



# The new imperative for corporate data responsibility

**Consumers believe data privacy  
is a human right. Corporations  
need to raise their game.**





# A data privacy wake-up call

The digital revolution has given businesses the ability to develop deep insights into the lives of their customers. Thanks to the widespread adoption of e-commerce, smartphones, and social media, companies today routinely know where their customers live, how old they are, where they shop, what they buy, and how they pay for it.

To a large degree, consumers have been okay with this. They know it can make for a better shopping experience, enabling things like quick reordering of favorite items and express checkout with saved payment information. Collecting and using personal customer information also comes with risks, and while data privacy is not a new challenge, consumers are becoming increasingly concerned with, and distrustful of, how companies safeguard their personal data against misuse and theft. Companies must take steps now to keep pace with expectations—or risk losing access to the data that increasingly drives strategy, insights, and success.

To learn more about how consumers are thinking about data privacy and what they expect from corporations, KPMG surveyed 1,000 Americans. The survey reveals that consumers overwhelmingly agree that data privacy is important and that they want corporations to take significant steps to better protect, manage, and ethically use their data.





# Contents

<b>Key findings</b>	<b>2</b>
<b>What do consumers think about data privacy?</b>	<b>3</b>
<b>Are consumers protecting their own data?</b>	<b>4</b>
<b>Who should be responsible for protecting consumer data?</b>	<b>8</b>
<b>What should corporations do now?</b>	<b>10</b>
<b>Methodology</b>	<b>14</b>
<b>Conclusion</b>	<b>15</b>
<b>Authors</b>	<b>16</b>



## Key findings



87%

**of consumers say data privacy is a human right**



68%

**don't trust companies to ethically sell personal data**



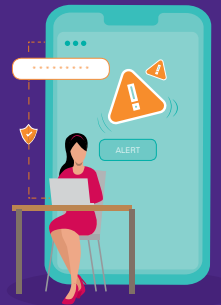
56%

**of survey respondents say companies should prioritize giving consumers more control over their own data in 2020**



84%

**are open to state legislation giving consumers more control over their data**



91%

**say corporations should take the lead in establishing corporate data responsibility**

Source: The new imperative for corporate data responsibility, KPMG LLP, 2020

# What do consumers think about data privacy?

## **The vast majority of Americans see data privacy not only as important but also as a human right—and a growing concern.**

Ninety-seven percent of survey respondents say data privacy is important to them, with 87% characterizing it as a human right. Eighty-six percent agree it is a growing concern. “The findings are unmistakable,” says Orson Lucas, principal, KPMG Cyber Security Services. “Data privacy and protection are clear priorities for consumers. Close attention to customer data handling, management, and protection practices are key, foundational elements of establishing and maintaining digital trust.”

## **Many Americans are finally paying attention to how businesses are using their data—and distrust what’s happening.**

Seventy percent of survey respondents say they are generally familiar with how companies collect their personal data, with 64% saying they generally grasp how companies use and store it, 63% understand with how they protect it, and 57% understand with how they sell it.

**Consumers biggest worries around data breaches center on the potential theft of their Social Security number (cited by 83% of respondents).** That’s followed by their credit card number (69%) and their passwords (49%). They worry much less about their medical records being stolen (16%), perhaps because they think that information is of minimal

interest to criminals. They may be partly right. A study by researchers at Johns Hopkins and Michigan State universities found that of 1,500 data breaches at healthcare entities in the U.S. from 2009 to 2019, only 22 involved the breach of sensitive medical information, while more than 1,000 involved nonmedical information that could be used in identify theft or financial fraud.<sup>1</sup>

## **When asked which types of data they trust companies to protect, respondents most often cite medical records (57%).**

Consumers are least trusting of how companies will protect their website browsing behaviors (only 44% say they trust companies with this), Social Security numbers (45%), and credit card numbers (46%).

## **While 75% of consumers say they are thinking more about data privacy in the wake of COVID-19, many are willing to forgo some personal data privacy to combat the spread of COVID-19 and return to work faster.**


Eighty-nine percent of consumers say they would allow employers to take their temperature to help keep people safe during COVID-19. Eighty-five percent would share a COVID-19 diagnosis with their employer to help get back to work faster, and 67% would share information about their lifestyle. Sixty-seven percent would share location data if it could help the country track COVID-19 cases.

