Articles + Publications | February 10, 2025

How Cos. Can Use Data Clean Rooms to Address Privacy

WRITTEN BY

Ronald Raether, Jr. | Joshua D. Davey | Christopher J. Capurso | Esther Kye

This article was originally published on February 10, 2025 on Law360 and is republished here with permission.

Businesses are constantly seeking innovative ways to improve their customers' experiences.

In past centuries, it was the owner of the general store who knew a customer's purchase preferences and needs. The owner would order goods they knew their customers would need and would market those items. In today's market, delivering a personalized experience requires analyzing data, which in turn requires complying with, among other things, privacy laws and customer expectations regarding their privacy.

One innovation intended to address these compliance concerns is the "data clean room," or DCR, a cloud data processing technology that allows companies to exchange and analyze data without sharing their entire customer information database.

For example, advertisers might analyze consumer purchase pattern data from different businesses in DCRs to offer targeted discounts to their customers only for services they would be interested in; credit card companies could leverage DCRs to share anonymized transaction history to identify fraud across different platforms; and retail shops can combine purchase histories with demographic information to curate products tailored for each consumer.

When used properly, the DCR can be immensely beneficial. Thus, DCR users need to put proper security measures in place to balance these goals with consumer privacy.

On Nov. 13, the Federal Trade Commission released a blog post[1] about DCRs to warn businesses not to think of DCRs as a one-stop solution to solve all compliance issues, because, despite their squeaky-clean name, the FTC believes DCRs can have complicated implications for user privacy.

How Data Clean Rooms Work

According to IAB Technology Laboratory's DCR Guidance and Recommended Practices, a DCR is a "secure collaboration environment which allows two or more participants to leverage data assets for specific, mutually agreed-upon uses, while guaranteeing enforcement of strict data access limitations."[2] This means that companies can share and match their deidentified transaction data to provide their consumers tailored experiences.

Prior to the use of DCRs, companies used anonymization techniques to protect consumer privacy while analyzing datasets subject to laws with use limitations — for example, replacing names with pseudonyms.

However, with advanced artificial intelligence algorithms able to sweep the internet and better analyze data patterns, there are growing concerns that anonymized data can be reverse-engineered if the unique characteristics of the data are combined with external information. This could lead to individuals being reidentified, despite a company's best efforts to protect consumers' personally identifiable information.

DCRs mitigate such concerns by providing a tool that further deidentifies data while still producing analysis that allows companies to provide consumers personalized experiences.

Specifically, DCRs use differential privacy. Differential privacy adds another layer of protection to anonymized data, making it harder to reverse-engineer personal information. Differential privacy is achieved by using mathematical frameworks to intentionally inject "noise," or irrelevant data, into aggregated datasets. The added data preserves the pattern of data for users to analyze but prevents them from reversing the pattern to track the information of any particular individual.

DCRs can be analogized to seeing a gathering of people through frosted windows. You might be able to get a general idea of whether music is playing or how many people are present, but you won't be able to discern the exact song or attendees' faces.

Additional DCR security measures may be added through a combination of data isolation, privacy-enhancing technologies, privacy control mechanisms and access controls, all of which ensure strict data protections while enabling analysis. Data isolation allows companies to separate different datasets and limit access to only certain subsets of data.

Companies can then manage both access and the potential effects of a data breach, even if a DCR is compromised. Privacy-enhancing technologies such as encryption and injection of irrelevant data can minimize the risk of personal data being tracked back to the individual. Access control mechanisms such as limiting the number or type of queries or access time can give DCR users additional control over each party's data use.

Regulatory Concerns and Lessons From Enforcement Examples

As reflected in the FTC's post, regulators are placing increasing scrutiny on technologies like DCRs to suggest they are not a "magic bullet" that automatically guarantees privacy compliance.

While DCRs allow companies to utilize their own datasets for analysis, the FTC notes, their efficacy depends on the safeguards implemented by the companies operating them. Effective efforts to regulate new technologies must include industry input and objectively address any potential issues.

There is a risk that excessive or burdensome regulation could tie up new technology based on only a few instances of companies pushing the limits, thereby stifling innovation and ultimately harming consumers. DCRs, when used with the proper security and administrative controls, help further the cause of protecting consumers' privacy through additional deidentification.

Federal and state regulators should focus on making DCR use safer, not making their use unfeasible. It is expected that the Republican-led FTC will agree. Andrew Ferguson, chairman of the FTC, has expressed that he will not be on the "pro-regulation side of the AI debate," and raised concerns that if "regulators and lawmakers attempt to ban or seriously curtail targeted advertising, they will be undoing the balance of the online economy."[3]

With a change in leadership, the FTC will likely be less aggressive toward regulating technology such as the DCR.

Even absent direct rulemaking, the risks of failing to ensure privacy safeguards when using DCRs or other technology remain. The FTC enforces prohibitions against unfair or deceptive acts or practices under Section 5 of the FTC Act, and the failure to implement good technical, administrative and physical controls may lead to FTC enforcement.

For instance, in January 2024, the FTC issued an order against X-Mode addressing the allegedly improper collection and use of precise geolocation data without consumers' affirmative express consent.[4] The order prohibits X-Mode from using, selling or disclosing sensitive location data.[5] Additionally, the FTC order mandates the deletion of previously collected precise geolocation data and the products and services developed based on it unless the consumers give consent or the sensitive location data is deidentified.

The FTC found X-Mode's original notices to be insufficient because, while it did identify collection, sharing and use of location information for ad personalization and analytics, it did not call out sensitive location collection and use for certain sensitive uses.

