KPMG

Corporate data responsibility

Bridging the consumer trust gap

August 2021

visit.kpmg.us/CDR2021

Bridging the trust chasm

As businesses collect more and more personal data, consumer privacy concerns continue to rise. To build consumer trust, companies should consider taking meaningful action to place data protection at the forefront.

Businesses have a voracious appetite for consumer data. This valuable customer information helps feed predictive analytics, personalize marketing campaigns, and introduce/improve products and services. But how do consumers feel about companies using their data? And what are their expectations of privacy?

KPMG conducted research to understand how corporate data practices and consumer expectations are shifting. Over the past year, 70 percent of companies increased their collection of personal consumer data, according to our survey. At the same time, many consumers are increasingly concerned about how companies are using their data. Four in 10 say they don't trust companies to use their personal data ethically, and three in 10 oppose sharing it for any reason.

To allay these concerns, consumers overwhelmingly say they want more transparency around how their personal data is being handled and protected. Without meaningful efforts to address these concerns, the number of people opposed to sharing information with companies will likely rise.

Businesses need to take action now to bridge the chasm between their activities and consumer expectations – or risk losing access to the data they need for growth. Building on the findings from our survey and our extensive experience helping clients, this report identifies opportunities for businesses to reclaim consumer trust by being more transparent and thoughtful about their data collection, use, and protection. We hope you find these insights helpful as your organization navigates the evolving data-privacy landscape.

Orson Lucas
Principal, Advisory,
US Privacy Services
Leader

Martin Sokalski
Principal, Advisory,
Emerging Technologies and
Digital Solutions Leader

Rob Fisher
Principal, Advisory,
US KPMG IMPACT Leader

KPMG

Key findings

Business leaders

70%
say their company increased collection of consumer personal data over the last year

62%
say their organization should be doing more to strengthen existing data-protection measures

33%
say consumers should be concerned about how their personal data is used by their company

29%
say their company sometimes employs unethical data collection methods

U.S. General Population

86%
say data privacy is a growing concern

68%
are concerned about the level of data being collected by businesses

40%
don't trust companies to use their data ethically

30%
aren't willing to share their personal data for any reason

Methodology

The U.S. General Population

The findings in this report are based on an online survey among a nationally representative audience of 2,000 U.S. adults, ages 18+, including a natural fallout of 974 U.S.-based workers, fielded from April 30, 2021, to May 6, 2021. The margin of error at the 95% confidence level is +/- 2.19 percentage points for the general population and 3.14 percentage points for U.S.-based workers.

Business leaders

The findings in this report are based on an online survey among 250 director-level (or higher) decision-makers with involvement in security/privacy/data decisions at companies with 1,000+ employees from April 30, 2021, to May 12, 2021. The margin of error at the 95% confidence level is +/- 6 percentage points.

Business practices around personal data continue to trail consumer expectations.

Business leaders and the American public are not on the same page. Seventy-five percent of business leaders say they are comfortable with the level of data their company collects, yet 68 percent of the U.S. General Population say they are concerned about it. Companies that aren't able to keep pace risk alienating consumers, potentially prompting a more conservative stance on sharing personal data—a troubling prospect for businesses reliant on consumer data to refine their marketing strategies and enhance their products.

"This split between business and consumer sentiment isn't new, but its persistence shows that businesses have a long way to go if they want to make the public more comfortable with how they are collecting, using and safeguarding data," says Orson Lucas, KPMG US Privacy Services Leader. "Failure to bridge this divide could present a real risk of losing access to the valuable data and insights that drive growth."

Many consumer concerns are grounded in mistrust of business ethics. When it comes to using personal data ethically, 40 percent of the U.S. General Population say they don't trust companies to do the right thing, and 13 percent don't even trust their own employer. So deep is this mistrust that 47 percent of those surveyed believe their smart devices are listening to their conversations, even though that notion has been discredited by research.