## **Consumers are deeply suspicious of what companies are doing with their personal data.**


68% **Don’t trust companies to ethically sell personal data**



54% **Don’t trust companies to use personal data in an ethical way**



53% **Don’t trust companies to ethically collect personal data**



50% **Don’t trust companies to protect personal data**



Source: The new imperative for corporate data responsibility, KPMG, 2020

<sup>1</sup> “How to Prevent Medical Records from Being Hacked,” by Ge Bai and John (Xufeng) Jiang, The Wall Street Journal, June 22, 2020.

# Are consumers protecting their own data?

## Despite their concerns about data privacy, Americans still engage in online behaviors they consider risky.

About three-quarters of survey respondents say they consider it risky to use the same password for multiple accounts (78%), use public Wi-Fi (75%), or save a card to a website or online store (74%), for example. Yet more than 40 percent do each of those things.

## Many Americans see risk in technologies even after they have become widely adopted.

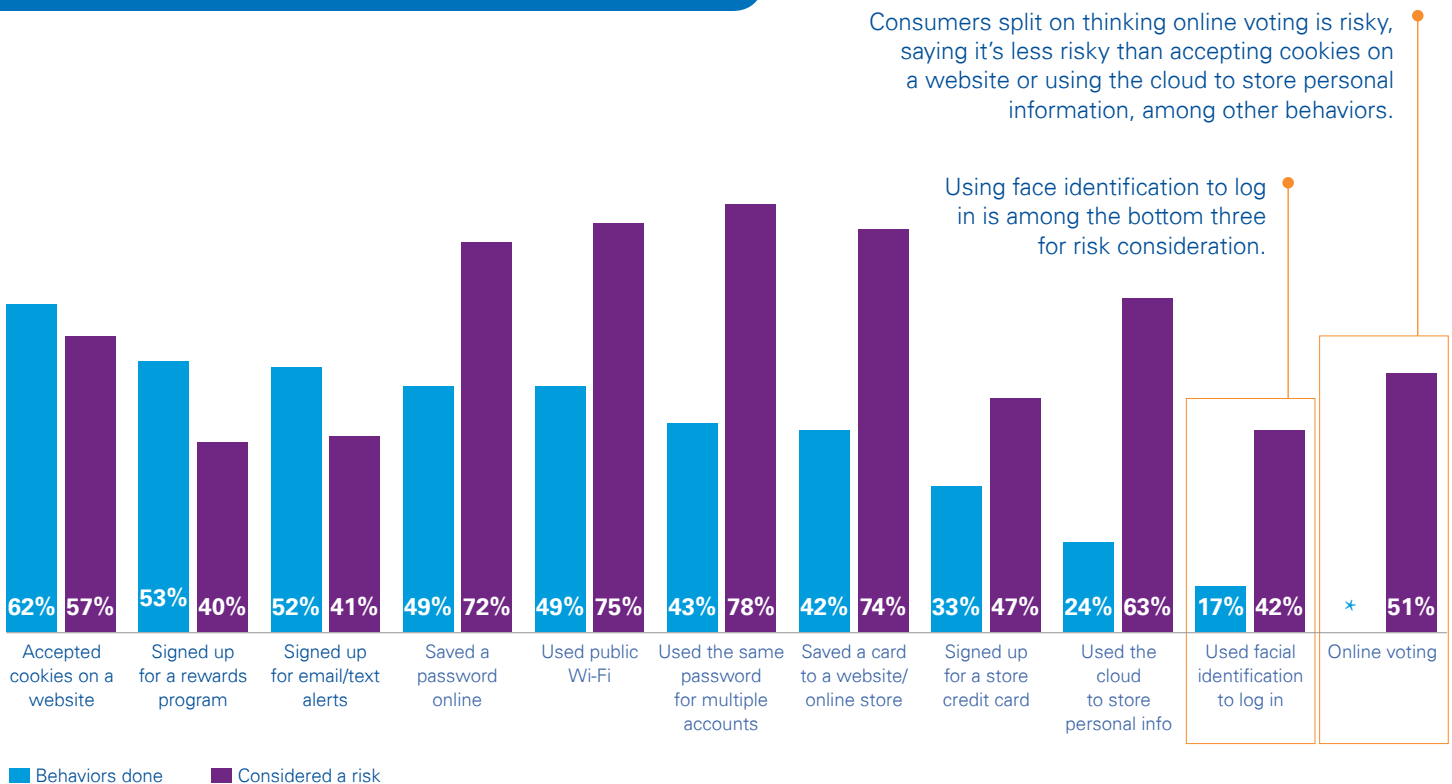
For example, while cloud computing has become commonplace across vast sectors of the business world, 63% of consumers consider that risky. Yet, consumers are less worried about online voting or facial recognition for log-in, with 51% and 42% considering those things risky, respectively. (See Figure 1.)

