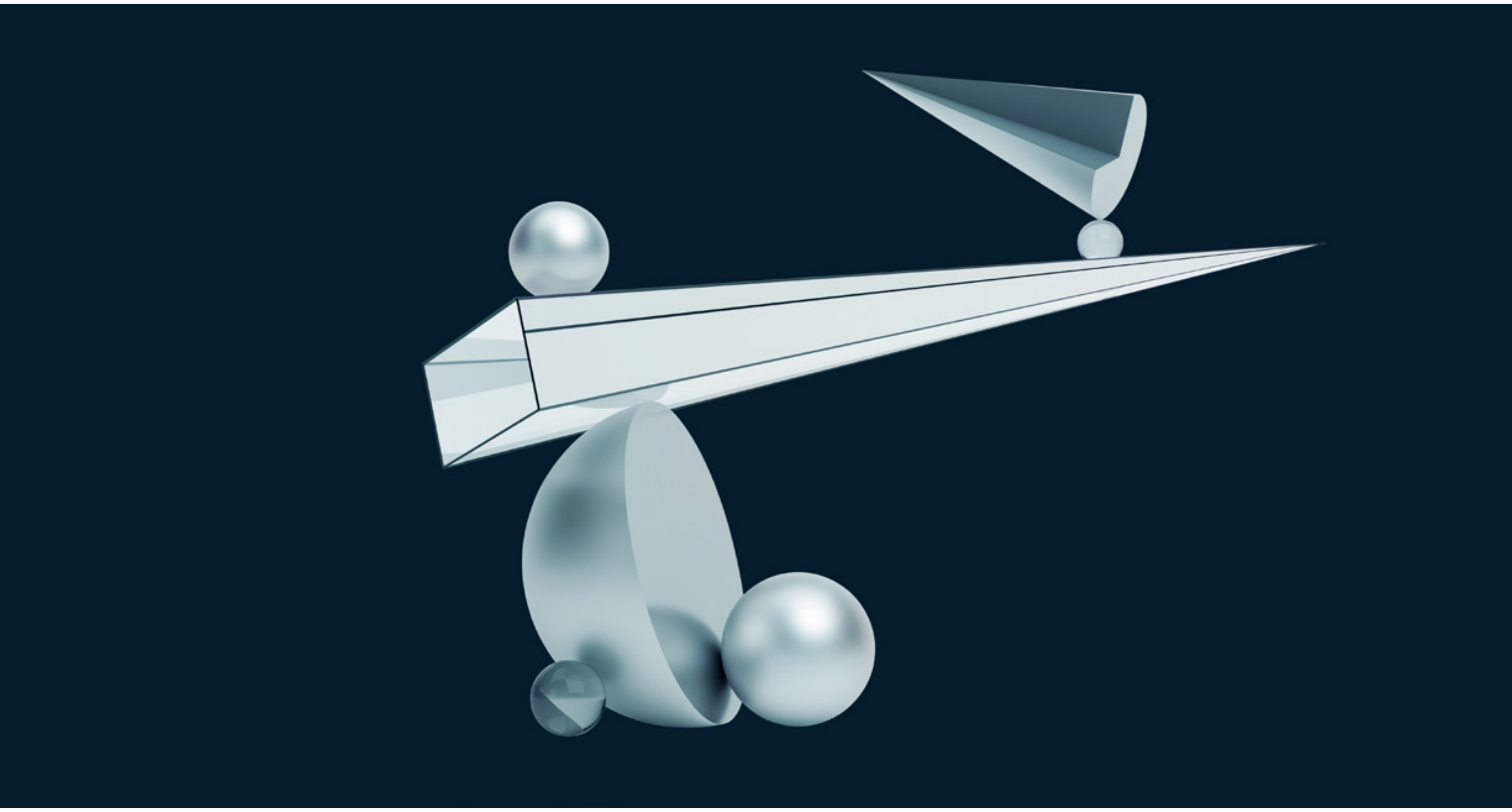
McKinsey
& Company

Marketing & Sales Practice

A customer-centric approach to marketing in a privacy-first world

Growing limits on the use of customer data cannot simply be circumvented through technical solutions. Any sustainable first-party data strategy must have the customer relationship at its core.