"While there is no standard definition of unethical consumer data use, it shouldn't be terribly difficult to identify," says Martin Sokalski, Principal, Advisory, Emerging Technologies and Digital Solutions Leader. "If companies would not want their data practices in the headlines—out of fear of what consumers might think—it makes sense to reconsider."

In addition to concerns about how businesses are collecting and storing data, there are even greater fears that this data might be compromised or sold. Many of the U.S. general population say they are very concerned about how companies collect (40%) and store (39%) their data, respectively. But even more are very concerned about the possibility that companies holding their data could be hacked (47%) or that their data could be sold (51%). To be fair, selling data to a third party is a tangential practice for most businesses these days: only 17 percent of business leaders say their company engages in this practice. Businesses may need to be more direct and transparent on this point to ease consumer fears.

"Communicating with the consumer around data use and protection is an ongoing responsibility," Sokalski says. "It's critical to closing the trust gap."

40% of the U.S. General Population *say they don't trust companies to do the right thing, and* ***13% don't even trust their own employer.***

1 Daniel J. Dubois, Roman Kolcun, Anna Maria Mandalari, Muhammad Talha Paracha, David Choffnes and Hamed Haddadi, "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," Northeastern University, updated July 21, 2020.

Business leader views suggest there is reason for consumer concerns.
While 95 percent of business leaders say their company has strong or very strong data protection measures in place, 62 percent concede that their companies should be doing more. This validates consumer concerns about corporate practices. In addition, when speaking about their own employer, 33 percent of business leaders corroborate that consumers should be concerned about how their personal data is used by their company, and 29 percent openly acknowledged that their company sometimes uses unethical data-collection methods.

"People tend to underreport behaviors that place them or their organization in a negative light," says Lucas. "It is a disturbing finding that more than one in four survey respondents work for a company that sometimes uses unethical data-collection methods. This goes a long way toward explaining why consumers are wary."

The chasm between businesses and consumers may continue to grow.
Seventy percent of business leaders say their company increased its collection of personal consumer data over the past year. But without intentional action to safeguard data and educate consumers, the gap between business practices and consumer expectations could continue to grow.

"The collection and use of consumer data has become so integral to business operations that it is hard to imagine companies will pull back unless forced to do so," says Rob Fisher, US KPMG IMPACT Leader. "But the longer companies lag behind consumer expectations, the risk of losing access to that data will grow exponentially. The challenge moving forward will be to better align practices with the expectations of customers and potential customers."

"Businesses should consider how leveraging data discovery and governance tools, as well as exploring the implications of new use cases powered by emerging tech like Machine Learning and AI, can enhance data protection and build consumer trust. These technologies can help organizations build greater visibility into their data practices, from better data tracking to helping ensure integrity and fairness throughout the lifecycle."

— Martin Sokalski, Principal, Advisory, Emerging Technologies and Digital Solutions Leader

One risk for businesses: Concerned consumers could shut off the personal data spigot.

As consumers worry about personal data privacy, they appear to be changing some of their behaviors.
Eighty-six percent of the U.S. general population say data privacy is a growing concern for them, and 30 percent say there are no circumstances under which they would be willing to share their personal data with businesses. Of course, words and actions don't always align. Many consumers regularly share their personal data—often to gain access to perks offered by businesses—and engage in online behaviors that could put their personal data at risk. These trends suggest a certain level of what could be viewed as resignation about the risks inherent in an increasingly digital world.

