The path to transparency —and trust

Corporate Data Responsibility Survey 2022

December 2022

visit.kpmg.com/us/cyber
visit.kpmg.us/marketingconsulting

There's a lot of data out there...

For decades, researchers, academics, and business leaders have pondered the ever-proliferating amount of data with which we contend and how to effectively collect, store, manage, understand, deploy, and protect it. Every day, every hour, every second, corporations extract vast quantities of customer facts, statistics, and behavioral trends. Data—big and small, structured and unstructured—is essential, and as the volume expands exponentially, so too are consumers' concerns over the security of their personal information.

For the past several years, KPMG has explored not just how companies collect, manage, and use data, but also the degree to which these activities are carried out ethically. This annual study examines the opinions of the U.S. general population, American workers and business leaders in relation to current consumer data practices. Ideally, as we consider the relationship between data privacy and data security, we want to capture the difference between the way consumers are feeling and the way companies are acting; what consumers are concerned about and what companies are focused on.

Year over year, the survey has confirmed that American workers increasingly don't trust companies to use the data they collect ethically and generally don't trust corporate America at all. The data suggests that Americans are themselves in a somewhat contradictory frame of mind. They're concerned about the improper use of their data, but still exhibit behaviors that increase their risk, suggesting they likely don't fully understand what's happening in the marketplace with respect to their personal information. Adding to the contradiction, the survey tells us that Americans approve of companies using data in ways that are beneficial to them but consider the sale of their data unacceptable. If data is to be sold, it must be done ethically and with complete transparency: Recent regulatory enforcement has underscored the criticality of transparency and consumer choice.

Americans don't typically understand what type of data companies need to provide the products and services they provide. Individuals, it would appear, are not necessarily able to articulate what they want, but companies largely have not attempted to explore this lack of perspective on the part of customers to address the issue. Clearly, there's much ambiguity between consumers' perception of value they trade for their information, and companies' ability to communicate the purpose of data collection and use (and indeed, sometimes even to fully understand the data they are collecting and using).

Increasing transparency around the collection and usage of consumer data will not be achieved overnight. It requires organizations to reassess value chains, operating models, and digital investments while government develops a new regulatory framework. But ongoing incremental change can transform the data dynamic.

Perhaps the most significant implication is how a transparent, collaborative, and secure data policy will impact firms in the marketplace: you don't do it out of the goodness of your heart; you don't do it because the government is forcing you to; you do it because it's good business and can be a competitive differentiator.

Hopefully, the results and insights from this year's survey will inspire you to boldly pursue creative new strategies and employ emerging technologies to expand your customer base, increase efficiencies, and achieve sustainable growth. We are always available to help you leverage and implement the latest thinking on data security and privacy and help ensure your organization is ready for tomorrow's challenges—today.

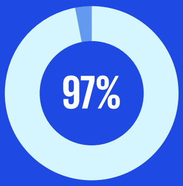
Orson Lucas
Principal, Advisory
U.S. Privacy Services Leader

Bret Sanford-Chung
Managing Director
U.S. Marketing Consulting

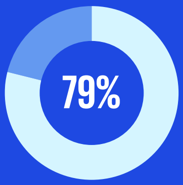
KPMG

Key survey data

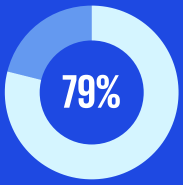
Business leaders



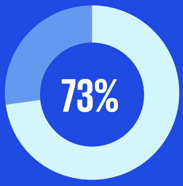
are confident in their organization's plans for collecting/using customer data over the next three years



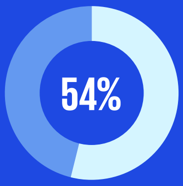
say their companies increased marketing and/or advertising technology spending during the pandemic



say consumer engagement (email opens/clicks, time spent on page, items added to cart, etc.) is their #1 source of consumer data

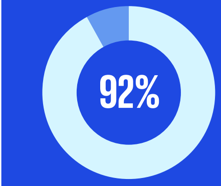


of companies are collecting more personal data than last year, but only 49 percent provide clear information about how/why data is collected/used, and only 45 percent provide timely breach reports

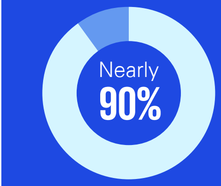


have proactively moved away from collecting third-party data, but 25 percent currently sell customer data to third parties

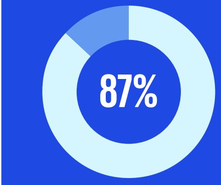
U.S. general population



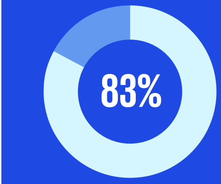
are very/somewhat concerned about protecting their personal data



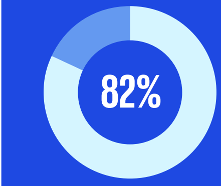
want companies to take their data responsibility seriously (89 percent), have guidelines and policies in place (89 percent), and share more details on how they protect data (87 percent)



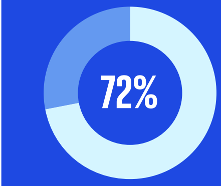
agree that companies should take the lead in establishing corporate data responsibility



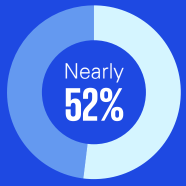
are concerned about companies selling their data



are concerned about corporate data breaches



believe using public Wi-Fi poses a security risk



of American Workers trust their companies to use their personal data ethically

Businesses still have not made consumers comfortable when it comes to data security

Business leaders are confident about their data collection and usage practices, but Americans remain concerned

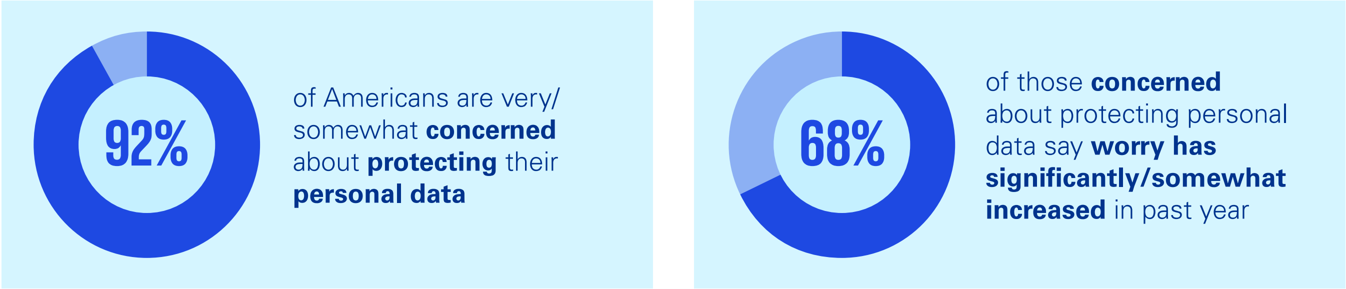
One fundamental finding that comes as no surprise to anyone is that the vast majority of Americans are worried about their data, with 92 percent of the U.S general population acknowledging they are very or somewhat concerned about protecting their personal information. This is an increase from 2021, when 86 percent noted this concern. Generationally, baby boomers are more concerned about data security than the other cohorts. Nearly all—95 percent—said they are somewhat or very concerned.

