McKinsey & Company

Risk Practice

The consumer-data opportunity and the privacy imperative

As consumers become more careful about sharing data, and regulators step up privacy requirements, leading companies are learning that data protection and privacy can create a business advantage.

by Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller

April 2020

As consumers increasingly adopt digital technology, the data they generate create both an opportunity for enterprises to improve their consumer engagement and a responsibility to keep consumer data safe. These data, including location-tracking and other kinds of personally identifiable information, are immensely valuable to companies: many organizations, for example, use data to better understand the consumer's pain points and unmet needs. These insights help to develop new products and services, as well as to personalize advertising and marketing (the total global value of digital advertising is now estimated at $300 billion).

Consumer data are clearly transforming business, and companies are responsible for managing the data they collect. To find out what consumers think about the privacy and collection of data, McKinsey conducted a survey of 1,000 North American consumers. To determine their views on data collection, hacks and breaches, regulations, communications, and particular industries, we asked them pointed questions about their trust in the businesses they patronize.

The responses reveal that consumers are becoming increasingly intentional about what types of data they share—and with whom. They are far more likely to share personal data that are a necessary part of their interactions with organizations. By industry, consumers are most comfortable sharing data with providers in healthcare and financial services, though no industry reached a trust rating of 50 percent for data protection.

That lack of trust is understandable given the recent history of high-profile consumer-data breaches. Respondents were aware of such breaches, which informed their survey answers about trust. The scale of consumer data exposed in the most catastrophic breaches is staggering. In two breaches at one large corporation, more than 3.5 billion records were made public. Breaches at several others exposed hundreds of millions of records. The stakes are high for companies handling consumer data: even consumers who were not directly affected by these breaches paid attention to the way companies responded to them.

Proliferating breaches and the demand of consumers for privacy and control of their own data have led governments to adopt new regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in that US state. Many others are following suit.

The breaches have also promoted the increased use of tools that give people more control over their data. One in ten internet users around the world (and three in ten US users) deploy ad-blocking software that can prevent companies from tracking online activity. The great majority of respondents—87 percent—said they would not do business with a company if they had concerns about its security practices. Seventy-one percent said they would stop doing business with a company if it gave away sensitive data without permission.

Because the stakes are so high—and awareness of these issues is growing—the way companies handle consumer data and privacy can become a point of differentiation and even a source of competitive business advantage. The main findings of our research are presented below. We then offer prescriptive steps for data mapping, operations, and infrastructure, as well as customer-facing best practices. These can help companies position themselves to win that competitive advantage.

A matter of trust—or a lack thereof

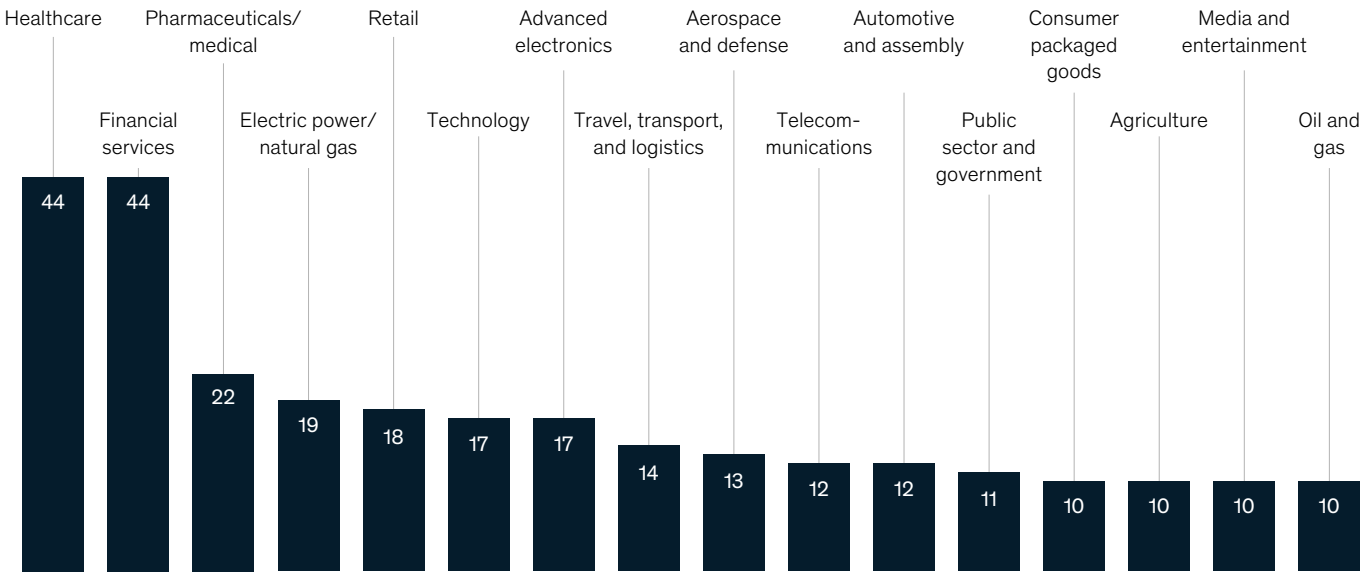
Consumer responses to our survey led to a number of important insights about data management and privacy. First, consumer-trust levels are low overall but vary by industry. Two sectors—healthcare and financial services—achieved the highest score for trust: 44 percent. Notably, customer interactions in these sectors involve the use of personal and highly sensitive data. Trust levels are far lower for other industries. Only about 10 percent of consumer respondents said that they trust consumer-packaged-goods or media and entertainment companies, for example (Exhibit 1).

