iab.

DATA CLEAN ROOMS:
A U.S. State Privacy Law Perspective

April 2025

Sponsored by orrick

TABLE OF CONTENTS

I. INTRODUCTION

The use of data clean rooms ("DCRs") for analytics, measurement, profile augmentation, and campaign planning is ubiquitous throughout the digital advertising industry. A DCR is a data collaboration environment, often provided by a vendor, that allows two or more participants to leverage data assets for mutually agreed-upon use cases, while enforcing strict data access limitations and security controls.[1] In essence, DCRs offer a privacy and security-enhanced data processing environment that allow companies to match and analyze personal information [2] ("PI") without exposing their raw underlying PI data sets to the other data collaboration party. These privacy-enhancing technologies ("PETs") include encryption, hashing, salting, noise injection, among others.

Several privacy myths have developed in the marketplace around DCRs. One is that PI does not "move" and, therefore, is not disclosed to DCRs (or any other party). Another myth is that, by using a DCR, privacy compliance is automatically guaranteed and falls outside of the privacy laws because PI is deidentified when processed by the DCR. This whitepaper debunks these myths, clarifies how U.S. state privacy laws apply to DCRs, and concludes:

- **DCRs process personal information, and PETs do not guarantee deidentification.** Data Contributors (as defined below) process PI in DCRs. Most PETs render such data pseudonymized.[3] We have not seen a use case where a DCR processes only deidentified PI for measurement, attribution, campaign planning, or similar use cases and is thus exempted from the reach of U.S. state privacy laws. That said, DCRs can process PI and generate deidentified *outputs* – typically for measurement and analytics purposes.
- **PI is disclosed to, and therefore "sold" to, DCRs if no service provider/processor relationship is established between a Data Contributor and a DCR.** At a minimum, DCRs process PI on an ephemeral basis. In other words, Data Contributors disclose personal information to DCRs, and DCRs process it even if the DCR promptly deletes it from the DCR application.

[1] *See* Data Clean Rooms Guidance and Recommended Practices (v.1.0), IAB Tech Lab, February 16, 2023, at 10, https://iabtechlab.com/wp-content/uploads/2023/02/FINAL-DRAFT-PUBLIC-COMMENT-Data-Clean-Room-Guidance-IAB-Tech-Lab.pdf.

[2] In this white paper, personal information ("PI") has the same definition as the terms "personal information" and "personal data" under applicable U.S. state privacy laws.

[3] "Pseudonymized" has the same meaning as defined under U.S. state privacy laws. *See., e.g.*, Cal. Civ. Code § 1798.140(aa). For clarity, pseudonymized information is still personal information.

- **In most commercial use cases of which we are aware, the Data Contributors, rather than the DCR, are the "business" or "controller," as defined under U.S. state privacy laws.**
- **Under most U.S. state privacy laws, Data Contributors can establish a service provider/processor relationship with DCRs for measurement, analytics, campaign planning, and profile augmentation use cases.** However, some regulatory uncertainty remains in California regarding these use cases.
- **Data Contributors should construe a "sale" between each other (either unidirectional or bi-directional) or their designated ad tech partners and ensure compliance with opt-out rights accordingly for certain use cases that generate record-level personal information.** For instance, when DCRs are used for campaign planning and profile augmentation that generate individual record-level outputs, a "sale" should be construed between Data Contributors or between Data Contributors and their respective DSPs/SSPs.

II. SCOPE OF DISCUSSION

This whitepaper does not address complementary services that DCRs frequently offer in conjunction with their core technology. For example, some businesses operating a DCR not only facilitate data collaboration, but also contribute and merge their own PI to enhance a Data Contributor's data—effectively acting as both a data broker and a DCR provider. Similarly, some businesses operating a DCR also run ad inventory on their own properties and leverage contributed PI to retarget their own audiences, blurring the line between a DCR provider and a publisher.

These ancillary uses of contributed PI introduce a separate layer of complexity and are subject to additional legal scrutiny under U.S. privacy laws. Factors such as the purpose of data use, the scope of user consent, data sharing arrangements, and transparency practices must be analyzed to determine the roles and obligations to which the DCR is subject under these use cases. Such analysis is outside the scope of this whitepaper.

This whitepaper also does not encompass all potential privacy considerations, such as data minimization, data subject consent, or platform-specific privacy requirements, such as Apple's App Tracking Transparency (ATT) framework. Organizations should remain mindful of broader privacy obligations that extend beyond the scope of this discussion.

III. KEY ROLES IN DATA CLEAN ROOMS

There are several key participants in a DCR:

A. DATA CONTRIBUTOR: Provides its data to a DCR.[4]

B. DCR PROVIDER: Supplies the application and query interface for performing computations or extracting insights by querying the data provided by the Data Contributors.[5]

C. DCR USER: Uses the DCR to run queries and extract outputs and insights from the data provided by Data Contributors. The DCR User may or may not contribute data or provide the DCR environment.[6]

There are other roles relevant to DCR operations, such offering enhanced or value-added services for data management or computation (e.g., predictive modeling, identity resolution, or retargeting).[7] There are also DCR infrastructure providers, such as AWS, on which DCR Providers operate their proprietary applications. These other roles fall outside the scope of this whitepaper.

IV. HOW DO DCRs WORK?

A. DCR INFRASTRUCTURE DESIGNS AND DATA FLOWS

The IAB Legal Affairs Council reviewed DCR setups and data flows amongst the key DCR Providers and created a set of descriptions that normalizes proprietary differences. These descriptions are simplified for analytical purposes and do not cover all possible DCR configurations or data flows. We categorized different models based on two factors:

1. Does the DCR require Data Contributors to copy and transfer PI stored from the Data Contributors' respective IT environments to the DCR Provider's environment? [8]
2. Does the DCR application run in the DCR Provider's environment or in at least one of the Data Contributor's environments?

---

[4] *See infra*, Data Clean Rooms Guidance and Recommended Practices (v.1.0), at 16.

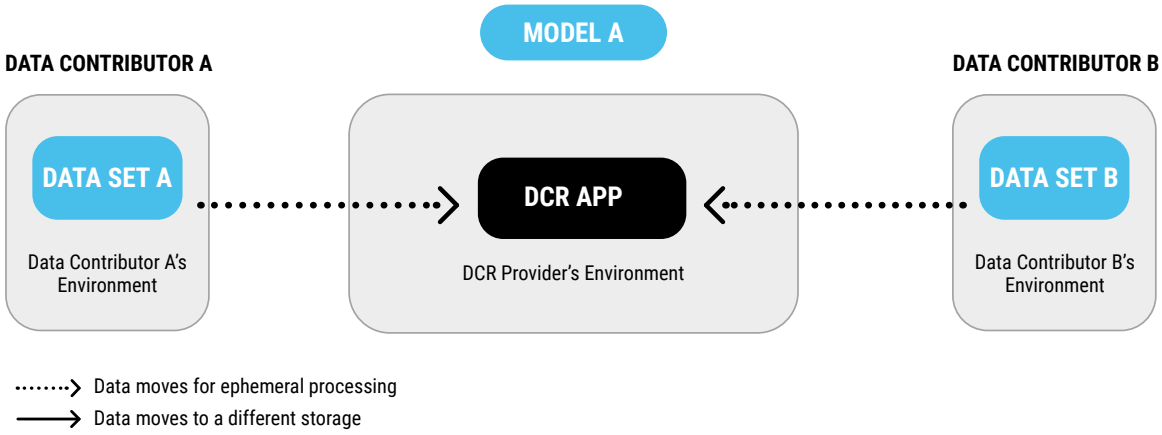
[5] *Id.*

[6] Id. To avoid confusion, this white paper refers to the term "Data Consumer," as defined in the IAB Tech Lab's *Data Clean Rooms Guidance and Recommended Practices*, as "Data User." This distinction is made because the term "consumer" often carries specific legal implications under U.S. state privacy laws, and using "Data User" helps clarify the intended meaning in this context.