For their part, business leaders are feeling extremely confident in their data programs. When it comes to data collection and usage in particular, businesses are collecting more data every year, with the amount of customer data growing by 10 points at respondents' own companies between 2021 and 2022 and 15 points across their industry year-over-year.

Indeed, approximately 62 percent of business leaders say they are more transparent today than they were three years ago regarding how data is processed. However, 80 percent of Americans are concerned that companies lack transparency around the use of consumer data. Nearly 9 in 10 consumers (87 percent) feel that companies should share more details on how they protect data.

As stated above, virtually all Americans are concerned about personal data security. What is even more interesting is that 70 percent said the intensity of that concern has increased in the last year. Baby Boomers in particular expressed a great deal of concern over the security of their personal data with nearly two-thirds (63 percent) saying they are very concerned—perhaps they feel they have the most to lose as the result of a data breach.

Personal data protection is top-of-mind for almost all; nearly 7 in 10 report increased worry over last year



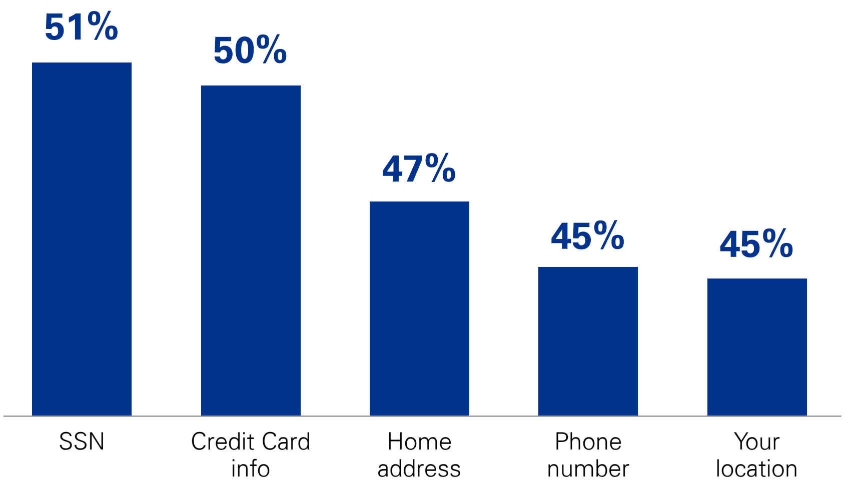
of Americans are very/ somewhat **concerned** about **protecting** their **personal data**

of those **concerned** about protecting personal data say **worry has significantly/somewhat increased** in past year

Source: KPMG, 2022 Corporate Data Responsibility survey.

And along with that concern, we're seeing a rising reluctance among Americans who are willing to share different types of data. Heading that list is financial information, such as social security numbers and credit card information. Next in terms of sensitivity is what would typically be classified as personally identifiable information (PII)—a home address, phone number, or even some of the geolocation tagging that companies employ, which is widely considered personal data.

Americans are more reluctant to share financial and personal data today versus three years ago

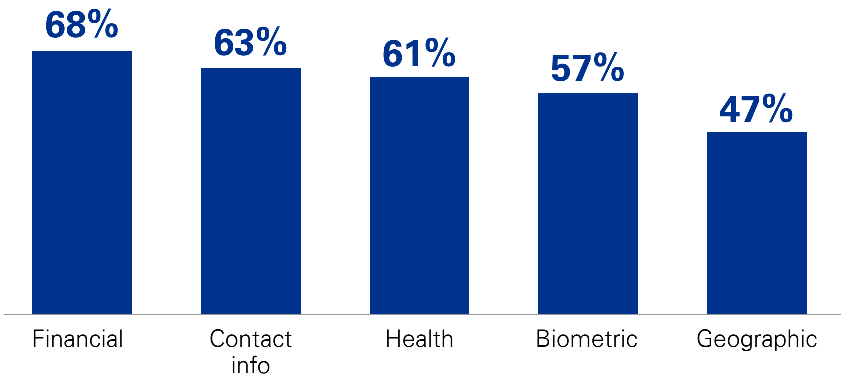


Source: KPMG, 2022 Corporate Data Responsibility survey.

Interestingly enough, on the flip side of consumer hesitancy to share, nearly two-thirds of business leaders (63 percent) perceive that consumers are less willing to share data with them than they have in past years.

Something of a corollary to consumers' concerns about sharing data is that, when they do, they have a very high expectation that businesses will protect it and keep it private. Not surprisingly, consumers are just about equally concerned about financial information, PII, and health-related data.

Types of data Americans expect businesses to protect and keep private



Source: KPMG, 2022 Corporate Data Responsibility survey.

Although there are significant HIPAA-specific rules and regulations surrounding the protection of health information, it's still high on the list of the data that Americans want kept private by business.

Bottom line: Implications and recommendations

Consumers want more trust in and control over the use and collection of their data. Companies that provide access to clear information about their data use collection processes can expect to improve the level of trust among customers.

And that confidence among consumers can lead to more cookie acceptances, more data sharing, and in turn, greater personalization. The key recommendation for businesses—marketers in particular—is to provide that information early in the customer relationship cycle to address consumers' main concerns—the sale of customer data, timely reports on data breaches, and overall data responsibility strategies.

This is essentially a recommendation to marketers at these organizations to consider putting out information like this to help address concerns and engender more trust in the firm's data collection practices.

Clearly, American consumers are concerned about their data, but companies, by and large, are operating as though all is well. Consumers are willing to share data if they perceive there will be a value exchange, but that's an issue of data privacy as opposed to data security. They will dispense with a degree of data privacy, but under all circumstances consumers expect their personal information to be secure. Companies need to make that distinction between privacy and security.