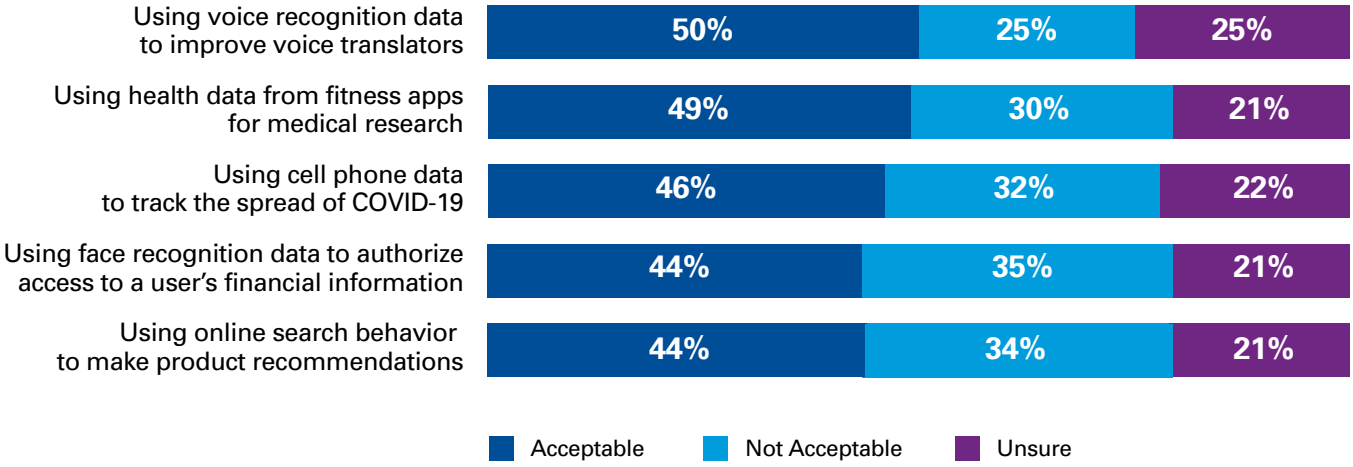
A shockingly low number of consumers can identify circumstances that would prompt them to willingly share their personal data.
Only 12 percent of the U.S. general population say they would share their data to make online ads more relevant to their interests, and only 17 percent say they would do it to help businesses create better products and services. Even to advance the greater good, only 30 percent say they would share their data.

As one survey respondent noted, "I don't feel comfortable with corporations having my personal information on file, as I am concerned about hacking and information leaks. Even if their intentions are good and legitimate, it leaves my information vulnerable." Another respondent added: "I don't want my information ever sold or shared with other companies. I also don't want my shopping behavior to be used to target me for other purchases."

Nonetheless, consumers indicate a greater willingness to share when presented with more specific use cases. This suggests there may be an opening for businesses to win consumer trust.
Many say there are acceptable use cases for their personal data. For example, 57 percent say using facial recognition technology to assist in criminal investigations is acceptable, while 52 percent are comfortable with companies using recorded calls for quality and training purposes. These findings suggest that the more specific businesses are about how personal data will be used, the more likely they will win consumer confidence. (See the U.S. general population data use findings on next page)

86% of the U.S. general population *say data privacy is a growing concern for them, and 30% say there are no circumstances under which they would* ***be willing to share their personal data with businesses.***

The U.S. general population responds more favorably when told exactly how their data will be used, although many aren't sure which use cases are acceptable.



View better data management not as a risk-avoidance exercise, but as an opportunity

By using increasingly precise consent management tools, smart businesses are giving consumers more control over the personal data they share and how it will be used. But many focus too much on how these tools manage corporate risk—like avoiding unauthorized use of consumer data—and miss massive opportunities to build richer relationships with consumers. When consumers opt in to share their data, it can indicate they are interested in a deeper level of engagement with a business, and businesses shouldn't miss these opportunities to engage. Businesses can use these opportunities to establish more productive and mutually-beneficial relationships with their customers and prospects.

— Orson Lucas, Principal, Advisory, US Privacy Services Leader

Businesses have an opportunity to shift consumer thinking on when to share personal data.

With heightened consumer concerns around data privacy, businesses should bring new rigor to their data practices. KPMG recommends the following actions to build enduring consumer trust.

Be more explicit and transparent about how consumer data will be used.
Seventy-six percent of the U.S. general population say they want more transparency around how their personal data is being used by companies, and 40 percent say they would willingly share their personal data if they knew exactly how it would be used—and by whom. At the same time, only 53 percent of business leaders say their company has taken active steps to demonstrate how consumer data will be used.

"The best data use disclosures are thorough, well-organized, and easy to understand," says Fisher. "They show consumers who is using their data and how, and draw a clear connection between the business use case and benefit to the consumer."