[7] *Id.*

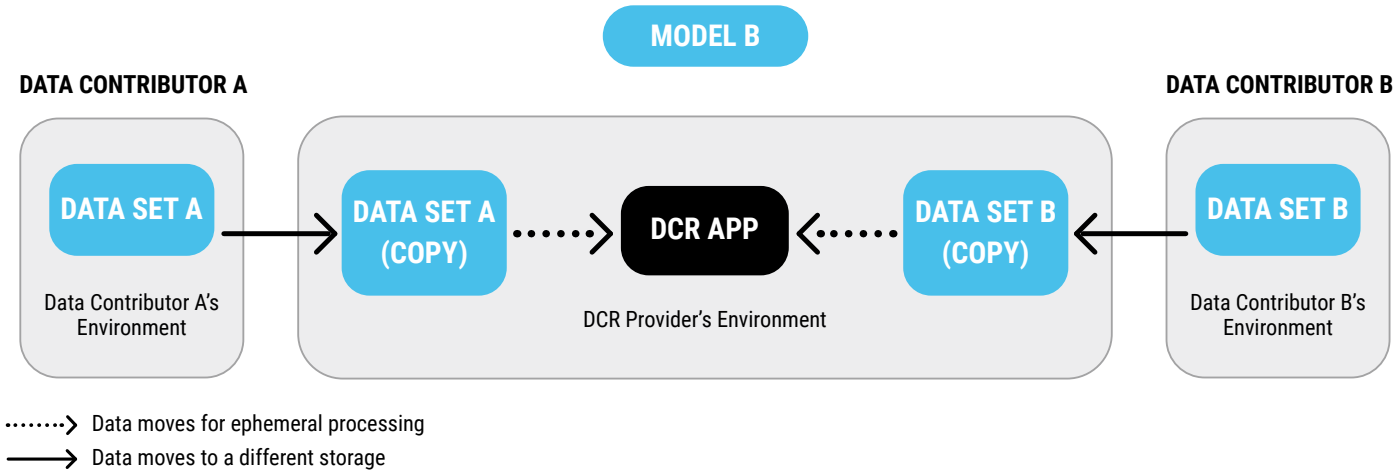
[8] Note that the PI typically remains logically segregated after moving. Logical segregation uses software or other tools to separate data into logical partitions or storage areas to control access and protect information. This can be done even if the partitions or storage are on the same physical device. *See* https://www.privacyengine.io/resources/glossary/data-segregation/

Models	Does the DCR Require the Transfer of PI from the Data Contributor Environment into the DCR Environment?	In Whose Environment Does the DCR Application Process PI?
A	No	DCR Provider
B	Yes	DCR Provider
C	No	Data Contributor



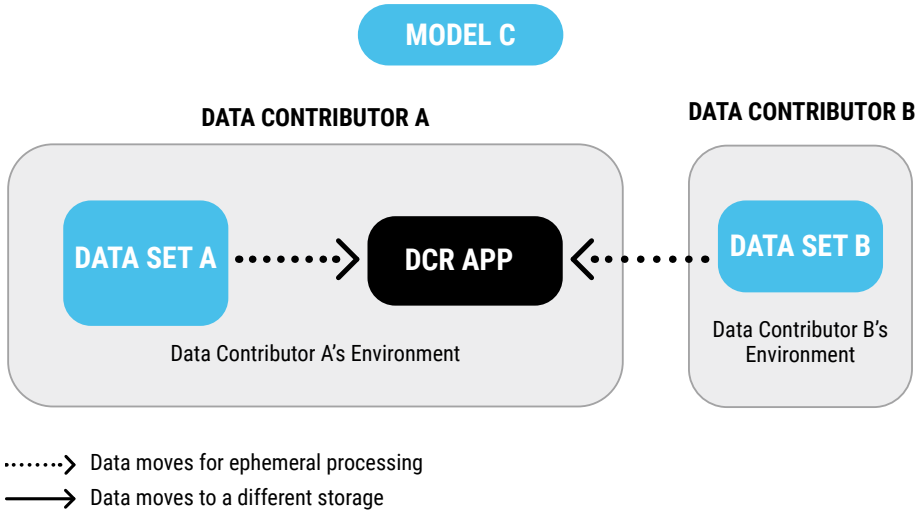
Key Characteristics of DCR Model A

1. Data Contributors store their PI in their respective IT environments (e.g., on-premises or in the cloud).
2. DCR Provider operates its DCR application in the DCR Provider's environment.
3. At the instruction of Data Contributors, DCR Provider queries PI stored in both Data Contributors' environments and ephemerally processes PI for matching and analysis within the DCR's application.
4. DCR Provider sends the data output to one or more Data Contributors or third parties per Data Contributors' instructions.
5. DCR application does not persist PI, meaning that PI is deleted immediately after the ephemeral processing.



Key Characteristics of DCR Model B

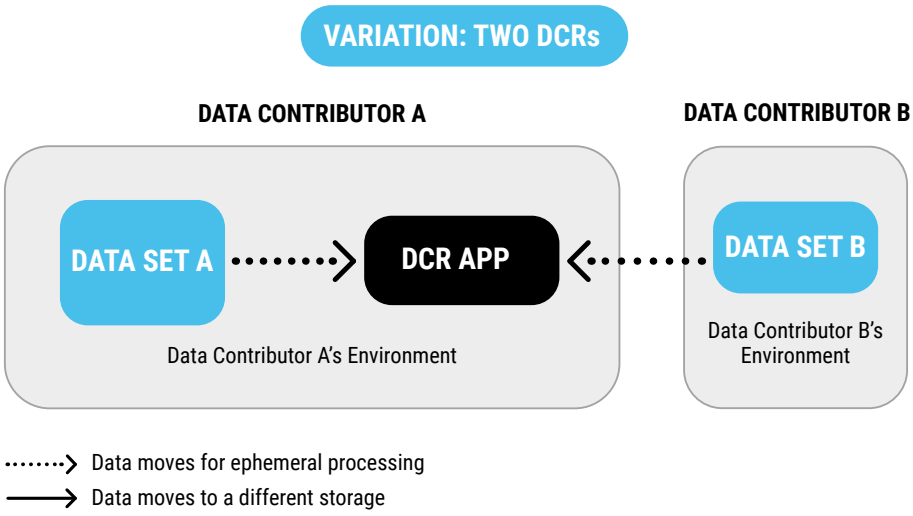
1. Data Contributors may copy or instruct the DCR Provider to copy and store the Data Contributors' respective PI into their respective instances in DCR Provider's environment. Each Data Contributor's PI remains technically segregated, and neither Data Contributor has access to the other Data Contributor's instance.
2. DCR Provider operates its DCR application in the DCR Provider's environment.
3. DCR Provider queries PI from Data Contributors and ephemerally processes PI for matching and analysis in the DCR Application.
4. DCR Provider sends the data output to one or more of Data Contributors or third parties per Data Contributors' instructions.
5. DCR application does not persist PI, meaning that PI is deleted immediately after the ephemeral processing.