by Marc Brodherson, Adam Broitman, Jason Cherok, and Kelsey Robinson



© Getty Images

May 2021

The way that customer data are gathered, used, and regulated has changed tremendously over the past decade. Tracking tools such as web cookies and Apple's Identifier for Advertisers (IDFA) have opened the door for an enormous increase in the sophistication of advertisement personalization and targeting, but they have also enabled occasional privacy violations.[1]

Regulators and tech companies are taking action to reassure customers. Government regulations, including the European Union's General Data Protection Regulation (GDPR) and the California Customer Privacy Act (CCPA), have already begun to place limits on the use of customer data.[2] In addition to the existing legislation in California and Delaware, privacy proposals in Hawaii, Maryland, Massachusetts, and New York may disrupt the current status quo as it relates to data.[3]

This shift is expected to have profound implications for digital marketers, who may no longer be able to rely on cookies to boost the efficacy of customer outreach. Those marketers and companies that do not figure out a strategy to maintain—and even grow—their access to first-party data may have to spend 10 to 20 percent more on marketing and sales to generate the same returns.[4]

A new approach to data-driven marketing should therefore be considered. This is not only about technical fixes or work-arounds. Instead, a strong, trust-based relationship with customers may be the key to a sustainable, effective data strategy.

This article lays out the four key components of this new approach, which we call data relationship management (DRM): data invitation, a data security center, data dialogue, and a data value proposition. Companies that can get this new data relationship right—and that have the people, processes, and technology to implement it effectively—may be able to develop a significant, long-term source of competitive advantage.

The evolution of customer data protection

Web cookies were invented in 1994 to enhance the user experience of the internet, but they quickly began to be used for marketing purposes as well. Furthermore, in 2012, Apple introduced its IDFA, a tool for the targeting and evaluation of advertising.

These developments, however, have also enabled third-party actors to take advantage of personal data. Our research suggests that only around 33 percent of Americans believe that companies are using their personal data responsibly (Exhibit 1). As a result of growing concern around data usage, government regulations have begun to limit the use of customer data; the European Union's GDPR was the first in 2018, but others—including the CCPA, the California Privacy Rights Act (CPRA), and the Delaware Online Privacy and Protection Act—have followed.

Private companies are now following suit. In January 2020, Google announced that it planned to phase out support for third-party cookies in Chrome within two years.[5] Chrome will be the third browser to make this restriction—Apple has already done so—which means that more than 85 percent of the browser market will block third-party cookies starting next year.[6] Apple has also begun to limit the sharing of digital identifiers with intelligent tracking prevention in Safari, and the IDFA has required users to opt in to let advertisers see their data since April 2021.[7]

[1] "Online behavioral tracking and targeting concerns and solutions," Electronic Frontier Foundation, eff.org.

[2] "General Data Protection Regulation," Intersoft Consulting, May 25, 2018, gdpr-info.eu; gdpr-info.eu; "California Consumer Privacy Act (CCPA)," State of California Department of Justice, 2018, oag.ca.gov.

[3] Sarah Rippy, "US state comprehensive privacy law comparison," International Association of Privacy Professionals, April 26, 2021, iapp.org.

[4] Erik Lindecrantz, Madeleine Tjon Pian Gi, and Stefano Zerbi, "Personalizing the customer experience: Driving differentiation in retail," April 2020, McKinsey.com.

[5] *Chromium Blog*, "Building a more private web: A path towards making third party cookies obsolete," blog entry by Justin Schuh, January 14, 2020, blog.chromium.org.

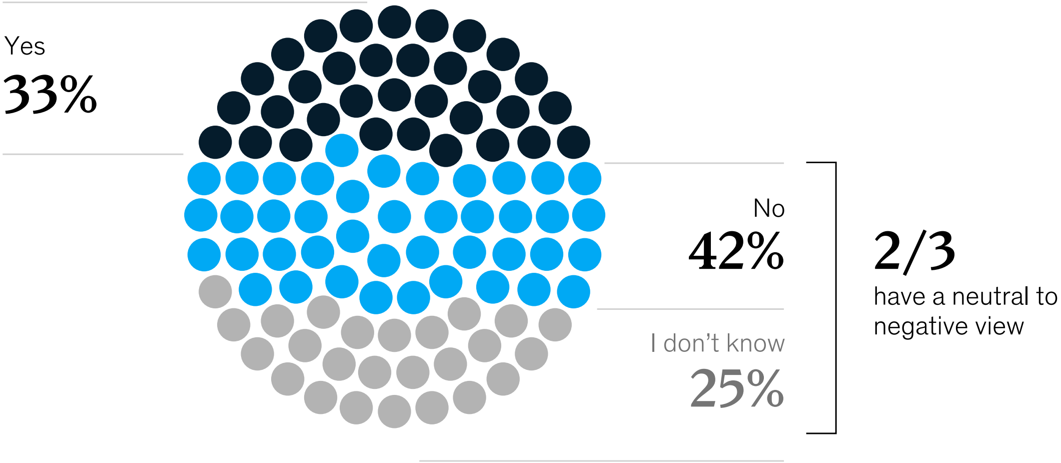
[6] "Browser market share worldwide – April 2021," StatCounter, April 2021, gs.statcounter.com.