**Figure 1: Online behaviors Americans engage in and consider risky**

### From the list, which of the following have you done?

\*Online voting not asked as part of "Which of the following have you done?" question.

### How much do you consider the following to be a security risk?



Source: The new imperative for corporate data responsibility, KPMG, 2020

“

## Data privacy issues are not going to go away.

In fact, consumer protections around data privacy, like the ones provided by the CCPA, are very likely to be codified in other states and eventually at the federal level. Simply put, privacy laws are only going to increase in volume and rigor. That's why visibility, protection, and trust are gaining such momentum in the marketplace and also why leading-edge companies are not looking at data privacy as just another compliance or check-the-box exercise. They see privacy as one of the pathways to growing their business by improving trust with their customers.

—Steve Stein,  
Principal, Cyber Security Services, KPMG

”

**Americans have some room for improvement when it comes to protecting their data.** Sixty-one percent of Americans don't use computer security software or, when available, multifactor authentication. Additionally, 69% of consumers chose not to install mobile device security software when available.

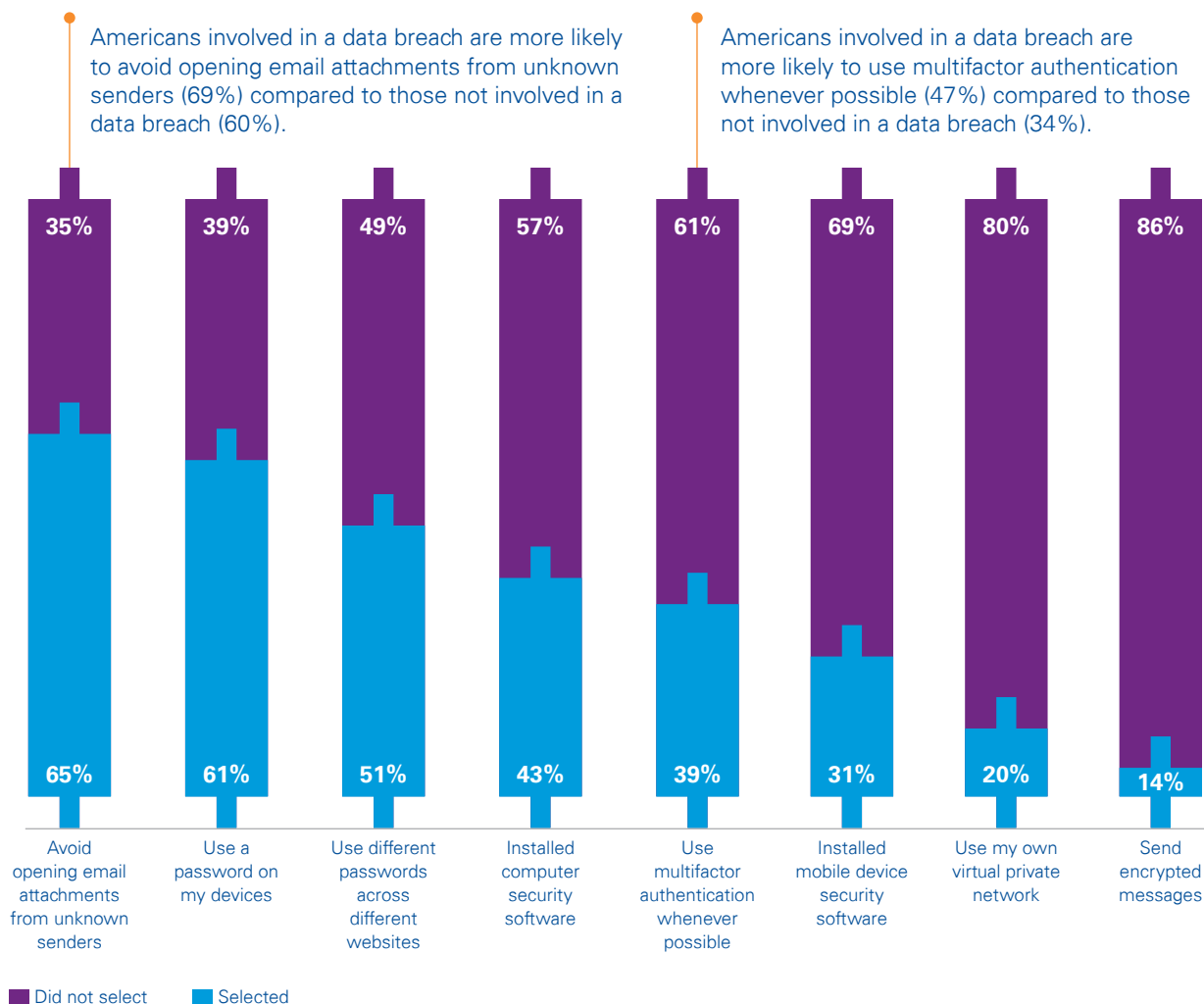
On a more positive note, people who've been involved in data breaches appear to have learned from their experience. Forty-seven percent in that group say they are likely to use two-factor authentication whenever possible, versus only 34% of those who haven't been impacted by a breach. (See Figure 2.)