About two-thirds of internet users in the United States say it is "very important" that the content

Exhibit 1

Consumers view healthcare and financial-services businesses as the most trustworthy.

Respondents choosing a particular industry as most trusted in protecting of privacy and data, % (n = 1,000)



Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

of their email should remain accessible only to those whom they authorize and that the names and identities of their email correspondents remain private (Exhibit 2).

About half of the consumer respondents said they are more likely to trust a company that asks only for information relevant to its products or that limits the amount of personal information requested. These markers apparently signal to consumers that a company is taking a thoughtful approach to data management.

Half of our consumer respondents are also more likely to trust companies that react quickly to hacks and breaches or actively disclose such incidents to the public. These practices have become increasingly important both for companies and consumers as the impact of breaches grows and more regulations govern the timeline for data-breach disclosures.

Other issues are of lesser importance in gaining the consumer's trust, according to the survey: the level of regulation in a particular industry, whether a company has its headquarters in a country with a trustworthy government, or whether a company proactively shares cyber practices on websites or in advertisements (Exhibit 3).

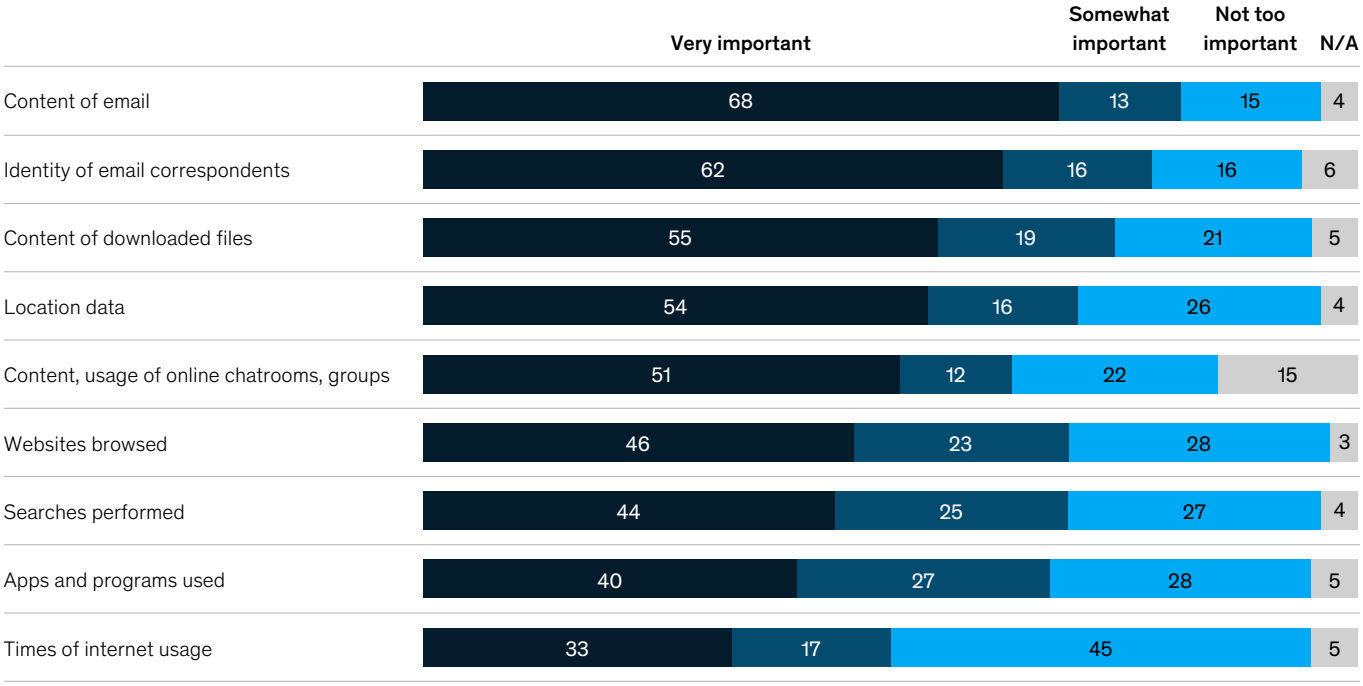
Consumer empowerment and actions

Given the low overall levels of trust, it is not surprising that consumers often want to restrict the types of data that they share with businesses. Consumers have greater control over their personal information as a result of the many privacy tools now available, including web browsers with built-in cookie blockers, ad-blocking software (used on more than 600 million devices around the world), and incognito browsers (used by more than 40 percent of internet users globally). However, if a product or service offering—for example, healthcare or money management—is