[7] John Wilander, "Intelligent tracking prevention 2.3," WebKit, September 23, 2019, webkit.org; Allison Schiff, "IOS 14.5 is live, ATT enforcement begins—and here's how we got here," AdExchanger, April 26, 2021, adexchanger.com.

Exhibit 1

Only about one-third of customers believe that companies are currently using their data responsibly.

How respondents view companies' use of their data[1]



[1] Q: *Do you believe companies are using your personal information (eg, email, phone number, web-browsing history) responsibly?*
Source: McKinsey survey of 2,037 Americans, conducted April 8–10, 2021; respondents were aged 18–99; balancing for gender and age was based on the 2020 US census; margin of error was 2.216%

Because customer protection is key, these developments will have a significant impact on digital marketing and should therefore be welcomed. But companies that are no longer able to personalize their outreach to customers at scale may have to spend around 10 to 20 percent more on marketing and sales to achieve their current level of returns.[8]

As underscored in a recent study by McKinsey and the Interactive Advertising Bureau, advertisers therefore need to continue to build their first-party database.[9] Keeping—and growing—access to customer data will partially be about technological fixes to improve data capture. It is likely that the more important component will be an entirely new approach to customer data.

A new DRM approach

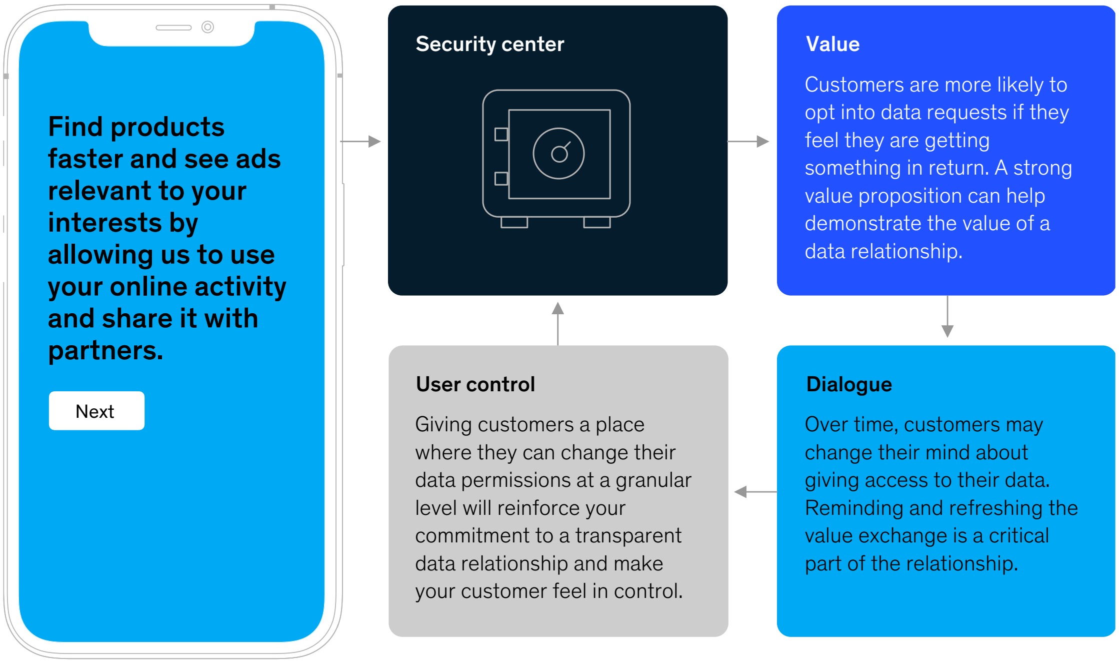
Many large firms have already created a strategy to ensure compliance with current regulations, and some may even have started to devise a comprehensive first-party data strategy. However, current best practices for data management may not be sufficient in the new data ecosystem.