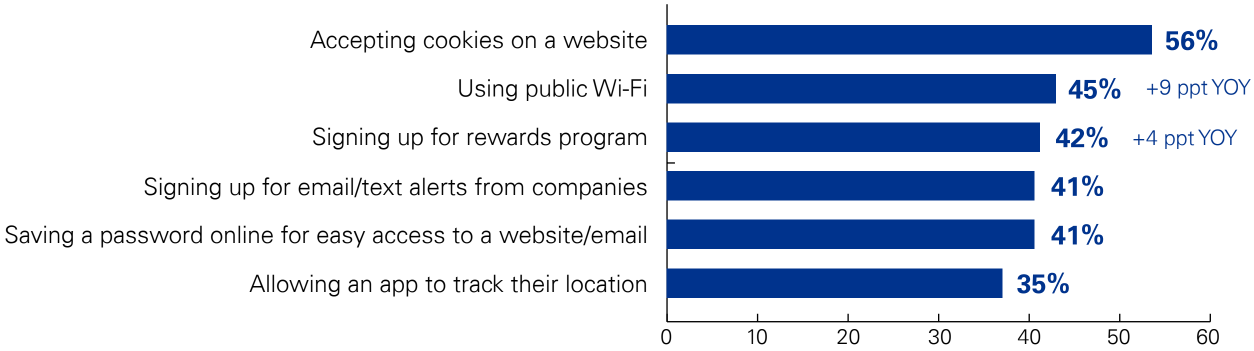
It’s not what they say, it’s what they do

Despite concerns, Americans continue to share personal data and engage in online activities they know may pose security risks

Although Americans claim that they’re concerned about their data, there is a discrepancy between their declarations and actions. This gap becomes even more pronounced when we look at American data-sharing behaviors.

Despite their ongoing anxiety, Americans continue to engage in online activities that might be considered likely to expose them to breaches and other data-related risks. They share data—a lot of it in fact. The most common data-sharing practices include accepting cookies online (56 percent of respondents), using public Wi-Fi (45 percent) and signing up for rewards programs (42 percent). In fact, public Wi-Fi and rewards programs have increased by nine and four points in 2022 relative to 2021. It’s no revelation, but most of these data-sharing behaviors relate to convenience. The other type of behavior aligns with a potential benefit or reward.

Top data-sharing behaviors—despite data security/privacy concerns



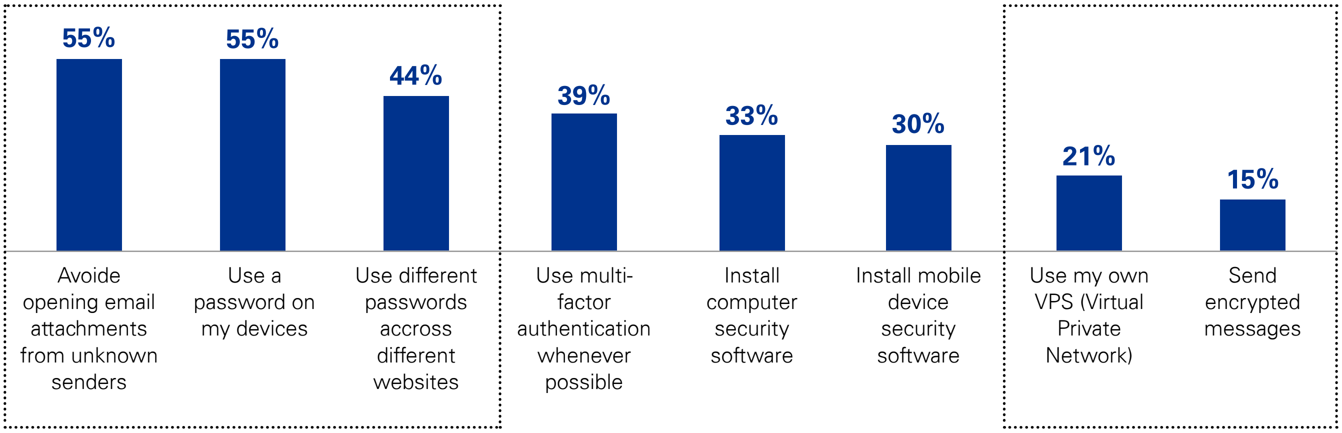
Source: KPMG, 2022 Corporate Data Responsibility survey.

It bears mentioning that the perception of certain behaviors as potentially risky does not seem to have an impact on whether or not Americans will continue to engage in them. For example, while nearly 60 percent of Americans believe that accepting cookies on a website may pose a security risk, nearly half of those who share that belief continue to engage in this practice. (We would remind you that cookies by themselves are not a threat. The danger is in their ability to track browsing histories.) Similarly, almost three-quarters of Americans (72 percent) believe using public Wi-Fi may be a security risk, yet more than 40 percent of those who consider it risky still do it.

Despite this misalignment of risk assessment on one hand, and actual data-sharing behaviors on the other, Americans of course still want their data to be safe and secure. And this leads them to incorporate a variety of behaviors and practices that are aimed at minimizing the likelihood of their data being compromised. Data security-oriented practices cover a broad spectrum. On one hand, we have the more obvious basic behaviors that rely primarily on the level of caution and vigilance one employs, such as being cautious about opening email attachments or diversifying passwords across different websites and accounts.

On the other side of this spectrum are the more advanced technology-driven practices that were developed with data protection in mind, such as connecting to the internet using a VPN, or using the communicators that offer message and encryption that are becoming more and more popular.

Data protection practices intended to secure data, ranging from basic to advanced



Source: KPMG, 2022 Corporate Data Responsibility survey.

Those more technologically advanced solutions are more popular among younger generations. We also found that those younger generations tend to be less reluctant to willingly share their data. Approximately a quarter each of Gen Z and millennials rely on VPNs. This suggests that while they may not be as concerned about sharing their data in general, they do want to share it in a secure manner that they feel they can control.

Bottom line: Implications and recommendations

In today's digital business environment, consumers are feeling pressured to opt-in to requests for personal data despite feeling uneasy about it, because they want to receive the benefits attached to a product or service. Consumers often use public Wi-Fi and accept cookies without reading the consent documentation, even though they know there may be risks involved.

This is an opportunity for businesses to double down on communicating their commitment to—and the benefits of—responsible and secure data sharing.

Companies are encouraged to deliver the message that consumers' lives online would be more convenient if the products and services they use frequently are tailored to their needs and priorities. Further—and an equally important messaging point—the personal data people share is the linchpin in this process and must be protected through a consistent process that makes them feel confident about providing it.