Give consumers more direct control over their personal data.
Seventy-seven percent of the U.S. general population and business leaders say they want more control over their data, but roughly four in 10 businesses aren't giving it to them. Currently, 59 percent of business leaders say their company gives customers control over how much personal data goes to whom, and only 52 percent offer the ability to opt out of sharing personal data. Only 50 percent allow consumers or clients to view the personal data the company has already collected on them, and only 48 percent offer access to a website devoted to the company's data collection and/or use practices. More encouragingly, 45 percent say giving consumers more control of their personal data is a priority for 2021.

Make data anonymous to whatever extent possible.
Forty-eight percent of the U.S. general population say they would be more comfortable with companies collecting and using their personal data if it was made fully anonymous. "Data anonymization techniques are becoming more sophisticated, and allow businesses to gain real market intelligence without compromising individual privacy," observes Lucas. "While this is not always realistic, it should be part of every company's data toolkit."

Seize the moment and take the lead.

Forty-nine percent of the U.S. general population say they don't know how to protect their personal data—suggesting that many might welcome some assistance. However, 64 percent say companies aren't currently doing enough to help them. The vast majority of the U.S. general population—88 percent—say they want corporations to take the lead in establishing corporate data responsibility and share more details on how they protect data.

"Our research has provided insights into how individuals want businesses to handle their personal data," says Sokalski. "Companies that take the lead on this issue—by demonstrating that they are hearing what consumers are saying and taking meaningful action—will be positioned to reap the ongoing benefits of access to consumer data."

Tap the power of competence, integrity and humanity

Building trust in your organization's data practices requires transparency and the ability to consistently live up to your standards. Your organization can enhance consumer trust by demonstrating competence, integrity, and humanity in connection with data practices. **Competence** reflects the ability to securely handle data because you have the appropriate technology, along with the right policies and practices, across the entire customer journey. **Integrity** aligns with the courage to be transparent about how you are using data and how it impacts the consumer. **Humanity** comes through developing data practices that treat consumers the way you might like to be treated. Elevating your trust factor might mean giving consumers more opportunities to opt out of sharing data, or even making 'opt out' the default choice. By demonstrating competence, integrity and humanity, businesses can build enduring consumer trust—an increasingly critical currency in our rapidly changing environment.

— Rob Fisher, Partner, Advisory, US KPMG IMPACT Leader

When it comes to data-security practices, employees paint a less glowing picture than business leaders

The vast majority of business leaders express confidence in their data security prowess, but their employees often paint a less rosy picture.

Ninety-five percent of business leaders say their company has strong or very strong data protection measures in place. Ninety-two percent say their company is prepared for a data breach, with 37 percent adding that their company has already been tested by an external security threat. And 98 percent say data privacy is a priority for their organization. A high percentage of business leaders also say their company offers a broad range of data security training to their employees, and that their employees take this training seriously.

Perhaps, but that doesn't mean consumers—or even their own employees—agree. In fact, many employees aren't convinced they're getting much out of their training, which means companies may be less secure than they imagine. Thirty-five percent of U.S.-based workers surveyed say their trainings are not useful, and many say they are not taking full advantage of the training programs available to them, especially if they work part-time. For example, only 47 percent of full-time employees and 42 percent of part-time employees say they have had training on password security. And the percentages are even lower for training on data protection (44% and 30%, respectively), email security (43% and 25%), privacy (40% and 30%), privacy policy compliance (34% and 25%), and phishing (29% and 14%).

In fact, barely half of U.S.-based workers surveyed report using basic data protection methods at their companies. Only 49 percent say they use a password on their devices, only 45 percent avoid opening email attachments from unknown senders, and only 38 percent have installed computer security software. Finally, less than half (44%) say they fully understand their company's data policies.