To be sustainable and effective, companies may consider rooting their approach to data in a stronger relationship with customers that is built on trust and a true exchange of value. This DRM approach has four key components: data invitation, a data security center, data dialogue, and a data value proposition (Exhibit 2). Companies that get this right may be better positioned to maintain access to first-party data, which—as we will see in a later section—can

[8] "Personalizing the customer experience," April 28, 2020.
[9] A first-party database is the result of a strategy to legally access a mass of first-party data. This can form the basis of a significant source of competitive advantage. For more, see Marc Brodherson, Adam Broitman, Craig Macdonald, and Simon Royaux, "The demise of third-party cookies and identifiers," April 2021, McKinsey.com.

Exhibit 2

A comprehensive data relationship management (DRM) program can help build a robust first-party database.



Find products faster and see ads relevant to your interests by allowing us to use your online activity and share it with partners.

Security center

Value

Customers are more likely to opt into data requests if they feel they are getting something in return. A strong value proposition can help demonstrate the value of a data relationship.

Dialogue

Over time, customers may change their mind about giving access to their data. Reminding and refreshing the value exchange is a critical part of the relationship.

User control

Giving customers a place where they can change their data permissions at a granular level will reinforce your commitment to a transparent data relationship and make your customer feel in control.

then be easily aggregated and managed in a customer data platform (CDP).

Data invitation

Today's privacy communications typically take the form of jargon-filled notifications. These notifications feature a pronounced "accept," and customers may have little idea of what they are agreeing to. Until recently, the "accept" prompt on a website was the main interaction by which a customer opted into tracking. In today's data landscape, however, companies will need to take more responsibility. Apple's push for more overt language around granting data permissions, for example, may move customers away from blindly clicking "accept." These new standards are intended to make it easy for customers to comprehend, and thwart, tracking by advertisers.[10]

A fully permission-based relationship should stand up to current and future regulations, as well as satisfy questions from skeptical customers. As citizens and customer-advocacy groups become more aware of—and involved in—issues around data privacy, building transparency-based trust will likely require a comprehensive, documented permission process.

Best practices around data invitation include the following:

— *Leverage an omnichannel approach to ensure the data invitation is delivered and seen.* This means messaging customers where they are most likely to see a company's message—be it by SMS, push, email, or in store—rather than simply using one channel to communicate.

[10] "User privacy and data use," Apple, April 26, 2021, developer.apple.com.

- *Make the invitation to customers to share their data highly visible, explicit, and personalized.* Videos, for example, can demonstrate to customers that the company is not just another faceless entity seeking to exploit their data.

- *Write the invitation in layman's terms.* Use language similar to what companies might use when issuing an invitation to a loyalty program, for example.

- *Use preprompts.* Explain the potential benefits of giving permission for data sharing before asking customers to make their decision (Exhibit 3).

A data security center

The second tenet of managing data relationships is the creation and promotion of a customer-facing data security center. This is not about changing or updating security protocols; it is about using transparent communication about existing data-protection measures to build trust and gain customer consent.

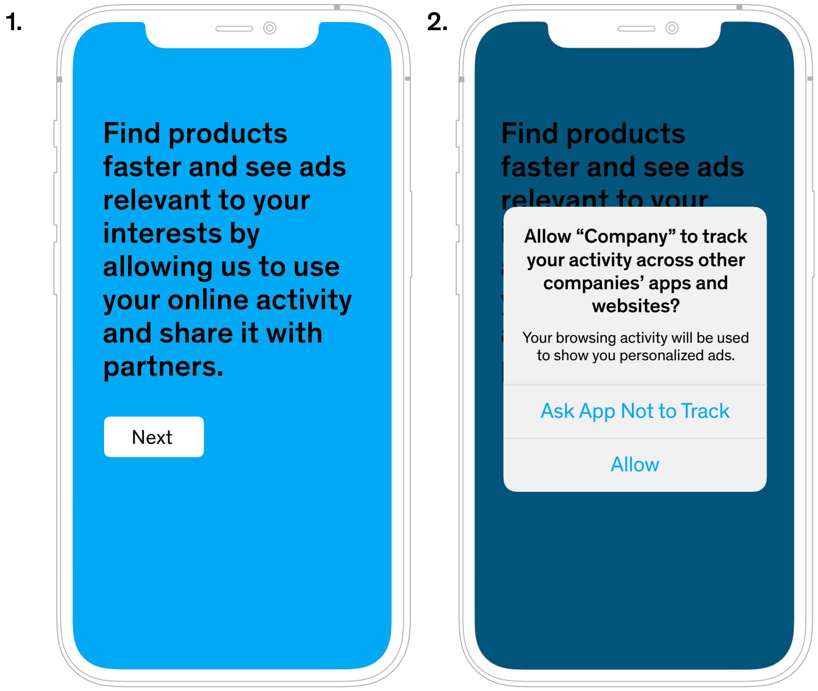
This security center should have the following three core elements:

- *A granular list of data that are being collected with a description of how they are being used.* This should include not only data that have

[11] "Delete your activity," Google Help Center, support.google.com.

Exhibit 3

Preprompts help to explain the benefits of giving permission for data sharing.



1.

Find products faster and see ads relevant to your interests by allowing us to use your online activity and share it with partners.

Next

2.

Find products faster and see ads relevant to your

Allow "Company" to track your activity across other companies' apps and websites?

Your browsing activity will be used to show you personalized ads.

Ask App Not to Track

Allow

been explicitly given by customers but also any geolocation data that may have been collected using device identifiers. Many large tech firms already provide this list to customers, along with the opportunity to delete these data.[11] While this may result in a leaner data set, it could also reinforce the notion that customers are truly in control of their data, which may make them more willing to share.

— *A preference center that enables customers to opt out of any future data collection or usage.* Many large tech firms and financial institutions have dedicated portions of their websites to preferences around data usage. A strategic data-preference center allows companies to build trust through transparency, which may make customers more willing to grant companies access to their data.

— *Rich, regularly updated content around data governance and protection.* Customers may not want to take the time to review content about data security, but innovative, forward-thinking marketers can identify ways to create engaging content that outlines the data relationship and captures customer attention. Content may be more universally appealing, for example, if it addresses the hygiene and security of personal data, in addition to corporate data-security practices. Communicating through examples and storytelling can also be effective in getting the attention of customers.

These sorts of data security centers are currently associated with large tech platforms, but other types of companies are now working to catch up. A large customer bank, for example, recently built a robust data security center, complete with a fraud-prevention checklist, a robust library of content, and prominently featured CCPA-compliance guidelines.

A global beverage manufacturer realized that future-proofing its data strategy in the face of new privacy regulations and Apple's IDFA opt-in approach would require it to collect data directly from customers. The company therefore wanted to boost its interaction with customers via online touchpoints. To manage consent and ensure regulatory compliance, it used a CDP that made it very easy for customers to opt out. Its data-strategy refresh also called for personalized campaigns and promotions—including email-marketing initiatives that would not have been possible without the company's first-party data—to build one-to-one customer relationships.

In today's data ecosystem, every company is fast becoming a tech company. Data centers are therefore vital to demonstrate a commitment to creating and maintaining comprehensive data-protection protocols.

Data dialogue

Much like customer relationship management, data relationship management requires an ongoing dialogue. In addition to increasing transparency, continued engagement acts as a reminder that the company both constantly strives to improve best practices for data security and uses customers' data to improve their overall experience of a product or service.

As continued headlines about data privacy appear in the most prominent newspapers and trade magazines, data privacy will likely remain a mainstream topic. While not all customers will be interested in actively engaging in an ongoing data dialogue, many may be comforted by transparency and reassured by a company's stated commitment to the safety of their data. Regulations such as the GDPR give customers the "right to be forgotten"; preempting customer fears and providing full information on data usage may help to ensure that they do not exercise this right.

A large financial institution recently ran an email campaign that promoted its practices on data security. The email directed users to a robust data-security and preference center on the company's website. This campaign enabled users to set their preferences, but it also built trust, which made the campaign an important brand-building exercise.

Data value proposition

Customer value is at the core of the data relationship, and a data relationship with a clearly defined and articulated value proposition will help ensure that customers stay engaged. Our research indicates that around two-thirds of customers would be happy to share their data, or would consider sharing data, if they got something of value in return (Exhibit 4). It is likely that an even larger majority could be enticed to share data with a company that communicates a clear, compelling value proposition.