The reality, however, is many companies are not doing this. Many are just moving forward apace, hoping customers continue to share data and that they don't experience a breach. Not only do companies need to develop and communicate the appropriate messaging when it comes to how they protect consumer data, but it's even more critical that they leverage technology and make sound decisions around enabling and building the required security structures.

Data collection: An ever-increasing corporate activity that creates ever-increasing consumer anxiety

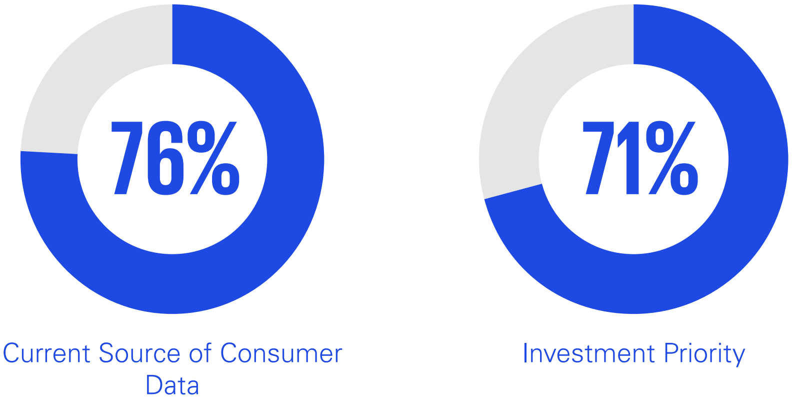
Customer data is fast becoming the currency of business and companies are collecting, using, and selling more and more of it

While U.S. consumers continue to share their data online, often against their better judgment, businesses on the receiving end are becoming consistently more invested in the process, and increasingly investing in, data collection.

Business leaders claim they’re focused on expanding the use of information that they collect by creating new and better products and services being the primary use case. However, we can also see more and more companies considering selling data to third parties. This year’s survey clearly indicates that companies are continuing to invest in consumer data collection and expand the use of this data. Indeed, nearly 80 percent of business leaders say their companies increased marketing and/or advertising technology spending during the pandemic, and nearly 90 percent expect that investment trend to further increase over the next five years.

The most common tactic through which companies collect data, cited by more than three-quarters of business leaders, is tracking consumer engagement. This includes email opens, counting clicks and conversions, calculating the time consumers spend on websites, watching their shopping behaviors and history, examining what’s in their carts, etc. It’s also the area in which more than two-thirds of business leaders expect to further invest going forward.

Consumer engagement is the top source of consumer data and is expected to see further investment



Current Source of Consumer Data

Investment Priority

Source: KPMG, 2022 Corporate Data Responsibility survey.

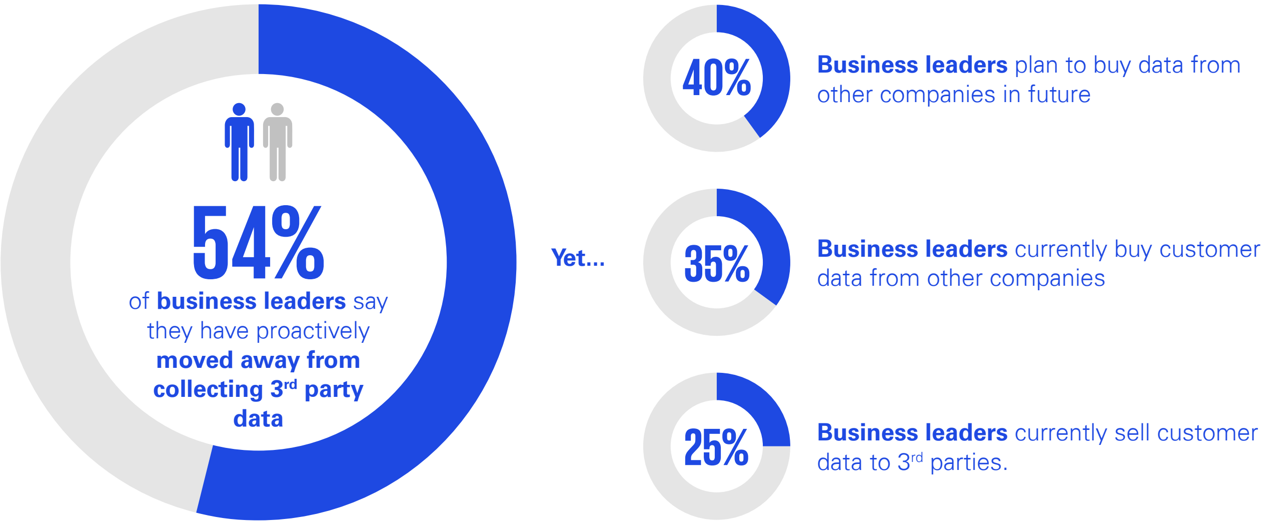
Some of the other data collection methods are less prevalent, but still about 60 percent of leaders say they collect customer data at the point of sale for service. Finally, a third of business leaders say that they do purchase data from other companies, and this leads us to some interesting insights. While improving products and services was the top use of consumer data in both 2021 and 2022, it also tops the list of uses that are decreasing in prominence compared to last year with a 10-point drop year-over-year from 84 percent to 74 percent.

Conversely, companies are exhibiting an increasing desire to monetize the customer data they collect by selling it to third parties. This sale of customer data to third parties has increased significantly, by 10 points, from 15 percent in 2021 to 25 percent in 2022.

In another interesting discrepancy, more than half of business leaders (54 percent) report that they are proactively moving away from collecting data from third parties. However, more than a third say they are actively buying data, and even more, 40 percent, plan to buy data in the future.

This is a somewhat contrary trend with a significant number of business leaders saying they are moving away from obtaining third-party data, while a smaller, albeit noteworthy cohort is still purchasing third-party data. Furthermore, a quarter of business leaders say they are also selling customer data to third parties.

Over half of business leaders are moving away from third-party data, but 40 percent still plan to buy data.



54% of **business leaders** say they have proactively **moved away from collecting 3rd party data**

Yet...