Key Characteristics of DCR Model C

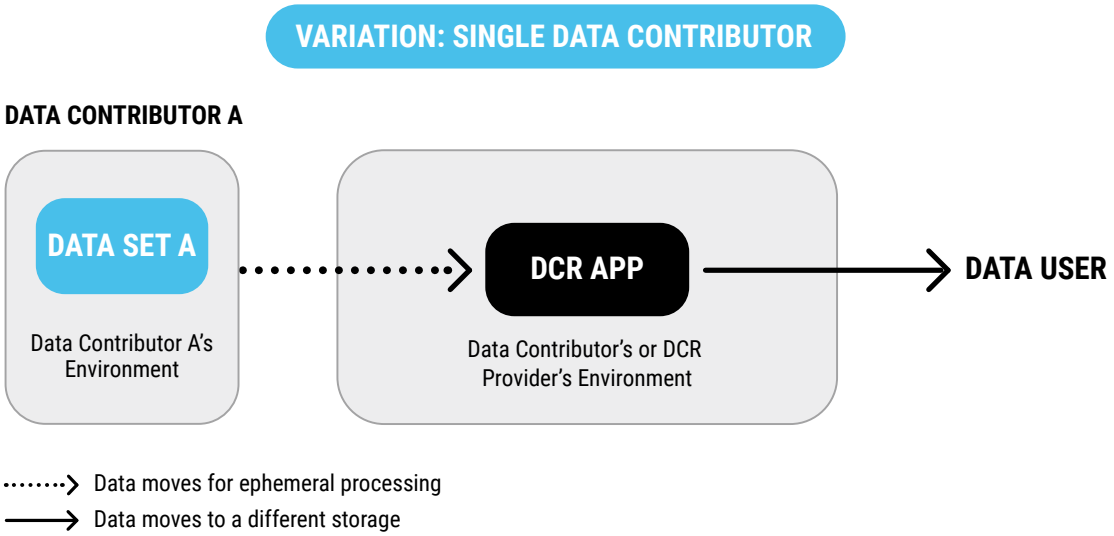
1. Data Contributors' PI is stored in their respective environments.
2. DCR Provider operates its DCR application in Data Contributor A's environment.
3. DCR Provider queries PI from Data Contributor B's environment and ephemerally processes PI for matching and analysis within Data Contributor A's environment.
4. DCR Provider sends the data output to one or more of the Data Contributors or third parties per the Data Contributors' instructions.
5. DCR application does not persist PI, meaning that PI is deleted immediately after the ephemeral processing.

Potential combinations of the models above exist when each Data Contributor designates its own DCR Provider. In the following example, at least two DCR Providers are involved. Other variations are available, depending on the environment DCRs operate in and whether the DCR Provider copies and stores PI in its own environment.



Key Characteristics of Variation: Two DCRs

1. Data Contributors designate their own DCRs.
2. Data Contributors' PI is stored in their respective environments (e.g., on-premise or in the cloud).
3. Each DCR Provider may operate its DCR application in a DCR Provider's environment (see DCR A) or in a Data Contributor's environment (see DCR B).
4. Each DCR Provider may either query PI stored in a Data Contributor's environment or copy a Data Contributor's PI into its DCR Provider's environment.
5. DCR A and DCR B may each or mutually query data in each others' DCR environment (depending on the use case) and ephemerally process data matching and analysis.
6. DCR A and DCR B send the data output to one or more of Data Contributors or third parties per their respective Data Contributors' instructions.



Key Characteristics of Variation: Single DCR

1. Data Contributor designates its own DCR.
2. Data Contributors' PI is stored in its own environment (e.g., on-premise or in the cloud).
3. The DCR Provider may operate its DCR application in a DCR Provider's environment or in the Data Contributor's environment.
4. DCR Provider may either query PI stored in a Data Contributor's environment or copy a Data Contributor's PI into its DCR Provider's environment.
5. DCR User runs queries in the DCR to extract outputs and insights from the data provided by Data Contributors. The data user does not contribute data or provide the DCR environment.
6. DCR applications do not persist PI, meaning PI is deleted immediately after the ephemeral processing.
7. The above variation is often used in measurement, analytics, and insight use cases, such as for brands to evaluate campaign efficacy in retail media networks.[9] The output is often, but not always, aggregated.

[9] *See* How Retailers Are Using Data Clean Rooms, IAB at https://www.iab.com/blog/how-retailers-are-using-data-clean-rooms/.

B. TYPICAL DCR USE CASES

Data Contributors in the digital advertising industry typically use DCRs for analytics and insights, measurement, profile augmentation, and campaign planning purposes (or a combination of such purposes).

1. **ANALYTICS & INSIGHTS:** Use of Data Contributors' PI for aggregated reporting, such as percentage of overlap or total count of unique PI records in multiple data sets.
2. **MEASUREMENT:** Use of Data Contributors' PI (e.g., click/view and conversion data) to report and analyze the performance of advertising campaigns.
3. **PROFILE AUGMENTATION:** Use of Data Contributors' PI in combination with another Data Contributor's PI to improve knowledge about an audience (e.g., preferences, inferences, characteristics, and behaviors). In the context of profile augmentation, when one Data Contributor's personal information enhances another party's dataset at an individual record level, the process often involves appending customer profile information, such as customer affinities or demographic details.
4. **CAMPAIGN PLANNING:** Use of Data Contributors' PI to create audiences for targeting ads, such as creating segments based on matching audience files or creation of models for look-a-like audiences (e.g., using analysis and machine learning to find new audiences similar to the existing overlapping database).

C. DATA COLLABORATION STEPS

The following operations are generally performed when leveraging DCRs for the various use cases described above.[10]

1. **DATA CONNECTION:** DCR Provider allows Data Contributors to connect their databases to the DCR and define the format and structure (e.g., data types and data fields).
2. **DATA TRANSFORMATION:** DCR Provider and/or Data Contributors may assemble the data in a form and shape ready to match such data with other data sets. This involves converting and organizing the data in a consistent format to ensure uniformity, remove redundancies, and improve the integrity of data. It can include changing the structure and format of data.
3. **DATA STAGING:** DCR Provider may require Data Contributors to copy PI into the Data Contributors' respective data storage instances in the DCR environment. The DCR Provider may also allow Data Contributors to store PI in their respective environments.
4. **DATA PREPARATION:** DCR Provider and/or Data Contributors may apply PETs and convert data to pseudonymized values. DCR Provider and/or Data Contributors can apply PETs, depending on their contractual arrangement.

[10] *See infra*, Data Clean Rooms Guidance and recommended Practices (v.1.0), at 17.

5. **DCR ENVIRONMENT AND INTERFACE:** DCR Provider may provide a user interface or a script/application programming interface for parties to interact with the DCR.
6. **DATA COMPUTATION:** DCR Provider provides different computational services requested by Data Contributors to collaborate on PI. Common collaboration types include determining the volume of overlapping records or the total volume of mutually exclusive records or using the underlying data for data modeling (e.g., look-a-like audiences).
7. **DATA OUTPUT:** DCR Provider generates computational output, which may be aggregated[11] (e.g., customer overlapping analysis, brand/sales lift analysis, reach and frequency analysis, and attribution report). It may also generate individual record-level output for customer profile augmentation, campaign planning (e.g., creating new audience lists as part of campaign optimization), or post-campaign measurement.

D. APPLICATION OF PRIVACY ENHANCING TECHNOLOGIES

PETs have many privacy and security benefits, such as reducing data leakage, enhancing data security, and minimizing data proliferation. These technologies aim to safeguard personal information from unauthorized access, use, and disclosure.

DCRs are commonly implemented in conjunction with one or more privacy-enhancing technologies such as hashing, salting, encryption, differential privacy,[12] secure multi-party compute,[13] commutative encryption,[14] or homographic encryption[15] to accomplish complex data processing functions for sharing and analysis without revealing raw personal information and without decrypting encrypted data.

[11] "Aggregated" means information that relates to a group or category of consumers from which individual consumer identities have been removed that is not linked or reasonably linkable to any consumer or household, including via a device. *See* Cal. Civ. Code § 1798.140(b).

[12] Differential privacy is a mathematical technique to rigorously guarantee a specific level of privacy for an operation by injecting noise.

[13] Secure multi-party compute is a technology where multiple parties perform a computation keeping their data private from each other and yet infer the overall results and insights.