"Part of the challenge for corporations will be getting employees and customers to do their part in protecting their own data," says Steve Stein, principal, KPMG Cyber Security Services.

"Developing defensible notices with understandable language and data protection controls that guide employees and consumers have to be embedded in the data security agenda," according to Stein.

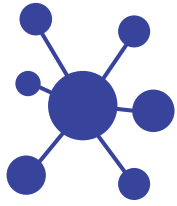
**Figure 2: Steps Americans take to protect their personal data**

**What do you do on a personal level to protect your data?**



Source: The new imperative for corporate data responsibility, KPMG, 2020





## Blockchain's growing role in ensuring data privacy

Blockchain's distributed ledger technology can be used to create decentralized identity systems in which different pieces of a consumer's personal identity, including associated metadata (such as credit information, home address, or other demographic information), are stored in different locations, with none of it accessible without a digital passport controlled by the individual consumer. Storing separate sets of data in different locations drives more security and privacy for personal data. Work toward this more secure data future has already started. ID2020, a global public-private partnership whose members include some of the world's largest tech companies, is seeking to develop a decentralized identity system worldwide.

Most recently, blockchain is used to ensure data privacy with contact tracing and other elements related to COVID-19. For example, a system leveraging blockchain helps track whether people have tested positive for COVID-19, if they've developed antibodies to it, and, once a vaccine is available, whether they have received the vaccine.<sup>2</sup>

Blockchain is also being used to bring rigor to contact tracing initiatives, which seek to identify individuals who may have come in contact with someone already contagious so they can self-quarantine and/or seek treatment.

"The great value in applying blockchain to data privacy is its ability to ensure that personal data sets are accurate and separate, which is important to business users, without exposing the identity of the individual, which is important to consumers," says Arun Ghosh, U.S. Blockchain leader at KPMG. "It is hard to envision a future for data privacy that does not incorporate blockchain as a fundamental enabling technology."

---

<sup>2</sup> "Using Blockchain to Beat COVID-19: Highlights From My Conversation With Shane Bigelow," by Shane Tews, American Enterprise Institute, May 1, 2020.

# Who should be responsible for protecting consumer data?

## Consumers recognize that the data privacy issue is too big for any one group to address alone—but insist that government and companies must play an active role.