40% **Business leaders** plan to buy data from other companies in future

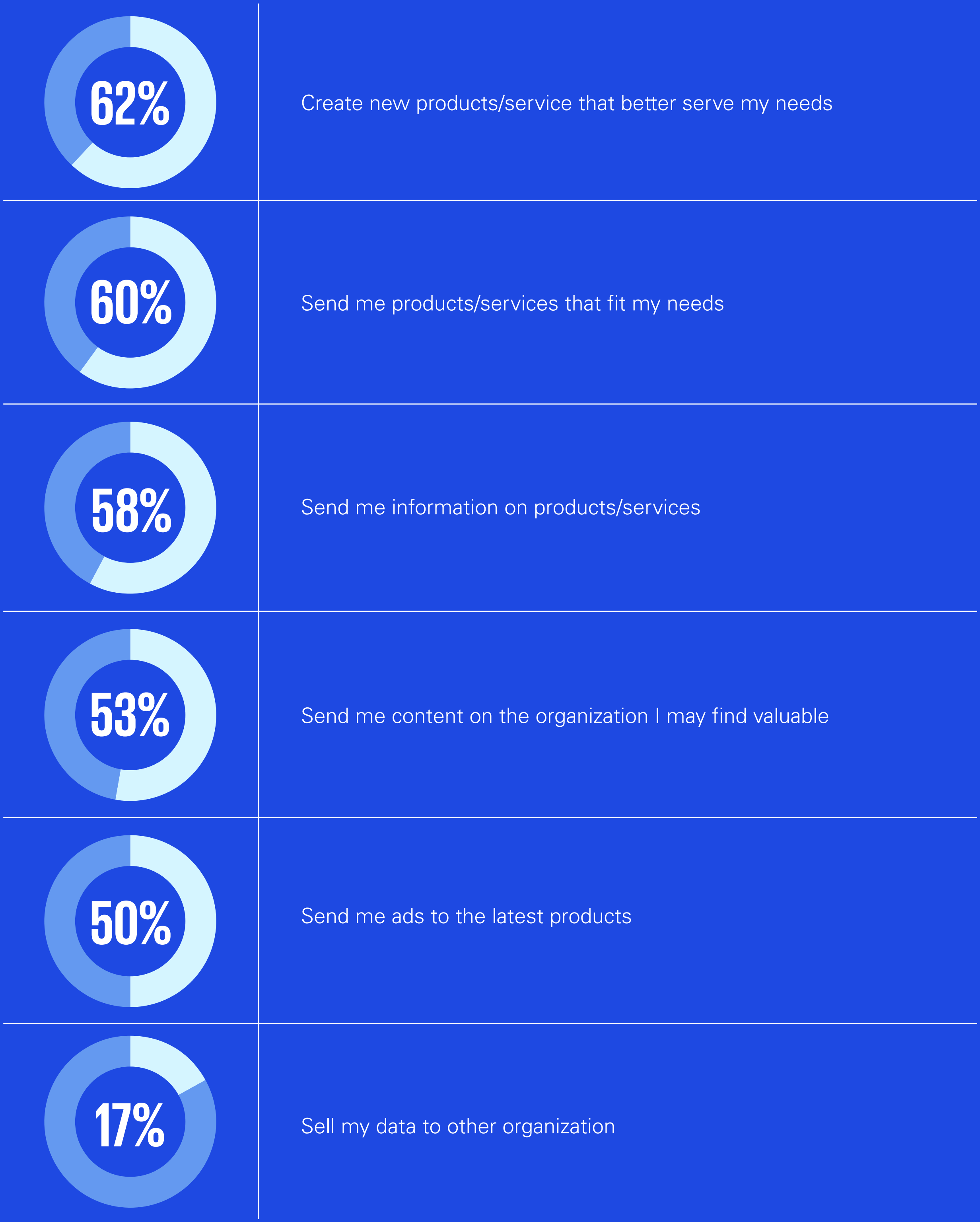
35% **Business leaders** currently buy customer data from other companies

25% **Business leaders** currently sell customer data to 3rd parties.

Source: KPMG, 2022 Corporate Data Responsibility survey.

When asked about acceptable company uses for their personal data, the least acceptable use, cited by only 17 percent of Americans, is selling their personal data. Not surprisingly, the most acceptable uses of data are those that benefit the consumer in some way. For example, approximately 60 percent of respondents say it's acceptable to use data in connection with products and services, and approximately 50 percent say it's acceptable to use data to send organizational content or ads.

Americans are OK with companies using data in ways that benefit them, but selling their data is not OK



Source: KPMG, 2022 Corporate Data Responsibility survey.

Bottom line: Implications and recommendations

Many companies continue to buy and sell consumer data despite this being consumers' greatest concern. Consumers simply do not want companies to sell their personal information. This practice can irreparably widen the consumer trust gap.

A wide array of Adtech and Martech strategies can be explored in this context. For example, personification isn't new, but it is gaining increased traction as a means of maintaining user privacy. Personified advertising leverages AI and machine learning to identify individual traits beyond the specific behavior a user may be demonstrating and communicates directly to a centralized server. Rather than leveraging a user's personal data directly, this solution can engage audiences at scale with targeted ads by creating persona-driven cohorts, such as demographic categories, age, interests, and educational background among others. This form of advertising can also leverage historical data to understand user habits, enabling companies to define millions of assets and create new relevant personas. Companies should be aware, though, of implications around AI usage with new and existing regulations, many of which are designed to propagate ethical AI practices.

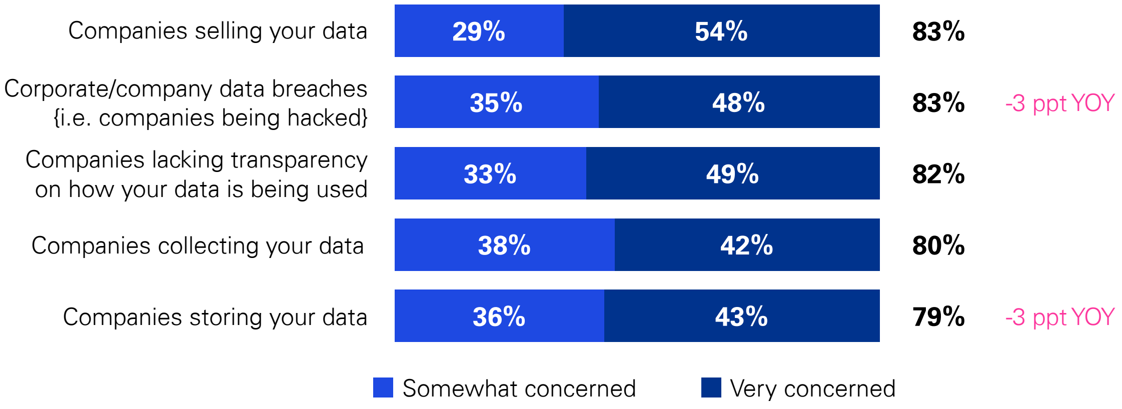
Consumers want transparency around collection and usage, but these are low priorities for businesses

Americans expect companies to be responsible for securing their data and will hold them to account if it is mishandled or compromised

Considering what's been revealed about attitudes toward data collection and usage from the standpoint of both the general U.S. population and business leaders, it makes sense that consumers have high expectations for how companies handle their data, and the precautions they take to protect it.