Exhibit 2

Consumer privacy and protection concerns vary by type of digital data.

Relative importance by data type, % of respondents (n = 792)



Source: Internet & American Life Project, Pew Research Center

critically important to consumers, many are willing to set aside their privacy concerns.

Consumers are not willing to share data for transactions they view as less important. They may even "vote with their feet" and walk away from doing business with companies whose data-privacy practices they don't trust, don't agree with, or don't understand. In addition, while overall knowledge of consumer privacy is on the rise, many consumers still don't know how to protect themselves: for example, only 14 percent of internet users encrypt their online communications, and only a third change their passwords regularly (Exhibit 4).

Evolving regulations

Privacy regulations are evolving, with a marked shift toward protecting consumers: the GDPR, for example, implemented in Europe in May 2018, gives consumers more choices and protections about how their data are used. The GDPR gives consumers easier access to data that companies hold about them and makes it easier for them to ask companies to delete their data.

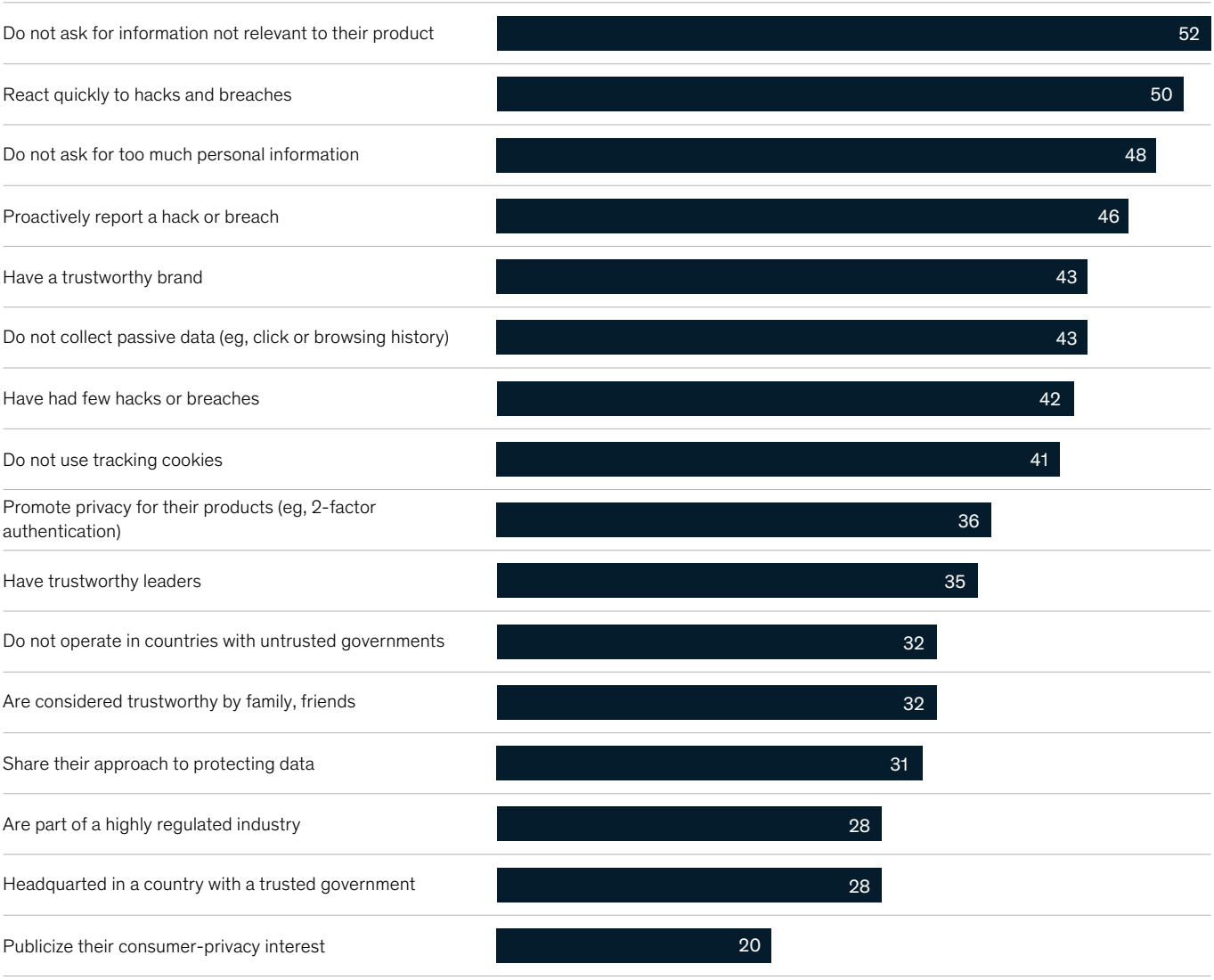
For companies, the GDPR requires meaningful changes in the way they collect, store, share, and delete data. Failure to comply could result in steep fines, potentially costing a company up to 4 percent of its global revenue. One company incurred a fine of $180 million for a data breach that included log-in and payment information for nearly 400,000 people.[1] Another was fined $57 million for failure to comply with GDPR. A side effect of this regulation is an increased awareness among consumers of their data-privacy rights and protections. About six in ten consumers in Europe now realize that rules regulate the use of their data