However, it is not always easy to demonstrate the value exchange that results from customer data collection. The creation of real value will likely require additional strategic thinking or the development of new benefits associated with data sharing. Companies should note that it is against CCPA regulations to directly exclude customers from discounts or services because they have opted out of data collection; therefore, customer value must be rooted in the benefits that a company can derive from data.

There are many different ways to share value with customers. Offers and discounts are one option that companies could consider; 57 percent of customers expressed excitement around receiving discounts or offers in exchange for the use of their data.[12]

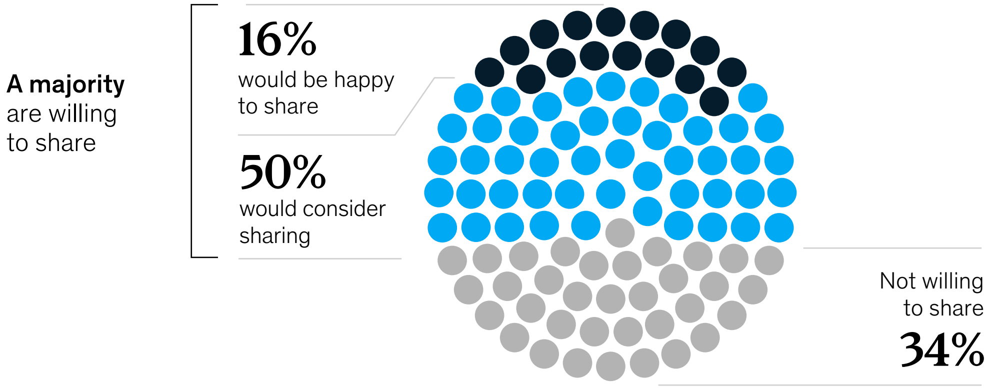
Improving the customer experience can be another way to create a compelling value proposition. Data can be used to improve customer experience by helping customers find what they are looking for more quickly, and by directing them to the new products and services that are likely to be most relevant to them. While collaborative filters might work without personally identifiable information, advanced modeling that uses these data can help bring surprise and delight to an otherwise flat customer experience.

[12] Gadi BenMark, Julien Boudet, and Phyllis Rothschild, “Why personalization matters for consumer privacy,” *MIT Sloan Management Review*, June 6, 2019, sloanreview.mit.edu.

Exhibit 4

Most customers would at least consider sharing personal information to get additional value.

Willingness of customers to share personal information[1]



[1] Q: *How willing would you be to share your personal information (eg, email, phone number, web-browsing history, app usage) to get additional value (eg, better customer service, easier shopping experience) in return?*
Source: McKinsey survey of 2,037 Americans, conducted April 8–10, 2021; respondents were aged 18–99; balancing for gender and age was based on the 2020 US census; margin of error was 2.216%

Information about customer preferences around call times and communication channels can also be used to ensure that customers receive communications at the time—and in the format—that they prefer. Shopping preferences can also be used to tailor suggested services; loyal online shoppers could be offered video-call access to a style consultant, for example.

There is evidence that customers prefer a personalized customer experience and may, therefore, be willing be provide data in return. Firms have seen a decrease of up to 60 percent in customer churn as a result of a data-driven approach to customer experience.[13] To increase the potential likelihood of customers opting in, companies should consider regularly reinforcing the customer-experience value that customers are getting in exchange for their data. One approach is to not only offer explanations for why customers are seeing recommendations but also solicit advice on whether the recommendations are good ones and—if not—what could be improved.

Delivering on the new data relationship requires the right people, processes, and technology

Changes in policy and overall approach may not be enough to fully implement the new data relationship. Instead, companies may benefit from ensuring that they have the right people, processes, and technology to shift mindsets and embed these changes throughout their operations.

Incremental changes are unlikely to be enough. The DRM strategy and its implementation should be central to the company's marketing function, which will require a fundamental shift in team structure and ways of working. The remainder of this article provides a few nonexhaustive examples of the types of changes needed.

People

The issue with many corporate data-privacy initiatives is that they are too technical or legalistic for the everyday customer. This complexity is often caused bythe team that is overseeing data-privacy programs.