For all the confidence business leaders express around their data security standards, a significant number acknowledge that their organization has room to improve. Sixty-two percent concede their company should be doing more to strengthen existing data protection measures, for example. In fact, many businesses are planning to step up their data-security game. A major driver of this focus is the shift to remote work since the start of the COVID-19 pandemic, which 59 percent of business leaders say has exposed their company to more security threats. Eighty percent of business leaders say the shift to remote work has caused their organization to heighten data-security protocols, and the same percentage say it has prompted them to increase their focus on data protection and privacy over the next 12 months.

Building trust

Businesses rely on consumer data for a wide range of applications. Eighty-four percent of business leaders say their organization uses personal consumer data to improve products and services, 70 percent say they use it to support the use or development of emerging technologies, and 50 percent use it to inform their marketing and advertising efforts.

Given the critical and growing importance of consumer data, it makes sense for businesses to develop policies and practices that address consumer concerns around how their data is being collected, used and protected, and to be forthright and empathetic in developing and sharing those policies and practices.

By taking the right approach to data—being more transparent and giving consumers more control—businesses have an opportunity to build consumer trust and solidify access to this critical resource.

Even in their own workplaces, many consumers worry about data privacy

Most business leaders say they are doing things right around the collection, use, and safeguarding of their employees' personal data. Eighty-six percent say they are transparent about the data collection process, and 71 percent say they're comfortable with the level of employee data they collect.

Still, U.S.-based workers are leery. Fifty-three percent say their company should be more transparent about their collection and use of employee data, and only 52 percent say their company regularly informs them of its data collection and use practices.

Employees are most opposed to their employers viewing their social media accounts (44% say it's not acceptable), monitoring their instant messaging (32%), and reviewing their browsing history (32%). They are less concerned about employers using their personal data to track when they start work (17%) or their productivity (24%).

"Companies that want to lead in the ethical use of personal consumer data can start at home by being transparent about how they collect and use data on their own employees," says Lucas. "Beyond being the right thing to do, it helps set a good example for how employees should think about the collection and use of consumer data."

Just about everyone wants government to play a bigger role in data security

Businesses and consumers may not be on the same page when it comes to how well businesses protect and ethically use personal consumer data. But they share at least one common desire—for the federal government to step up and get involved.

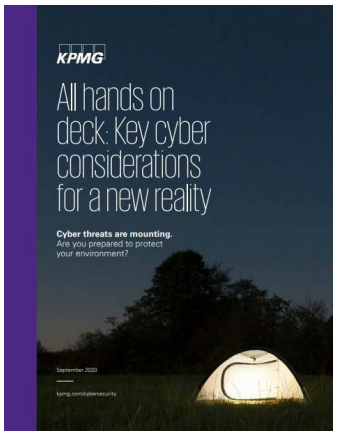
Eighty-seven percent of the U.S. general population and 76 percent of business leaders agree there should be more rules and regulations around data collection, management, and storage. When asked who is most capable of setting these new rules and regulations, a greater percentage of both the U.S. general population and business leaders point to the federal government rather than businesses themselves, state or local governments, or consumers. And 77 percent of business leaders say the U.S. should pass a national law to protect consumer data privacy.

How can KPMG Help?

To create experiences that regularly exceed customer expectations, businesses must be intentional about putting customers at the forefront in order to build their trust. By designing and orchestrating seamless and personal customer, employee, and partner experiences, organizations can improve their reputations among customers and build teams that understand the business's overarching vision.

KPMG helps enterprises create experiences that build customer trust by incorporating strategies and practices that give consumers more explicit and transparent control over the personal data they share and its usage. Pre-configured technologies can be customized to get companies started faster on the path to refining data collection, use, and protection processes in order to bridge the trust gap between corporate data practices and consumer expectations.

Related content



All hands on deck: Key cyber considerations for a new reality

Regulatory and compliance transformation library

Contact

Orson Lucas
Principal, Advisory
US Privacy Services Leader
olucas@kpmg.com

Martin Sokalski
Principal, Advisory
Emerging Technologies and Digital Solutions Leader
msokalski@kpmg.com

Rob Fisher
Principal, Advisory
US KPMG IMPACT Leader
rpfisher@kpmg.com

kpmg.com/socialmedia

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