The vast majority of Americans, 83 percent, are worried about the ways in which companies handle their data, with the sale of data to third parties at the top of the list. More than half of that figure, 54 percent, consider selling data to third parties to be very concerning. Similarly, 83 percent of general population respondents are concerned about data breaches. While this is a huge number, it actually represents a three-point decline from 2021. Other concerns include a lack of transparency related to how data is being used (82 percent), and issues related to how companies collect (80 percent) and store data (79 percent), which is also three points less than in 2021.

A large majority of Americans worry about their data being sold, exposed, collected, and stored*

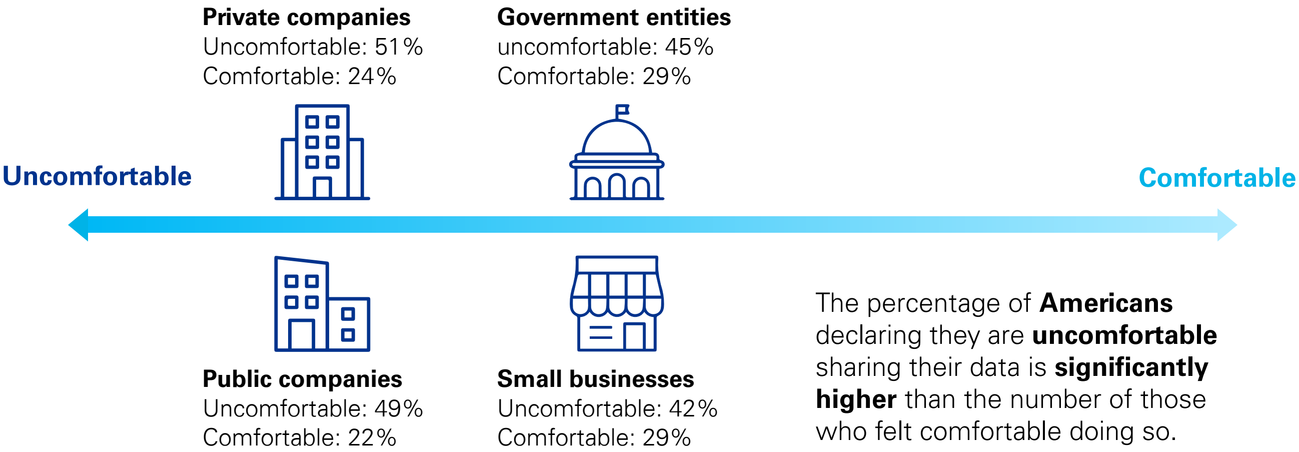


Source: KPMG, 2022 Corporate Data Responsibility survey.

Overall, Americans are equally uncomfortable—in fact, very uncomfortable—sharing personal data on a number of measures. The percentage of consumers who declare they're uncomfortable sharing their data is significantly higher than the number of those who feel comfortable doing so. The uneasiness is highest when it comes to sharing data with large privately held companies, whether they're private or public.

Looking across the spectrum, half of Americans have high levels of discomfort sharing data with large public and private companies. The attitudes warm up slightly in connection with government entities and small businesses, with approximately 44 percent of Americans uncomfortable sharing data with those organizations.

Americans are uncomfortable sharing personal data



Private companies
Uncomfortable: 51%
Comfortable: 24%

Government entities
uncomfortable: 45%
Comfortable: 29%

Uncomfortable

Comfortable

Public companies
Uncomfortable: 49%
Comfortable: 22%

Small businesses
Uncomfortable: 42%
Comfortable: 29%

The percentage of **Americans** declaring they are **uncomfortable** sharing their data is **significantly higher** than the number of those who felt comfortable doing so.

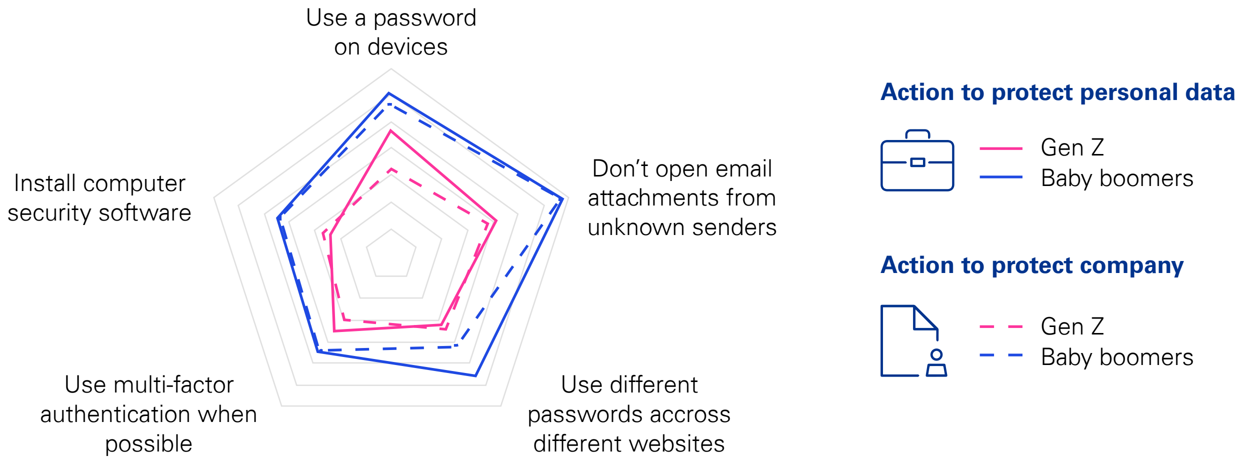
Source: KPMG, 2022 Corporate Data Responsibility survey.

And in terms of data breaches, Americans are very serious about companies being held responsible for mishaps with and mishandling of data. While 82 percent of Americans are concerned about company data breaches, 89 percent claim that companies should be held responsible for such events.

