank You!

Research & Insights

- Chris Bruderle, Vice President, Industry Insights & Content Strategy (chris@iab.com)
- Meredith Guinness, Senior Manager (meredith@iab.com)

Measurement, Addressability & Data Center

- Jeffrey Bustos, Vice President (jeffrey@iab.com)
- Angelina Eng, Vice President (angelina@iab.com)

iab.