[14] Commutative encryption is a type of encryption where double encryption using two different keys produces ciphertext that can be correctly decrypted only by using the keys in an arbitrary order. It is a way to enhance privacy, as it requires two keys from two different parties to decrypt the ciphertext, which provides an additional layer of protection.

[15] Homomorphic encryption is a type of encryption that allows a party to perform computation on data while the data are still encrypted.

V. DO U.S. STATE PRIVACY LAWS APPLY TO DATA CLEAN ROOMS?

One common myth is that DCRs convert PI into deidentified data and, therefore, such processing falls outside the purview of U.S. state privacy laws. This myth is erroneous and must be debunked.

Based on our interviews with representatives of major DCR Providers, we have not identified a use case whereby DCRs process only deidentified PI, as defined under U.S. state privacy laws, to compute and generate output results. Most PETs convert the underlying personal information, whether directly identifying or pseudonymous, to a set of unique deterministic or probabilistic identifiers for each record–in other words, a pseudonymous digital representation of individual consumers. As we discuss in more detail below, clean rooms still match "unique identifiers"[16] that are "capable of being associated" or are otherwise "linked" to a "consumer."[17] Therefore, such unique identifiers, either deterministic or probabilistic, constitute "personal information,"[18] as defined under U.S. state privacy laws. The fact that the DCR cannot connect the identifiers to the original personal information might be positive for data security purposes but does not render the DCRs outside the ambit of U.S. state privacy laws.

A. IS THE RECORD-LEVEL INPUT DATA PROCESSED BY A DCR DEIDENTIFIED?

A pseudonymized record-level identifier in a DCR is PI and does not fit within the definition of "deidentified" data under U.S. state privacy laws, as illustrated in the California Consumer Privacy Act ("CCPA") definition of "deidentified:"

> Information that cannot reasonably be used to ***infer information about, or otherwise be linked to, a particular consumer*** provided that the business that possesses the information: (1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household; (2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information

[16] "Unique identifier" means "[a] persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or *other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device* that is linked to a consumer or family. *See, e.g.*, Cal. Civ. Code § 1798.140(aj) (emphasis added).

[17] "Consumer" means "a natural person who is a California resident however identified, including by any unique identifier after *See, e.g.*, Cal. Civ. Code § 1798.140(i), Conn. Gen. Stat. § 42-515(7), Colo. Rev. Stat. 6–1–1303(6).

[18] Under U.S. state privacy laws, "personal information" or "personal data" is typically defined as "information that identifies, relates to, describes, is reasonably *capable of being associated with*, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *See, e.g.*, Cal. Civ. Code § 1798.140(v) (emphasis added), Conn. Gen. Stat. § 42-515(18), Colo. Rev. Stat. 6–1–1303(17).

> solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision, (3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.[19]

The key test for determining if data are deidentified is whether the information can be used to infer information about, or otherwise be linked to, an individual. When applying one or more PETs described above – whether encryption, hashing, or salting – Data Contributors' respective data sets are converted by the DCR Provider into unique deterministic or probabilistic identifiers that link particular individuals from both record sets within the DCR environment. Therefore, the information is still PI; it is a unique, persistent identifier that is able to link a consumer across data sets, even if such linkage can occur only in an isolated environment like a DCR application. Stated simply, the record-level data in the DCR is still a digital representation of the consumer. There are misconceptions that, because the hashed, salted, and/or encrypted value is nearly impossible to revert to the underlying raw PI (even with a brute force attack using current technology), it is no longer "linked to a particular consumer." Such an argument is incorrect, because whether the hashed, salted, or encrypted value can revert to the raw PI is simply irrelevant to determine when a value is PI.

This analysis is aligned with a recent FTC blog post,[20] which arrives at a similar conclusion in the context of whether hashed data are anonymous (but the principle applies to other forms of cryptography discussed above):

> This logic is as old as it is flawed – ***hashes aren't "anonymous" and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized***. FTC staff will remain vigilant to ensure companies are following the law and take action when the privacy claims they make are deceptive.
>
> Regardless of what they look like, all user identifiers have the powerful capability to identify and track people over time. Therefore, ***the opacity of an identifier cannot be an excuse for improper use or disclosure.*** (Emphasis added)

B. IS THE OUTPUT GENERATED BY A DCR DEIDENTIFIED?

DCRs can generate outputs at the individual record level, which can be used for targeted advertising or profile augmentation. In particular, the record-level pseudonymized data output generated by DCRs is often combined with additional data to re-identify a person for

[19] *See, e.g.*, Cal. Civ. Code § 1798.140(m) (emphasis added), Conn. Gen. Stat. § 42-515(13), and Colo. Rev. Stat. 6–1–1303(11).

[20] *See* No, hashing still doesn't make your data anonymous, at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

customer segmentation and targeting purposes. Of course, record-level consumer targeting cannot be performed without reasonably linking the information to the consumer. Therefore, such output is personal information.

DCRs may also generate aggregated or deidentified output for measurement and analytics purposes. Customer overlap analyses or frequency/lift analyses (e.g., 20% overlap) often generate aggregated/deidentified output relating to groups or categories of data in which individual consumer identities have been removed and are not linked or reasonably linkable to any consumer or household, including a device. However, DCRs must still process pseudonymized PI for these use cases in order to compute the final aggregated outcome.

In conclusion, the notion that DCRs transform PI into deidentified data and thereby are not processing PI within the scope of U.S. state privacy laws is a misconception that must be dispelled. DCRs typically process pseudonymized data, generating unique deterministic or probabilistic identifiers that remain capable of linking to individual consumers, even if not directly reversible to the original PI. These identifiers, persistent in nature and capable of linking individuals across datasets, meet the definition of personal information under U.S. state privacy laws.

VI. IS PERSONAL INFORMATION "SOLD" WHEN UTILIZING CLEAN ROOMS AND TO WHOM?

This section examines whether, for each DCR use case set forth in Section IV, personal information is "sold"[21] and how the "sale" relationship should be construed. Specifically, we will review the common claim that PI does not "move" when handled by DCRs and therefore cannot constitute a "sale." We will also examine, under U.S. state privacy laws, which parties are "controllers" or "businesses" that determine the purposes and means of PI processing. We will further review whether DCR Providers act as "service providers/processors" or "third parties" to the party to which personal information is "sold" or whether recipient Data Contributors or other parties in the ad tech stack are "third parties" in certain contexts.

A. IS PI DISCLOSED, AND THEREFORE "SOLD," TO DCRS WITHOUT ESTABLISHED SERVICE PROVIDER/PROCESSOR RELATIONSHIPS?

Certain market actors claim that PI does not "move" when processed through DCRs, and, therefore, the PI is not "disclosed" by the Data Contributor for privacy compliance purposes. Thus, the argument goes: if no disclosure occurs, then no "sale" takes place. However, the facts belie this claim.

[21] *See, e.g.*, Cal. Civ. Code § 1798.140(ad), Conn. Gen. Stat. § 42-515(22), and Colo. Rev. Stat. 6–1–1303(23).

The definition of "sale" includes "releasing, disclosing, disseminating, making available, transferring, or otherwise communicating" PI.[22] This means that the physical movement of data between storage locations is a relevant factor in determining whether PI is disclosed and therefore "sold." Also relevant is whether PI is "made available" from its original storage environment during ephemeral processing.

In DCR Model A,[23] Data Contributors' PI is disclosed to DCRs for ephemeral data processing and the data are deleted immediately thereafter. In Model B, Data Contributors' PI both moves to the DCR Providers' environment for storage before ephemeral processing, even if Data Contributors still maintain a high level of control of their PI in their own instances in that environment. In Model C, one Data Contributor's PI is made available to the DCR residing in the other Data Contributor's environment for ephemeral processing.