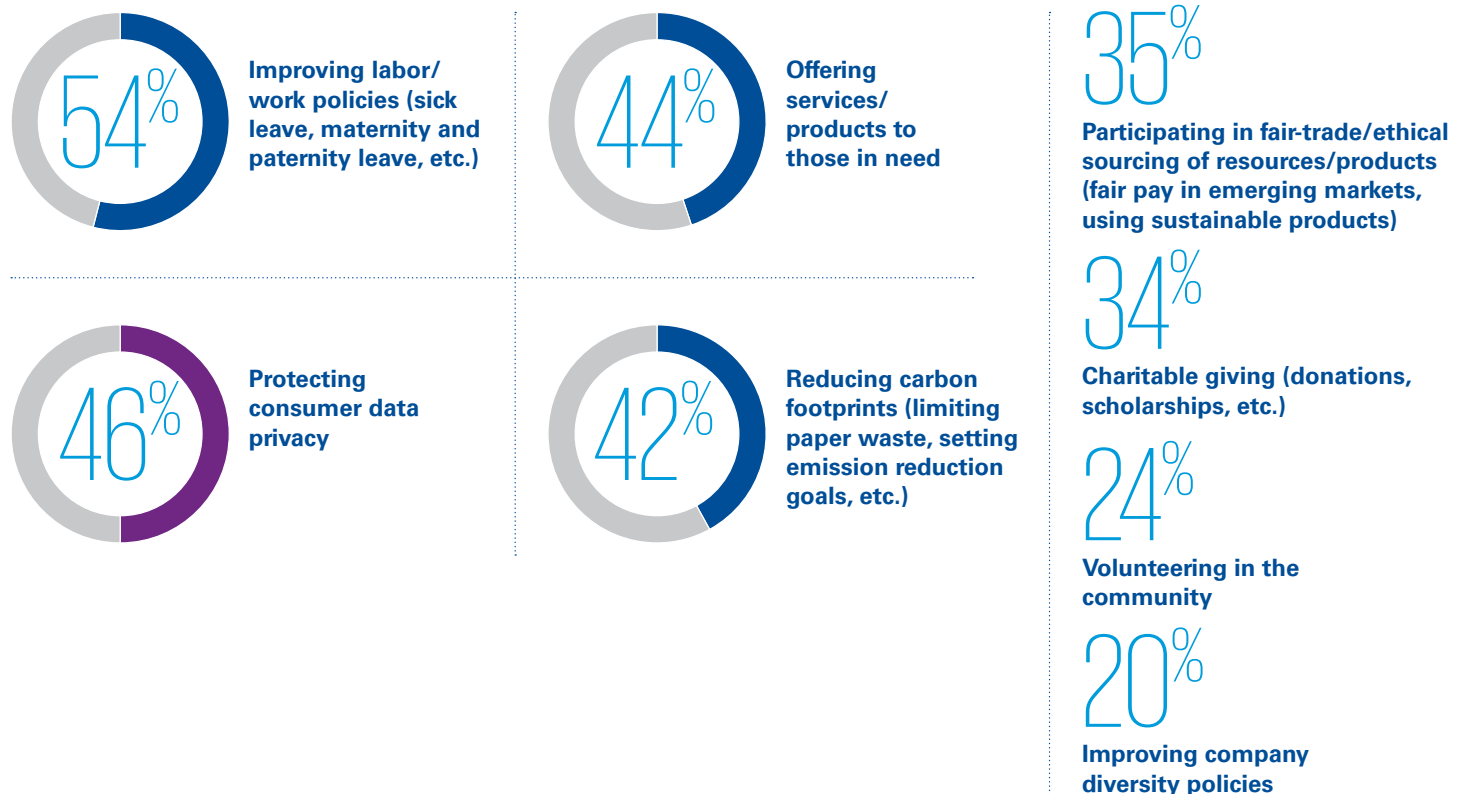
Eighty-six percent of survey respondents say consumers themselves have a responsibility to protect consumer data, but even more say government (90%) and companies (91%) have a role to play. Nine in 10 respondents say companies

should put data privacy guidelines and policies in place (92%), be held responsible for corporate data breaches (91%), take corporate data responsibility seriously (91%), and take the lead in establishing corporate data responsibility (91%).

In fact, when asked to prioritize a list of activities companies should pursue as part of their corporate social responsibility (CSR) agenda in 2020, data responsibility came in second, outpaced only by improving labor/work policies. (See Figure 3.)

**Figure 3: What consumers think corporations should prioritize for CSR agendas in 2020**

When it comes to corporate social responsibility, which of the following should organizations prioritize in 2020? Select all that apply.



Source: The new imperative for corporate data responsibility, KPMG, 2020

**Consumers want companies to give them more control over their own data.** Fifty-six percent of survey respondents say companies should prioritize giving consumers more control over their own data in 2020. Nearly as many say companies should provide consumers with timely, clear reports on data breaches and limit the use or sale of consumer data (55% and 53%, respectively). More than 4 in 10 respondents (48%) also want companies to provide clear insight into how and why consumer data is collected and used, provide consumers with more visibility into how it is used (44%), and update consumers on the specifics of how they are protecting and securing personal data (43%).

**Consumers are also open to legislation that would give them more control over their data.** Eighty-four percent of survey respondents say they would support state legislation giving consumers more control of their personal data, and many seem willing to look to California as a model. While only 33% say they are familiar with the California Consumer Privacy Act (CCPA), which took effect at the start of this year, they overwhelmingly back many of its central features when asked about them.

Nine in 10 respondents agree that all citizens should enjoy the following rights accorded to Californians by the CCPA: the right to delete personal data (91%), the right to know how their data is being used (91%), the right to opt-out of having their data used (90%), and the right to nondiscrimination in the use of their data (89%).

## “The overarching takeaway is that consumers crave transparency.”

The easier companies make it for consumers to keep tabs on how their data is being used and protected, the easier companies will find it to build consumers' trust. This is increasingly resonating with our corporate clients—by focusing activities that build greater internal and external visibility into the data that they collect, it becomes much easier to protect that data and maintain or gain trust with clients. This is being done with forward-thinking corporations and likely to gain greater acceptance among corporate stakeholders responsible for data management.