[1] The fine was imposed by the Information Commissions Office, the British data regulator, and is currently under regulatory process review.

Exhibit 3

Consumers trust companies that limit the use of personal data and respond quickly to hacks and breaches.

Respondent trust by practices, % (n = 1,000)

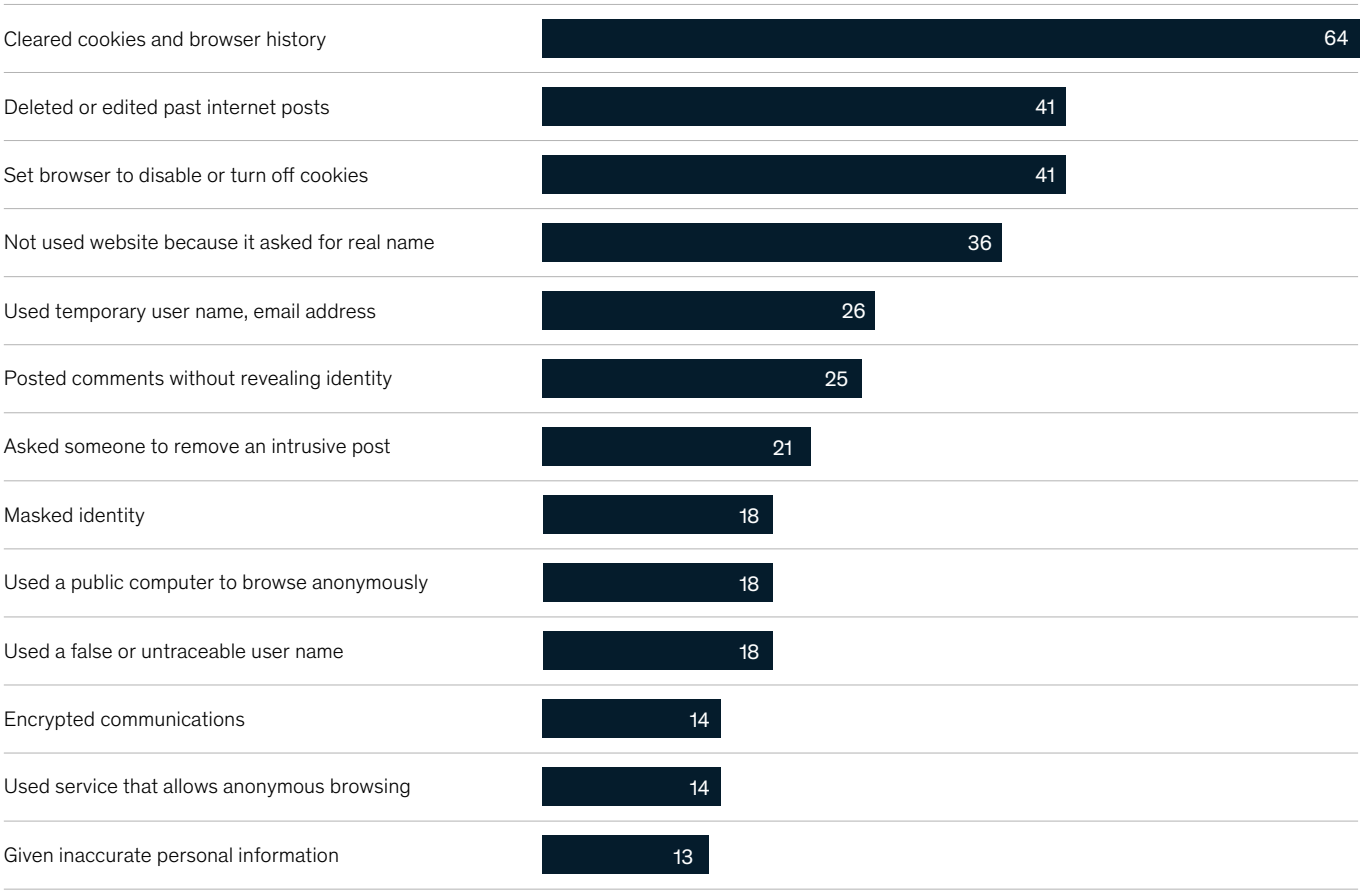


Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

Exhibit 4

Consumer concerns over data collection and privacy are mounting, but few take adequate protective precautions.

Respondents taking action, % (n = 792)



Source: Internet & American Life Project, Pew Research Center

within their own countries, an increase from only four in ten in 2015.

The GDPR has been considered a bellwether for data-privacy regulation. Even in Europe, policy makers are seeking to enact additional consumer-privacy measures, including the ePrivacy regulation (an extension of GDPR), which focuses on privacy protection for data transmitted electronically. Its status as a regulation (rather than a directive) means that it could be enforced uniformly across EU member states. The ePrivacy regulation is likely to be enacted in 2020.

Beyond Europe

Governments outside Europe have also begun to enact data-privacy regulations. In Brazil, for example, the Lei Geral de Proteção de Dados, or LGPD (General Data Protection Law) will go into effect in August 2020. Brazil's previous data-protection regulations were sector based. The LGPD is an overarching, nationwide law centralizing and codifying rules governing the collection, use, processing, and storage of personal data. While the fines are less steep than the GDPR's, they are still formidable: failing to

comply with the LGPD could cost companies up to 2 percent of their Brazilian revenues.