In all cases, even if the Data Contributors' PI does not persist (i.e., PI is immediately deleted after the matching), it is still transferred and disclosed to the DCR, even if only transiently This movement of PI to a DCR constitutes a "disclosure" and qualifies as "making available" PI, which meets the definition of "sale" under state privacy laws unless an exemption applies—such as when a service provider or processor relationship is properly established between a Data Contributor and a DCR.[24]

B. WHICH PARTY IS THE "BUSINESS" OR "CONTROLLER" THAT DETERMINES THE PURPOSES AND MEANS OF PROCESSING?

In most commercial use cases, the Data Contributors, rather than the DCR Provider, are the "business" or "controller," as defined under U.S. state privacy laws. Typically, those laws define a "business" or "controller" as a person that "alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information."[25] Data Contributors who leverage DCRs determine what data (whether first- or third-party data) to send to a DCR for matching. Data Contributors then determine for what use cases the PI should be processed (e.g., what queries can be made upon data), choose the types of PETs to be applied, and instruct the DCR Provider with whom the output data should be shared.[26]

[22] Cal. Civ. Code § 1798.140(ad).

[23] *See* all model descriptions under Section IV(A) this whitepaper.

[24] Cal. Civ. Code § 1798.140(ad)(2) and (aj).

[25] *See, e.g.*, Cal. Civ. Code § 1798.140(d) and Colo. Rev. Stat. 6-1-1303(7).

[26] For the avoidance of doubt, if the DCR provides any additional services referenced in the introduction section of this article, the DCR may become a "data controller" or "business," and additional legal analysis would be needed.

C. UNDER U.S. STATE PRIVACY LAWS, CAN A DATA CONTRIBUTOR CREATE A VALID SERVICE PROVIDER/PROCESSOR RELATIONSHIP WITH A DCR?

U.S. state privacy laws broadly define the "sale" of personal information to include "disclosing…personal information by the business to a *third party* for monetary or *other valuable consideration.*"[27] There are some notable exemptions to "sale," which include the disclosure of personal information to a processor that processes the personal information on behalf of a controller.[28] U.S. state privacy laws require processors to act under the direction of the controllers[29] and be bound by statutorily required contractual restrictions.[30] In other words, when DCRs act as service providers/processors to Data Contributors under a properly established service provider/processor relationship, Data Contributors do not "sell" personal information to DCRs.

There are nuances under the CCPA, particularly regarding the restrictions on service providers' combining personal information and the prohibition against contracting with a service provider for cross-context behavioral advertising. However, after examining the specific requirements under the CCPA—including whether a DCR can lawfully combine personal information for permitted business purposes and whether a DCR can match personal information for profile augmentation and campaign planning, given the CCPA's prohibition on service providers' engaging in cross-context behavioral advertising—our conclusion remains the same, as detailed in Section VII.

D. HOW TO CONSTRUE THE "SALE" RELATIONSHIP?

Even if both Data Contributors have established proper relationships with the DCR Provider, they must still assess whether PI is being sold through DCRs for each use case described in Section IV(B) of this whitepaper. The legal construct depends on myriad factors, such as whether the output data contain PI and how the output PI will be used.

A Data Contributor can engage and instruct a DCR to share individual record-level output for profile a augmentation with one or more Data Contributors, potentially in a bi-directional arrangement. Such augmentation enhances the recipient Data Contributors' PI or generates additional consumer insights (e.g., look-alike modeling for segmentation). Such use is for the recipient Data Contributors' own commercial or economic interests. Therefore, this transaction qualifies as a "sale" from a "controller" (i.e., the Data Contributor) to a "third-party" "controller" that now has enhanced data of which it controls the purposes and means of processing.

---

[27] *See, e.g.*, Colo. Rev. Stat. 6-1-1303(23) (emphasis added).

[28] *See, e.g.*, Colo. Rev. Stat. 6-1-1303(23).

[29] *See, e.g.*,, Colo. Rev. Stat. 6-1-1303(18).

[30] *See, e.g.*,, Cal. Civ. Code 1798.100(d), Cal. Code Regs. tits. 11, § 7051, and Conn. Gen. Stat. §42-521(b). Such restrictions usually include, but are not limited to, observing the duty of confidentiality, deleting or returning PI at the end of the provision of services, assisting the first party to demonstrate compliance, and cooperating with the first party for reasonable assessment.

Consequently, when a consumer opts-out of "sale," the PI must be excluded from use for profile augmentation. The prevailing market practice is to suppress the data from the DCR's processing.

Similarly, for campaign planning, a Data Contributor can engage and instruct a DCR to share individual record-level output with one or more recipient Data Contributors or their respective DSPs/SSPs. Such arrangement can also be bi-directional. Based on the same rationale, depending on the data flows, a "sale" should be construed between the disclosing Data Contributors and the recipient Data Contributors and/or between the disclosing Data Contributors and their respective DSPs/SSPs. Thus, when the consumer opts-out, PI must be removed from use for campaign planning. The prevailing market practice is to exclude the PI from the DCR's processing for the campaign planning use case.

For measurement and analytics use cases where Data Contributors engage the DCR as a service provider/processor, Data Contributors can instruct the DCR to generate measurement output that is either aggregated or at the individual record level. In the case of generating the aggregated output, a "sale" is not construed, because each Data Contributor does not receive PI in the output, and parties instruct the DCR to match personal information for "business purposes"[31] under the CCPA. When the measurement and analytics output is at the individual record level that is not fully deidentified, the prevailing market practice is to construe a "sale" between the Data Contributors and suppress the opted-out PI from the DCR's matching.

VII. CAN A DATA CONTRIBUTOR ESTABLISH A SERVICE PROVIDER RELATIONSHIP WITH A DCR UNDER THE CCPA

Although it is common for Data Contributors to engage DCRs as their service providers, there is significant legal uncertainty in the marketplace about whether, and under what circumstances, PI can be combined in DCRs or used for the ultimate purpose of cross-context behavioral advertising[32] under the CCPA.

Specifically, the CCPA prohibits service providers from combining PI received from different businesses unless it does so pursuant to a **"business purpose"**[33] (other than the marketing and advertising business purpose) or pursuant to a specific rule promulgated by the California Privacy Protection Agency ("CPPA"):

[31] Cal. Civ. Code § 1798.140(e)(1) (ad auditing), (4) (short-term, transient use), (5) (analytics service), and (6) (advertising and marketing).

[32] Cal. Civ. Code § 1798.140(k) (defining "cross-context behavioral advertising" as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts").

[33] Cal. Civ. Code § 1798.140(e).

> "Service Provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business a consumer's personal information for a business purpose pursuant to a written contract, ***provided that the contract prohibits the person from…combining the personal information*** that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, ***provided*** that the service provider may ***combine personal information to perform any business purpose*** as defined in regulations adopted ***pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency.***[34]

Furthermore, CCPA regulations impose the following restrictions:

> A service provider or contractor cannot contract with a business to provide cross-context behavioral advertising. Pursuant to Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but ***the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers.*** A person who contracts with a ***business to provide cross-context behavioral advertising is a third party*** and not a service provider or contractor with respect to cross-context behavioral advertising services.[35]

This section discusses in more detail these CCPA restrictions, including the relevant statutory language, regulatory background, and policy considerations for a more consumer-protective construction. We reach the same conclusion and legal construction set forth in Section VI(C) of this whitepaper: that a Data Contributor can create a valid service provider relationship with a DCR Provider.

A. UNDER THE CCPA, CAN A DCR LAWFULLY COMBINE PERSONAL INFORMATION FOR PERMITTED BUSINESS PURPOSES?

1. The intent of Section 7050 of the CCPA is to provide the parameters for permitted combinations of PI by service providers.