—Orson Lucas  
Principal, Cyber Security Services, KPMG

”



# What should corporations do now?

**With heightened consumer interest in data privacy, businesses must bring new rigor to their data privacy practices—or risk losing access to much of the information that makes today’s personalized customer experience strategies possible.**

In a recent study by Harvard Business Review Analytic Services, 46% of consumers said they’d stopped shopping with a retailer simply because they’d read its privacy statement and were not comfortable with it. Thinking about what they were getting from businesses in exchange for sharing their personal data, only 44% said they felt the exchange was worthwhile.<sup>3</sup>

If corporations don’t take the lead, as consumers have indicated they should, government may soon force business’s hand. Already, consumer

enthusiasm for the protections provided by the CCPA suggest that other states may eventually follow suit. And while federal policymakers have thus far been reluctant to impose regulations on data privacy, they’re not oblivious to what their constituents want. The bipartisan Exposure Notification Privacy Act introduced in the U.S. Senate on June 1 would give consumers controls over how their personal data is used by COVID-19 contact tracing and exposure notification apps.

---

<sup>3</sup> “The Great Data Exchange: What Businesses and Consumers Value in the Digital Economy,” Harvard Business Review Analytic Services, June 2020.

## As employers seek to improve their data privacy practices, KPMG recommends the following measures:

1	<b>Adopt a principles-based approach to data privacy and security.</b>	“With consumers indicating that they see data privacy as a human right, and new legislation expected in the years ahead, it is critical that companies begin to mature privacy programs and policies,” said Lucas. “Consumer demand for the ethical use of data and increased control over personal data must be a core consideration in developing data privacy policies and practices. Companies should consider adopting a principles-based approach to retain the flexibility needed to comply with the evolving regulatory environment and technology landscape.”
2	<b>Leverage emerging technologies to better protect and manage customer data.</b>	Data is the lifeblood of a modern organization. However, technology debt inherent to most organizations means that very few have robust and regular visibility into what data they have, who is accessing it, what it’s being used for, with whom its being shared, and how long it is retained. Further, ensuring that it is accurate and readily available is at least as challenging as managing a physical supply chain. To take full advantage of sprawling data sets—and to respond quickly and accurately to what KPMG expects will be expanding requirements to give consumers greater control over their personal data—businesses should consider leveraging data discovery and protection tools and exploring novel uses of blockchain and artificial intelligence (AI). These technologies can be employed to help companies better track the source of their data, assure its accuracy, make it easily discoverable, and protect it.
3	<b>Conduct privacy impact assessments, especially as new return-to-work solutions are introduced amid COVID-19.</b>	As companies look to bring employees and customers back to their facilities and retail spaces, many will undertake initiatives such as conducting temperature checks upon arrival; developing health questionnaires; monitoring employee interactions with customers, vendors, and business partners; and tracking COVID-19 cases. Because these are net new processes, many companies have not assessed the impact of personal information collection and use for information like geolocation and various types of protected health information (PHI). Where these new technologies and processes are implemented, it is prudent to assess and document the potential implications and decisions around data privacy. Where possible, companies should seek to embed privacy considerations and controls by design into the tools and processes used in these initiatives.
4	<b>Lead from strengths and make sure consumers know about your data privacy strategy.</b>	To build trust and goodwill with consumers, companies that develop strong data privacy controls will want to make sure consumers know about them. This will require an ongoing, multichannel communications strategy. In addition, some return-to-work solutions developed in response to COVID-19, such as testing and contact tracing, will require consent from employees, and companies will need to make employees comfortable enough to provide that consent. “Getting buy-in from employees and customers will be critical to getting back to workplaces while satisfying privacy rights,” says Stein. Coupled with a focus on data ethics, companies have a real opportunity to differentiate themselves, building deeper relationships with existing customers all while simultaneously increasing their market share.



## Strong data supply chains can contribute to data privacy and security

Your data analytics team wants to know if your customer files are current before launching a new targeted marketing campaign. A long-time customer in California wants assurance that you've deleted their personal data across your enterprise. The IT director at one of your European subsidiaries wants to know if the data file you sent over last week has all the information it will need to assure it can be used in compliance with the European Union's General Data Protection Regulation.

For many organizations, responding to inquiries like these with confidence can be challenging. Saddled with siloed information systems and struggling to oversee the gush of data flowing into those systems, they find it hard to confirm exactly when and where individual bits of data came from, whether they are up-to-date, and which regulations may be applicable to their use. They also can find it difficult to fully share with a consumer every piece of their personal data on file and how all of them are being used or protected.