Similarly, that same month, the FTC ordered InMarket Media, a data aggregator and digital marketing company, to delete all the location data it previously collected, and any products developed using this data, due to allegedly failing to fully inform consumers about how their data could be used for targeted advertisements.[6] The data and products derived from this data were ordered to be deleted unless the company obtains consumer consent or ensures the deidentification of the data.

The FTC has also brought cases against BetterHelp in March 2023[7] and GoodRx in February 2023[8] for allegedly disclosing consumers' sensitive health data without proper authorization. These examples underscore the importance of maintaining transparency and obtaining consumer consent for companies to avoid legal exposure.

While it is uncertain whether the FTC's enforcement priorities may change, state attorneys general have similar unfair or deceptive acts or practices authority and thus could similarly police consumer data privacy.

For example, the California Privacy Protection Agency implements and enforces the California Privacy Rights Act of 2020. The California attorney general's office has also secured settlements against businesses in the retail, food service and mobile game industries for alleged violations of the California Consumer Privacy Act.

Additionally, the Texas Attorney General Ken Paxton launched a dedicated team in his Consumer Protection Division to focus on enforcing Texas's privacy laws, including the Deceptive Trade Practices Act. The current patchwork of state privacy laws provide different regulatory frameworks for consumer data privacy.

Companies should ensure they have robust privacy policies, procedures, and personnel or business practice trainings in place to strengthen administrative control over consumer information in compliance with states' comprehensive privacy laws.

Best Practices for Mitigating Risks

All strong compliance programs adopt privacy by design and defense in depth. This starts with reasonable technology controls.

DCRs already establish access and rights controls. DCR users or DCRs also deidentify consumer data. However, diligence by DCR users is required to ensure that such controls are sufficient. For example, there has been much debate about what steps are required to truly deidentify information.

Regulators at the state and federal level have tried to provide guidance on this question. For instance, the Health Insurance Portability and Accountability Act provides concrete guidelines on how protected health information can be considered deidentified. The HIPAA safe harbor deidentification is satisfied when specific patient identifiers, or identifiers of related persons, are removed so that a covered entity has no actual knowledge to reidentify the patient.

Once the protected health information is deidentified, it is not considered protected health information, and the restrictions on its use or disclosure are much less stringent. These concepts should be addressed in any agreement with the DCR. In addition to diligence, companies engaging DCRs or similar devices should consider additional administrative controls.

Consumer Notice and Consent

Organizations should implement clear notice and consent process about using a DCR to analyze consumer information. As with the application of any new technology, businesses should review and update their privacy policies to provide consumers notice and obtain consent to make sure they cover the full range of potential uses and sharing, such as the use of DCRs.

For example, the business should comply with the rules they notified and obtained consent from consumers about, including the use of DCRs, to ensure that a reasonable consumer would expect such uses and/or sharing.

This requires tagging the data with consent rules to align with the consumer's expressed desires. The business can then limit where that personal information is being disclosed, shared or sold to align with the consumer's consent.

Vendor Management

A DCR provider who has access to the datasets could cause the personally identifiable information to leave the DCR. To prevent issues from arising, a business must have a solid vendor management program.

While there are no one-size-fits-all solutions, business should consider several factors as part of their vendor

management programs. A business should review the state privacy laws to check if their vendors qualify as service providers under that law.

If a vendor qualifies, the business should specify in the vendor contract the purpose of processing personal information; restrictions prohibiting the vendor from retaining or disclosing information; protocols in the event of a security incident; confirmation that the vendor will cooperate in the business's compliance with privacy laws; and the vendor's responsibility of maintaining reasonable security practices and properly segmenting data they process on behalf of the business.

It would also be helpful to include the business's right to audit the vendor's security practices, authorize or object to the vendor's subcontractor selection, and require the vendor's subcontractor to have the same obligations as the vendor.

Businesses engaging DCR provider vendors should additionally consider the vendor's work procedures and policies regarding data deidentification and ownership of the data. Companies during their due diligence in choosing a vendor should test administrative controls and security procedures the vendor has in place to make sure the DCR and the data processed in it will remain deidentified and accessible only to necessary employees.

Furthermore, businesses should consider who has the right over the processed data that comes out of DCRs. Data ownership, trade secret and copyright issues can arise when the business and vendor do not discuss in advance who has rights over the analyzed dataset. Setting up a contributory model — a set of defined guidelines that allow contributors to add to the system — could also be helpful in leveraging proper administrative controls over the data.

DCRs offer a robust solution for organizations that seek to improve their customer experience while also protecting customer privacy. When equipped with appropriate security measures, DCRs can mitigate businesses' reidentification concerns, enabling businesses to analyze data and tailor products and services to meet customer needs.

Implementing comprehensive administrative controls, security processes and vendor management systems are vital steps for businesses to leverage innovations like DCRs within the boundaries of legal compliance.

---

[1] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/11/data-clean-rooms-separating-fact-fiction?utm_source=govdelivery.

[2] https://iabtechlab.com/blog/wp-content/uploads/2023/06/Data-Clean-Room-Guidance_Version_1.054.pdf.

[3] https://www.ftc.gov/system/files/ftc_gov/pdf/guardian-ferguson-dissenting-statement-final.pdf.

[4] https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-order-x-mode-successor-outlogic-

prohibiting-it-sharing-or-selling-sensitive-location.

[5] https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-order-x-mode-successor-outlogic-prohibiting-it-sharing-or-selling-sensitive-location.

[6] https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-finalizes-order-inmarket-prohibiting-it-selling-or-sharing-precise-location-data.

[7] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter.

[8] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Privacy + Cyber