To create a successful data relationship, larger firms should consider investing in a full-time data relationship manager. While candidates for such a role would need to be technologically savvy, the ideal candidate would have a multidisciplinary background—someone capable of thinking about technology, business, and user experience. This data relationship manager needs to deliver messages in a way that is not only understandable but also valuable to the end user.

Processes

An agile approach to working gives data relationship managers the ability to test a variety of tactics across functional areas of an organization. For example, a small and agile pod could be formed to run a series of parallel experiments that aim to better understand what it would take for a customer to enter into a data relationship. A new brand narrative, and creative ideas to disseminate it, will need to be developed and executed. Innovative communication strategies can be tested nearly in real time with customers through a test-and-learn approach that is similar to the strategies currently used around performance marketing or personalization tests.

Technology

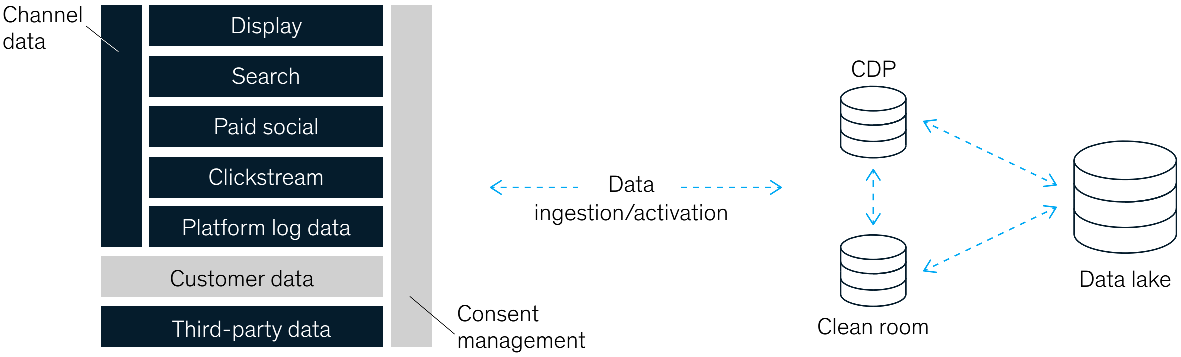
The right technologies are a key part of the delivery equation; secure infrastructure is required to deliver on the promise of the data relationship. A CDP, for example, can aggregate everything a company knows about its customers—including both customer data and channel data—in one place (Exhibit 5), thereby assisting in the management of first-party data assets. This platform also streamlines preference management and facilitates the process if customers want to invoke their CCPA or GDPR rights.

When consent has been given and the appropriate security protocols are in place, there are instances when companies may want to use customer data securely in external platforms such as advertising

[13] Rachel Diebner, David Malfara, Kevin Neher, Mike Thompson, and Maxence Vancauwenberghe, "Prediction: The future of CX," *McKinsey Quarterly,* February 2021, McKinsey.com.

Exhibit 5

The implementation of a secure customer data platform (CDP) can streamline the management of first-party data assets and customer preferences.



exchanges. In these cases, appropriate portions of the company's total data lake should be transferred to a data clean room to ensure that no identifiable data are shared with partners.[14]

In addition, companies could consider a technology-enabled data map of all customer data points, along with information about how the data were collected and what consent was given when the data were collected. A consent management platform can help to ensure that the necessary permissions are captured, stored, and managed at each step of the customer journey. Without a platform of this sort, companies can be at risk of both losing (or misusing) data and being the subject of legal proceedings.

Our experience has shown that many companies are responding to the quickly evolving world of regulations around customer data by prioritizing the technical side of data management. This may be a mistake. While it is vital to find, and invest in, the right technical measures, a sustainable data strategy also needs to have a strong human focus. Companies can seek to generate trust by building a transparent, permission-based relationship with customers that has a strong value proposition. Companies that invest in these elements of data relationship management have an opportunity to take a leadership position around data protection that could pay dividends in the years to come.

Marc Brodherson is a senior partner in McKinsey's New York office, where **Adam Broitman** is an associate partner; **Jason Cherok** is a partner in the Pittsburgh office; and **Kelsey Robinson** is a partner in the San Francisco office.

The authors wish to thank Amir Azer, Shital Chheda, Craig Macdonald, Simon Royaux, and Stephan Zimmermann for their contributions to this article.

[14] A data clean room contains aggregated data rather than customer-level data. These aggregated data will never leave the clean room. Instead, advertising exchanges could import their own first-party data to compare with data within the clean room.