Another interesting point is the difference between how Americans view personal versus company data. In the radar chart below, the solid lines represent personal data and how respondents act to protect it, while the dashed lines indicate how they protect company data. Clearly, the behaviors around protecting company data are less prevalent than the ones related to personal data. This suggests that people exhibit more caution with their own data than with company data.

There are also generational differences: Younger generations, especially Gen Z, are less likely to engage in various data protection practices relative to baby boomers, who are much more conscious of and engaged in these types of behaviors.

Concerned about the potential exposure of personal and corporate data, Americans are taking action



Source: KPMG, 2022 Corporate Data Responsibility survey.

Bottom line: Implications and recommendations

Consumers want companies to take their data responsibilities seriously, put guidelines and policies in place, and share details about how they protect data. This view relates to the concern around transparency or the lack thereof. In short, 86 percent of Americans believe data privacy is a human right, meaning they believe they quite simply have the right to have their data properly, securely, and ethically managed.

All data incidents, large and small, should be communicated transparently and in a timely manner. Companies need to strengthen data security practices at their companies or risk a tarnished reputation.

There has to be a change in what companies are doing every day in regard to personal data versus what consumers want them to do. Business, information security, and marketing leaders—along with their Adtech and Martech partners—must work together to devise innovative ways to decrease the gap between company actions and consumer priorities, and communicate why those consumers should trust them.

What can companies do to address these concerns? The top three suggestions according to survey respondents are:

1. **Provide clear, timely reports on data breaches when cases occur (55 percent).** Further, it is imperative that companies ensure tight integration between information security incident response teams, and internal/external counsel to help ensure timely and appropriate notification of individuals impacted by a breach.
2. **Limit the use and sale of consumer data (53 percent).** Companies should actively practice data minimization and purpose use limitation principles, ensuring only data that is required to fulfill business purpose(s) is collected, data is used only for the purpose specified, and data is deleted when it is no longer required.
3. **Permit more consumer control over their personal data (52 percent).** Consent and preference-management solutions that are embedded into many leading privacy management platforms play a key role in fine-grained customer control and empowerment around their data.

Does management know what's going on in the data trenches?

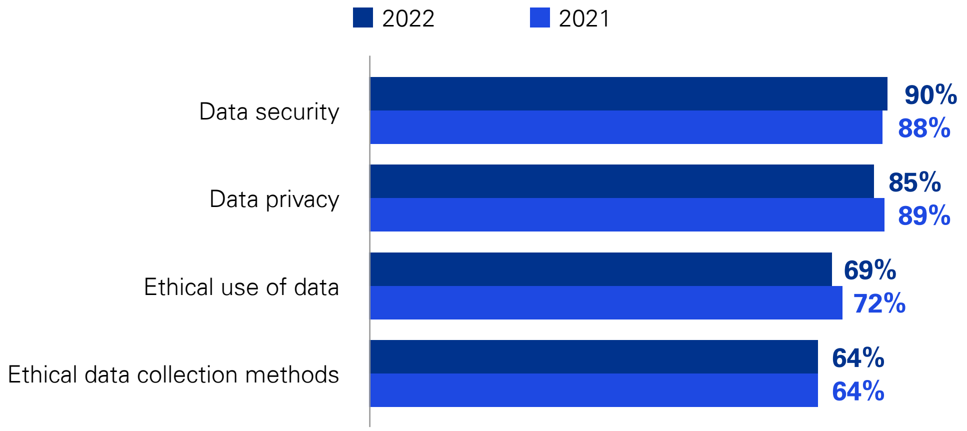
Businesses say security, privacy, and ethical collection and usage of data are priorities, but trust is low among American workers

There is a clear dichotomy between what we're hearing from business leaders and frontline American workers around their personal views on data responsibility and what they say is actually taking place on the ground at their organizations.

Looking at the differences in responses between director-level executives and the VP/C-suite levels, it appears that senior leadership has a more optimistic view of data security and privacy relative to middle management, which overall is somewhat more skeptical regarding their organizations' ability to address worker and consumer concerns. Much like we found in 2021, everyone is not on the same page.

Year over year, business leaders still say that security and privacy are top priorities, with security ticking up slightly and privacy down a little. These appear to be universal truths for companies in a data-driven business environment.

Data security and privacy remain top business priorities–well above ethical collection and usage



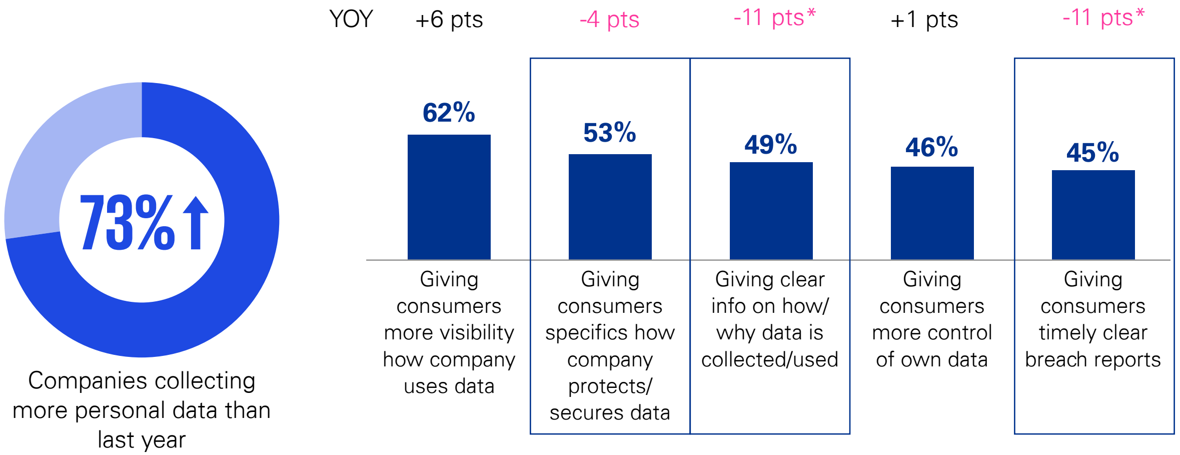
Source: KPMG, 2022 Corporate Data Responsibility survey.

Many companies across virtually every industry are feeling the pressure of being held legally liable for data breaches and failure to provide and properly act upon consumer choices such as opt out of sale of personal information. The business cost of maintaining data security and privacy is high at every level of the enterprise, from financial, productivity, and reputational perspectives. The upshot, however, is that while the concerns and the priorities around ensuring privacy and security are as strong as ever, their pursuit at some organizations may come—often inadvertently—at the expense of the ethical collection and use of consumer data and how they're collecting it as well.