With consumers paying closer attention to how their personal data is being collected, used, and protected—and governments imposing new regulations that give consumers more control over that data—companies need to assure the same levels of visibility and control into their data supply chains that they've long prized in their physical supply chains. Getting there requires building robust and highly automated information systems and governance procedures that can assure that organizations know what information they have, where it is located, how its use is governed, and how it is being protected. Beyond providing the capability to comply with data privacy laws and regulations, a robust data supply chain can make it easier for organizations to extract actionable insights from their data.

Building a robust data supply chain can be a large undertaking, but the tools are readily available—from well-organized data lakes and highly structured data warehouses to metadata management tools and advanced business intelligence tools. "Creating a strong and transparent data supply chain is becoming a foundational requirement for companies that want to excel at data privacy and security," says Jodi Morton, chief data officer, KPMG LLP. "You can't properly protect customer data if you don't have a firm grasp on data management and the ability to be strategic and nimble as you adopt new technologies and methodologies."





## Leveraging AI to improve data privacy and security

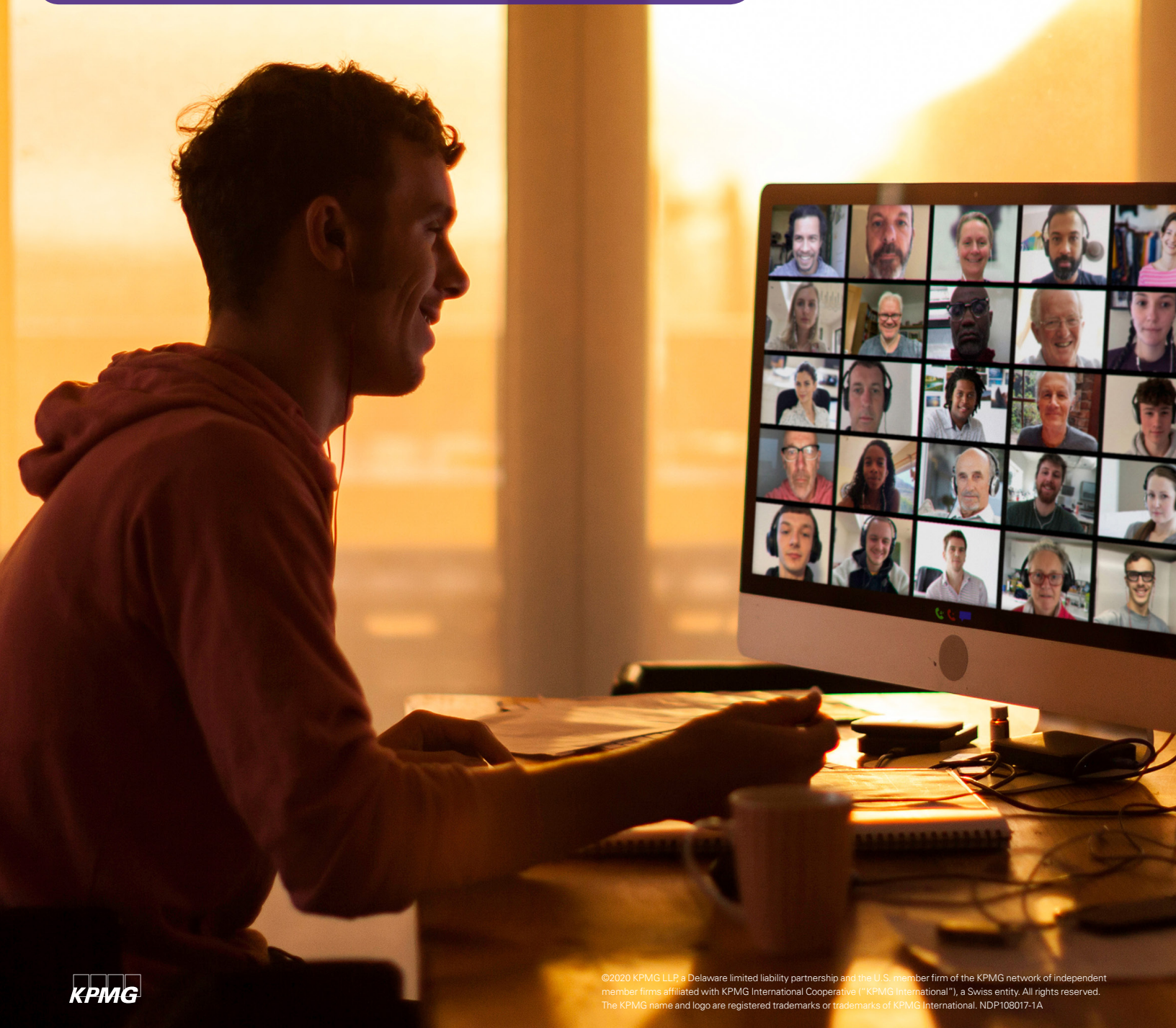
Data privacy is a dynamically changing expectation that will be a reality every organization will have to deal with in the future. With the Digital Revolution well underway, all organizations, big and small, find themselves dealing with disparate regulatory requirements—with more inevitably on the way. Further complicating this issue is the fact that customers can't all be treated the same. Privacy rules for protected groups, subgroups, and individuals differ within jurisdictions. Also, individuals themselves frequently hop in and out and between subgroups as their life-stage and personal preferences change.