In the United States, the California Consumer Privacy Act (CCPA) went into effect in the state in January 2020. It gives residents the right to know which data are collected about them and to prevent the sale of their data. CCPA is a broad measure, applying to for-profit organizations that do business in California and meet one of the following criteria: earning more than half of their annual revenues from selling consumers' personal information; earning gross revenues of more than $50 million; or holding personal information on more than 100,000 consumers, households, or devices.

The CCPA is the strictest consumer-privacy regulation in the United States, which as yet has no national data-privacy law. The largest fine for mishandling data was, however, issued by the US Federal Trade Commission (FTC).

Compliance investments

Companies are investing hefty sums to ensure that they are compliant with these new regulations. In total, Fortune Global 500 companies had spent $7.8 billion by 2018 preparing for GDPR, according to an estimate by the International Association of Privacy Professionals. Companies have hired data-protection officers, a newly defined corporate position mandated by the GDPR for all companies handling large amounts of personal data. Despite these measures, few companies feel fully compliant, and many are still working on scalable solutions.

A central challenge—particularly for companies that operate internationally—is the patchwork nature of regulation. Requirements are very different from one jurisdiction or market to another. To address regulatory diversity and anticipate future regulations, many companies have begun systematizing their approach to compliance. Some have begun creating regulatory roles and responsibilities within their organizations. Many are trying to implement future-proof solutions. Rather than meeting CCPA requirements only in California, Microsoft is applying them to all US citizens, though other states do not yet have policies as restrictive as the CCPA. This practice will probably become more common, as many companies are using the most restrictive legal requirements as their own standard. For most companies in the United States, this means following CCPA's guidelines.