[34] Cal. Civ. Code §1798.140(ag)(1)(d) (emphasis added).

[35] Cal. Code. Regs. tit. 11 § 7050(b) (emphasis added).

The CCPA prohibits service providers from combining PI except pursuant to regulations promulgated under 1798.185(a)(10).[36] Upon reviewing the regulations and rulemaking history, we conclude that the CPPA promulgated Section 7050[37] of the CCPA to set forth the circumstances under which a service provider can combine PI received from multiple businesses. The regulation states that "a service provider or contractor shall not retain, ***use***, or disclose personal information collected pursuant to its written contract with the business" unless certain prescribed exemptions apply. Thus, the regulations set forth the limited parameters under which service providers can process PI on behalf of the business. The rule-maker's intent for such parameters to include "combinations" within "use" of PI in Section 7050 of the CCPA is clear in the preface to that section in the Final Statement of Reasons:

> These changes are necessary to clarify how service providers' and contractors' obligations apply to the personal information they collect or process pursuant to their written contract with the business, to make the regulation more precise, and to make it easier for companies and consumers to read and understand. These changes ar also necessary because Civil Code section 1798.185(a)(10) and (11), require th Agency to issue regulations identifying the business purposes and circumstances under which a service provider or contractor ***may use and/or combine*** consumers' personal information.[38]

This inference is also supported in the conclusion of Section 7050 in the Final Statement of Reasons:

> [The changes to Section 7050] clarify the limited ***circumstances in which service providers and contractors are allowed to combine personal information***, and thus, ensure that they are not using the personal information collected pursuant to the written contract for a commercial purpose other than for a business purpose specified in the contract or for a purpose permitted by the CCPA and these regulations.[39]

Importantly, any ambiguities must be interpreted in a manner that aligns with the intent of the statute. Here, the Final Statement of Reasons clarifies the limited circumstances where combinations of PI by service providers are permitted.

[36] Cal. Civ. Code § 1798.185(a)(10).

[37] Cal. Code. Regs. tit. 11 § 7050.

[38] *See* Final Statement of Reasons, available at: https://cppa.ca.gov/meetings/materials/20230203_item4_fsor.pdf, Page 25 (emphasis added).

[39] *See id.*, page 26 (emphasis added).

2. Section 7050(a) permits service providers to combine personal information pursuant to business purposes defined under the CCPA.

Under Section 7050(a) of the CCPA, a service provider may "retain, use, or disclose" PI for the "specific business purpose(s) set forth in the written contract between the business and the service provider or contractor that is required by the CCPA and these regulations." Because "use" encompasses combining PI, a DCR can combine PI for "specific business purpose(s)" when engaged as a service provider.

"Business purpose" is a defined term under the CCPA to include the use of PI for the business's operational purposes or other notified purposes or for the service provider's or contractor's operational purposes. The CCPA includes a list of "business purposes" such as auditing, security, debugging, maintaining or servicing accounts, short-term, transient use, analytics services, advertising, and marketing services.[40] "Business purposes" specifically excludes cross-context behavioral advertising, disclosing the personal information to another third party, or building a profile about the consumer.[41]

Data Contributors can engage DCRs as their service providers and, in doing so, combine PI for measurement, analytics, and insights purposes—each of which fits into several business purposes, including 1798.140(e)(1) (ad auditing), (4) (short-term, transient use), (5) (analytics service), and (6) (advertising and marketing). Because DCRs perform data computational services for Data Contributors, their use of DCRs as service providers for campaign planning and profile augmentation also fits into several business purposes, including 1798.140(e)(5) (analytics service) and (6) (advertising and marketing).

3. Section 7050(b) of the CCPA specifically permits service providers to combine personal information pursuant to marketing and advertising business purposes within certain parameters.

The CCPA provides that service provider combinations are permitted for marketing and advertising purposes, as long as (i) the service is not cross-context behavioral advertising,

[40] Cal. Civ. Code § 1798.140(e)(4) (stating: "Short-term, transient use, includ[es], but [is] not limited to, non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.").

[41] *See* Cal. Civ. Code § 1798.185(e).

and (ii) the personal information of opted-out consumers is not included.[42] Section 185(a)(10) of the CCPA also allows combinations for advertising and marketing purposes.[43]

Thus, a service provider is permitted to combine PI for marketing and advertising purposes (except for cross-context behavioral advertising, which is analyzed in the next section), as long as the personal information of opted-out consumers is excluded.[44]

B. CAN A DCR MATCH PERSONAL INFORMATION FOR PROFILE AUGMENTATION AND CAMPAIGN PLANNING PURPOSES CONSIDERING THE CCPA'S PROHIBITION OF SERVICE PROVIDERS FROM ENGAGING IN CROSS-CONTEXT BEHAVIORAL ADVERTISING?

Service providers are prohibited from engaging in cross-context behavioral advertising under the CCPA and its regulations.[45] Although the rule is perfectly clear, how it applies in a number of use cases, including for DCRs, is not. In other words, is cross-context behavioral advertising something done by ad servers that literally target consumers with ads or does it begin earlier when PI is matched, such as in DCRs? The legal issue is where to draw the admittedly fine line between DCR service providers' lawfully matching personal information as a data computational service pursuant to CCPA business purposes (e.g., analytics service[46] and advertising and marketing[47]) and unlawfully engaging in cross-context behavioral advertising.[48]

The prevailing market practice is for Data Contributors to designate DCR Providers as "service providers" to match PI pursuant to CCPA business purposes with the understanding that certain

[42] Cal. Civ. Code §1798.140(e)(6) (Such permissible marketing and advertising business purposes include "providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.").

[43] Cal. Civ. Code §1798.185(a)(10) and Cal. Code. Regs. tit. 11 § 7050(b). ("A service provider or contractor cannot contract with a business to provide cross-context behavioral advertising. Pursuant to Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-context behavioral advertising is a third party and not a service provider or contractor with respect to cross-context behavioral advertising services.")

[44] Reading Sections 7050(a) and (b) of the CCPA together, both sections speak to the scope of permitted combinations. Any other interpretation would lead to the odd result of permitting combinations (excluding opted-out consumers). For non-cross-context behavioral advertising marketing and advertising services (Cal. Civ. Code §1798.140(e)(6)), but not for other business purposes.

[45] Cal. Civ. Code §1798.140(e)(6) and Cal. Code. Regs. tit. 11 § 7050(b).

[46] Cal. Civ. Code § 1798.140(e)(5).

[47] Cal. Civ. Code § 1798.140(e)(6).

[48] Cal. Civ. Code § 1798.140(k).

downstream uses can include campaign planning and audience segmentation. In other words, market participants frequently assert that matching in DCRs for campaign planning purposes is distinct from actually targeting consumers, which is done by other ad tech participants.[49]

On the other hand, the CCPA's anti-avoidance provision requires the CPPA to disregard intermediate steps or transactions if they are merely components of a larger scheme designed to circumvent the law—particularly to evade the definition of a "sale." [50] The scope of the anti-avoidance provision has not been clarified by the CPPA or the California Attorney General's Office in the context of matching in DCRs or by other service provider market participants when the ultimate downstream use case is cross-context behavioral advertising.

Although we believe the service provider construct is highly beneficial for consumer privacy for the reasons set forth in Section VIII and there is a colorable basis for the legal positions of companies engaging DCRs as service providers to undertake matching for the ultimate use of campaign planning and audience segmentation, its regulatory acceptance in California is unclear at this time. Companies should be aware of that risk while awaiting regulatory clarity.