Machine learning and other algorithmic AI capabilities can help organizations manage the complexity and scale required to holistically address privacy challenges. The same big data algorithmic learning techniques that have helped companies predict user behavior in shopping and click-stream entertainment can be leveraged efficiently to better anticipate and respond to their customer's data privacy preferences and ensure jurisdiction-level, organization-level, and individual-level privacy compliance. All this is possible with today's capabilities.

In the not-so-distant future, these same tools might be deployed to develop a personalized privacy ring-fence for use on individuals' smartphones and computing devices. "Algorithmically derived privacy assessment apps (on phones and other computing devices) could make it easier for consumers to understand privacy implications by tracking changes in their behavior and signaling when their privacy preferences should be modified," said Dr. Sreekar Krishna, principal, Innovation & Enterprise Solutions, KPMG LLP. "Similarly, corporations may be able to build enterprise-scale algorithmic privacy barriers around their data lakes and warehouses to ensure that data flowing in and out of them does so in accordance with their privacy policies."

# Methodology

The findings in this report are based on the results from a survey of 1,000 respondents. The sample was balanced to reflect national representative of age, race, gender, and region. The online survey was fielded between May 19, 2020 and May 21, 2020. The margin of error (MOE) for the total sample at the 95% confidence level is +/- 3.1 percentage points.





# Conclusion

**Business leaders appreciate how much their organizations have come to rely on personal consumer data to provide deep insight into what their customers want, and to deliver it to them in increasingly targeted and personalized ways.**

Many business leaders also understand that to retain the consumer's willingness to share personal data their organizations must improve their data privacy and protection strategies. Indeed, in a survey of 600 global technology executives in late March and early April, KPMG found that improving cybersecurity and data privacy is one of the top four objectives for which their organizations are investing in emerging technologies such as process automation, smart analytics, cloud computing, AI, and blockchain.

All these efforts will be important to building consumer trust and preparing corporations for the next round of regulations that appear at the federal and state levels. In the meantime, COVID-19 only accelerates the data privacy issue. As businesses scale operations back to normal, it will be critical that all their stakeholders, especially customers and employees, are confident that the personal data collected to facilitate that restart will be used ethically and safeguarded properly.

“

## Getting data protection and management right isn't optional.

Corporations rely on the insights they get from customer data to sharpen their strategy and enhance the customer experience. But with access to that data comes an obligation to protect it. Ultimately, consumers will hold organizations that fail to do so accountable.

— Orson Lucas  
Principal, Cyber Security Services, KPMG

”



# Authors



## Orson Lucas

**Principal,  
Cyber Security Services,  
KPMG**

Orson Lucas, coleader of the KPMG Privacy Services offering, has over 19 years of experience helping clients identify and protect their most sensitive information assets as well as helping clients across industries to navigate complex privacy, security, and other compliance risks.



## Steven Stein

**Principal,  
Cyber Security Services,  
KPMG**

Steven Stein is global lead of the KPMG Information Governance Services methodology and U.S. coleader of the KPMG Privacy Services offering. Steven focuses on data privacy and protection; information governance; records management; and governance, risk management, and compliance (GRC). He leads global projects for Fortune 100 corporations in privacy, information, and data governance strategy; GRC program design and implementation; regulatory change management; and data minimization.



# Contact us

## **Orson Lucas**

**Principal, Cyber Security Services**  
**KPMG**

**T:** 704-502-1067

**E:** olucas@kpmg.com

## **Steve Stein**

**Principal, Cyber Security Services**  
**KPMG**

**T:** 312-952-3110

**E:** ssstein@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

©2020 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDP108017-1A