Another difficult aspect of privacy regulation has to do with the deletion and porting of data: regulations allow consumers to request that their data be deleted or that enterprises provide user data to individual consumers or other services. For many companies, these tasks are technically challenging. Corporate data sets are often fragmented across varied IT infrastructure, making it difficult to recover all information on individual consumers. Some data, furthermore, may be located outside the enterprise, in affiliate or third-party networks. For these reasons, companies can struggle to identify all data from all sources for transfer or deletion.

Proactive steps for companies

Several effective actions have emerged for companies that seek to address enhanced consumer-privacy and data-protection requirements. These span the life cycle of enterprise data, and include steps in operations, infrastructure, and customer-facing practices, and are enabled by data mapping.

Data mapping

Leading companies have created data maps or registers to categorize the types of data they collect from customers. The solution is best designed to accommodate increases in the volume and range of such data that will surely come. Existing data-cataloging and data-flow-mapping tools can support the process.

Companies need to know which data they actually require to serve customers. Much of the data that is collected is not used for analytics and will not be needed in the future. Companies will mitigate risk by collecting only the data they will probably need. Another necessary step is to write or revise data-

Companies should develop clear, standardized procedures to govern requests for the removal or transfer of data.

storage and -security policies. The best approaches account for the different categories of data, which can require different storage policies.

Of further importance is the growing appetite for applied analytics. Today, leading companies need robust analytics policies. Given the proliferation of advanced machine-learning tools, many organizations will seek to analyze the high volumes of data they collect, especially by experimenting with unsupervised algorithms. But unless companies have advanced model-validation approaches and thoughtfully purposed consumer data, they should proceed with extreme caution, probably by focusing specifically on supervised-learning algorithms to minimize risk.

Operations

Leading organizations have developed identity- and access-management practices for individuals according to their roles, with security-access levels determined for different data categories. About one-third of the breaches in recent years have been attributed to insider threats. This risk can be mitigated by ensuring that data sets are accessible only to those who need them and that no one has access to all available data. Even the most robust practices for identity and access management can fail—some breaches can be caused by individuals with approved access—so additional activity monitoring can be helpful.

To act quickly when breaches do occur, organizations will want to pressure-test their crisis-response processes in advance. People who will be involved in the response must be identified and a strong communications strategy developed. One of the highest predictors of consumer trust is the speed of company reporting and response when breaches occur. Indeed, most new regulations require companies to disclose breaches very quickly; the GDPR, for example, mandates the announcement of a breach within 72 hours of its discovery.

Companies should develop clear, standardized procedures to govern requests for the removal or transfer of data. These should ensure expedited compliance with regulations and cover consumer requests for the identification, removal, and transfer of data. The processes should support data discovery in all pertinent infrastructure environments within a company and across its affiliates. Most companies today use manual processes, which creates an opportunity for streamlining and automating them to save time and resources. This approach also prepares infrastructure environments for future process developments.

Working closely with third parties, affiliates, and vendors, companies can gain an understanding of how and where their data are stored. This knowledge is especially important when third parties are supporting the development of products and features and need access to consumer data. Some companies are considering establishing review boards to support decisions about sharing data with third parties.

Infrastructure

Organizations are working to create infrastructure environments that can readily accommodate the increasing volumes of data collected, as well as attending technological innovations. Best practice is to store data in a limited number of systems,

depending on data type or classification. A smaller systems footprint reduces the chance of breaches.

Customer-facing best practices

Leading companies are building "privacy by design" into consumer-facing applications, with such features as automatic timed logouts and requirements for strong passwords. Security and privacy become default options for consumers, while features strike a balance with the user experience.

It is important for organizations to communicate transparently: customers should know when and why their data are being collected. Many companies are adding consumer privacy to their value propositions and carefully crafting the messages in their privacy policies and cookie notices to align with the overall brand.

Our research revealed that our sample of consumers simply do not trust companies to handle their data and protect their privacy. Companies can therefore differentiate themselves by taking deliberate, positive measures in this domain. In our experience, consumers respond to companies that treat their personal data as carefully as they do themselves.

Venky Anant is a partner in McKinsey's Silicon Valley office, where **Lisa Donchak** is a consultant; **James Kaplan** is a partner in the New York office; **Henning Soller** is a partner in the Frankfurt office.

Designed by Global Editorial Services