VIII. POLICY CONSIDERATIONS FOR LEGAL CONSTRUCTION

The aforementioned service provider limitations should be narrowly construed to provide consumers with the most expansive level of privacy protection. While a broad interpretation of the privacy laws is ordinarily most protective of consumers, that is not the case in this instance because service providers are bound by legally required restrictions that do not apply to "third parties," including prohibitions against further selling PI, only processing PI for narrowly prescribed business purposes defined under the CCPA, and not retaining, using, or disclosing PI for any other purpose.[51]

Notably, under the CCPA, both "service providers" and "third parties" must be bound by a set of terms imposed by the CCPA.[52] The key difference, however, is that the "service providers" must be bound by prescribed "business purposes,"[53] while "third parties" are bound by "limited and specified purpose(s) for which the personal information is made available to the third party."[54]

[49] Market participants also argue that DCRs function similarly to other data analytics IT tools. DCRs do not determine the purposes or means of data processing, but operate strictly under Data Contributors' instructions. Classifying DCRs as third parties or data brokers would imply the same for any data analytics tool that combines multiple data sources, which market participants assert is not the case.

[50] Cal. Civ. Code § 1798.190. Market participants assert that the legal construct described above is not intended to evade the definition of "sale" or hinder consumers' right to opt out. Rather, it construes a "sale" between the underlying parties that actually engage in the transaction, while the DCR technology facilitates the process.

[51] Cal. Civ. Code § 1798.100(d)(3) and Cal. Code. Regs. tit. 11 § 7051(a).

[52] Cal. Civ. Code § 1798.100(d)(3), Cal. Code. Regs. tit. 11 § 7051(a), and Cal. Code. Regs. tit. 11§ 7053(a).

[53] Cal. Civ. Code § 1798.140(e).

[54] Cal. Code. Regs. tit. 11§ 7053(a)(1).

If under the CCPA, parties cannot establish a service provider relationship with the DCRs due to the restriction on combining PI or the prohibition against engaging a service provider for cross-context behavioral advertising purposes, it will lead to less privacy-centric and, in some cases, bizarre outcomes. For example, for California consumers only (and not in any other states under their "processor" paradigms), Data Contributors would be treated as "selling" PI to the DCR, which subsequently "sells" data to the other Data Contributor or other endpoints (e.g., DSPs/SSPs), depending on the data flows described above. As "third parties," DCRs would be permitted to use the matched PI for their own commercial purposes if contractually permitted. This is not an intended or desired outcome. Although Data Contributors may still impose stringent contractual use limitations on DCRs, it largely depends on the market power of both parties, which is a suboptimal outcome for privacy protection purposes.

Further, by virtue of a DCR's "selling" data to the other Data Contributors or other endpoints, DCRs would become data brokers, as defined under California law, which is a bizarre, counterintuitive outcome considering the role that DCRs play.[55] That is because DCRs typically process PI only temporarily and do not retain it after processing. Even under Model B, DCR providers have limited technical and administrative access to their clients' PI, as it resides within the clients' own environments. Yet, because DCRs would be considered data brokers under such legal construct, they would be legally required to comply with deletion requests under the Delete Act,[56] when in fact there is no underlying PI to delete due to the ephemeral nature of the processing.

IX. CONCLUSION

Although DCRs have many benefits, these benefits must be managed in a manner that complies with privacy laws. DCRs process personal information, do not de-identify personal information in all use cases, and do not always prevent personal information from being disclosed to other parties. State privacy laws continue to apply to processing personal information through DCRs.

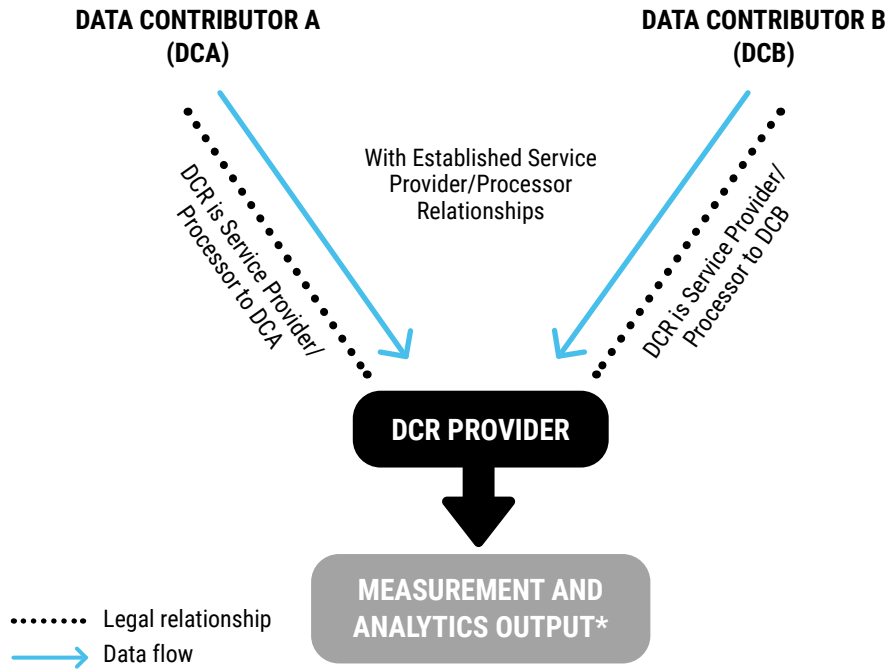
Additionally, not only is the service provider/processor relationship between Data Contributors and DCRs supported by the statutory and regulatory language under state privacy laws, it is the most privacy protective means of matching consumer data. That said, market participants must be mindful, in particular under the CCPA, that certain service provider use cases have a clearer trajectory, such as measurement, analytics, and insights, while the regulatory landscape for DCRs to engage in campaign planning and audience augmentation as service providers is presently unclear.

[54] Cal. Code. Regs. tit. 11§ 7053(a)(1).

[55] Cal. Civ. Code § 1798.99.80(c) (defining "data broker" as a company that "knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship").

[56] Cal. Civ. Code § 98.99.86.

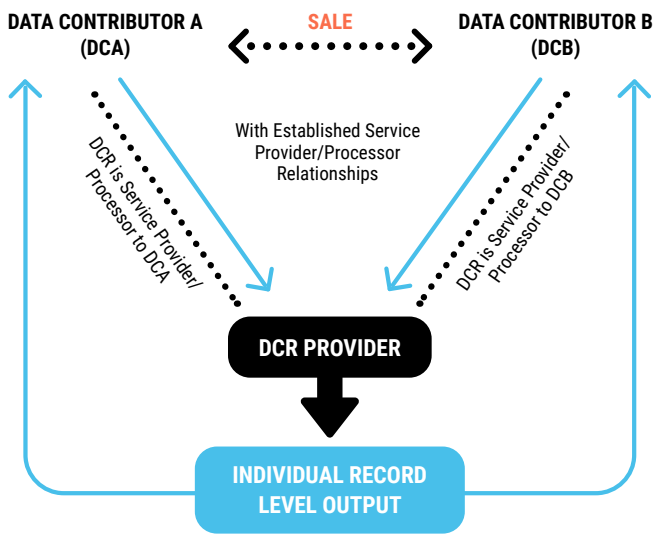
APPENDIX: PREVAILING LEGAL CONSTRUCTS UNDER U.S. STATE PRIVACY LAWS FOR PARTIES ENGAGING WITH DCRs



Measurement, Analytics, and Insights Use Cases

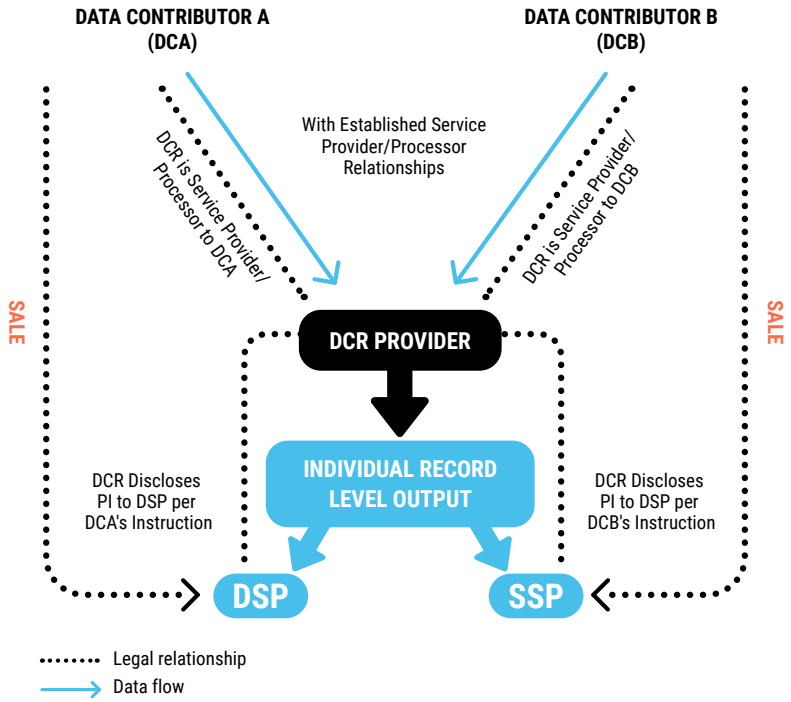
1. Data Contributors designate the DCR Provider as their service provider/processor. DCR Provider generates output for measurement, analytics, and insights.
2. If the measurement and analytics output is aggregated and/or deidentified:
    a. No sale of personal information occurs between Data Contributors and DCR Provider if there is an established service provider/processor relationship.
    b. No sale of personal information occurs between DCA and DCB.
3. If the measurement and analytics output is at the individual record level and is not anonymized:
    a. No sale of personal information occurs between Data Contributors and DCR Provider if there is an established service provider/processor relationship.
    b. A sale occurs between DCA and DCB, unless parties establish a service provider/processor relationship. We understand that the predominant market position is to treat it as a "sale" and remove the opted-out data from being matched rather than perfecting a service provider/processor relationship.

* Measurement and analytics output are often, but may not always be aggregated. Certain measurement output takes an aggregated form (e.g., 20% overlap, 2 million unique records in a combined data set). Certain market participants may also generate individual record-level output. Parties may try anonymizing record-level individual production, such as using synthesized IDs or applying K-anonymity.



Profile Augmentation and Campaign Planning Use Cases

1. Data Contributors designate the DCR Provider as their service provider/processor.
2. Individuals who have opted out of "sale" or "sharing" are suppressed from the data sharing.
3. Data Contributors "sell" PI to each other when one receives output data containing PI (e.g., pseudonymous information) from the other Data Contributor.



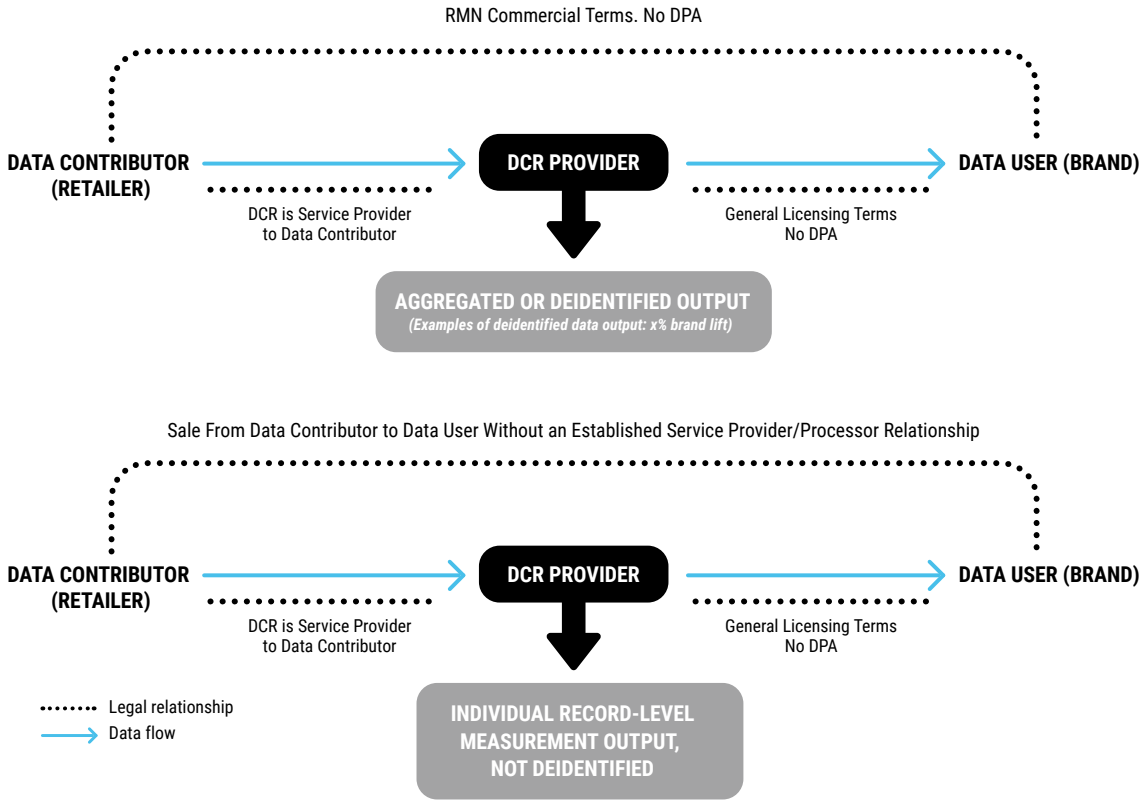
Campaign Planning Use Case

1. Data Contributors designate the DCR Provider as their service provider/processor.
2. Individuals who have opted out of "sale" or "sharing" are suppressed from the data sharing.
3. Data Contributors sell PI to their respective DSPs/SSPs.

The analysis above also applies to the two DCR variations under Section IV(A), whereby the DCRs serve as service providers/processors to Data Contributors with an established service provider/ processor relationship.

In the retail media network use case where a DCR is used for measurement and analytics, the same legal construct applies:

RETAIL MEDIA NETWORK USE CASE



1. Retailer contributes its first- and third-party PI to DCR.
2. Through the DCR user interface, Brand (i.e., a named product supplier conducting its digital advertising campaign through the retail media network) provides instructions on campaign design (e.g., consumer segments, cadence, onsite or offsite, etc.) without contributing PI.
3. Upon campaign execution, DCR Provider generates a campaign report to Brand.
4. If the measurement and analytics output is aggregated or deidentified:
    a. No sale of personal information occurs between Retailer and DCR Provider if there is an established service provider/processor relationship.
    b. No sale of personal information occurs between Retailer and Brand.
5. If the measurement and analytics output is at the individual record level and is not deidentified:
    a. No sale of personal information occurs between Retailer and DCR Provider if there is an established service provider/processor relationship.
    b. A sale occurs from Retailer to Brand, unless there is an established service provider/processor relationship. We understand that the predominant market position is to treat it as a "sale" and remove the opted-out data from being matched rather than perfecting a service provider/processor relationship.

Interactive Advertising Bureau, Inc. ("IAB") provides this whitepaper as a resource for general information. Please be aware that this whitepaper does not constitute legal advice, and if you have any legal questions, please consult your attorney. While IAB has made efforts to assure the accuracy of the material in this whitepaper, it should not be treated as a basis for formulating business and legal decisions without individualized legal advice.

IAB makes no representations or warranties, express or implied, as to the completeness, correctness, or utility of the information contained in this whitepaper and assumes no liability of any kind whatsoever resulting from the use or reliance upon its contents.