Business leaders point to increased transparency in how they collect data year over year, and they're also very confident in their future plans for collecting and using customer data. It's encouraging that corporate decision makers feel that their data programs are on the right path, but workers aren't convinced. Indeed, those who say they trust their company to use data ethically fell from 63 percent in 2021 to 52 percent in 2022, while those who say they do not trust their company rose from 13 percent in 2021 to 23 percent in 2022—in fact, 20 percent of American workers say they don't trust corporate America at all. This underscores the need for strong data governance and management practices, such as data discovery across structured, unstructured and semi-structured data sources (internally and with third parties), and sustainable mapping and inventory practices. Indeed, privacy and data governance responsibilities are in many ways continuing to converge.

Companies are collecting more data than ever, but a number of data program measures that consumers value are faltering. Providing clear information on how and why they collect data, and timely responses and reporting on data breaches—perhaps the most important area for most consumers—have dropped considerably. Providing specifics on how they are protecting customer data has also declined. These are among the greatest concerns Americans have with how their data is managed; companies should prioritize the reversal of these trends.

Corporate data collection is up, but several critical data policy measures are down*

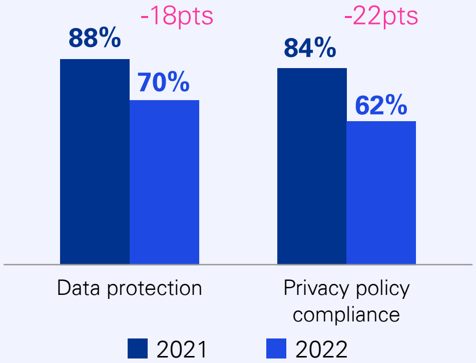


* Denotes significant difference from 2021

Source: KPMG, 2022 Corporate Data Responsibility survey.

Perhaps the most alarming corporate data responsibility development is in relation to training. Despite business leaders declaring that data security and privacy are their highest priorities, employee training around data protection and privacy policy compliance year over year is down 20 points on average. In fact, in this year's survey, one in five American workers said they have not completed any security/data trainings at their company. And unfortunately, often where training is completed, it is largely a "check-the-box" activity (and not focused on cultural transformation).

Data privacy/security training is also on the decline, potentially increasing risks*



Source: KPMG, 2022 Corporate Data Responsibility survey.

And...

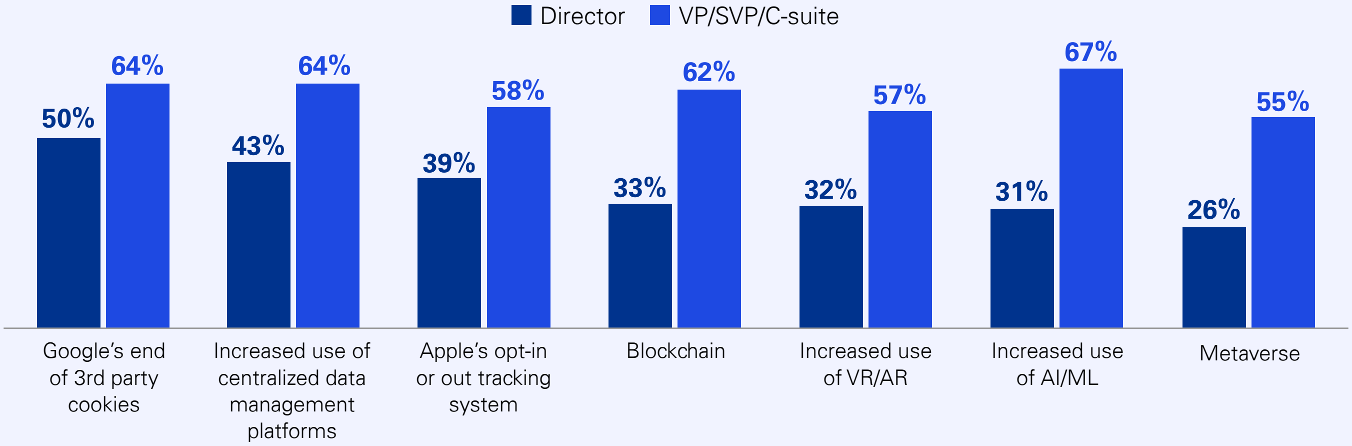
One in five **America Workers** report they **have not completed ANY** security/data training at their company

One might imagine, with concerns and potential liabilities rising in terms of data breaches, data security, and how data is actually being used, that training would be on the upswing. This cannot stand—with three-quarters of companies collecting more personal data than last year, insufficient training may contribute to an increase in data program risk. Clearly, many trainings are driven by broad regulatory initiatives, such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the U.S., and as companies become familiar with the relevant rules, some may feel the need for training diminishes. However, training, particularly in connection with data security and privacy, should not be a "one and done" endeavor. Training needs to be an ongoing effort considering the fluid nature of data responsibility and the ever-changing regulatory, governance, and technology environments.

Another noteworthy gap in the way frontline director-level executives and upper management view the data dynamic is their opinions regarding the present and the future. Today, all levels largely agree on the challenges they face, with 43 percent considering new data laws and regulations to be among their biggest challenges; 33 percent expressing similar concerns about the issue of poor data quality; and 30 percent worrying about the uncertainty created by heightened legal and regulatory risk.

The divergence is in the way frontline versus senior managers think about their organization's level of preparation for future technology changes, such as centralized data management platforms, blockchain, VR/AR and AI/ML, and the metaverse. And the disparities increase as the technologies get newer and more sophisticated. Not only are workers and consumers not on the same page with companies, in many cases executives within these firms are not aligned.

Despite agreement on current challenges, frontline and senior managers have widely divergent views on preparedness for future technology challenges



Source: KPMG, 2022 Corporate Data Responsibility survey.

Where do these contrary opinions come from? Is upper management trying to put a more positive spin on their companies' preparedness and capabilities around their data practices? Or, are they less informed about what's happening in the "data trenches?" What does "preparedness" mean to a middle manager versus a senior manager? A director would look at it from a more tactical and granular perspective. Do we have the right staff in place? Does the team have the right skill sets? A senior manager will take a more strategic approach. What can we do to take advantage of these new technologies? How are we going to leverage new solutions to improve our competitive posture?

While the good news is that middle and senior management overall agree on current challenges, their preparedness to tackle technology issues down the road diverges. Companies would do well to close these gaps by breaking down the silos between senior management and functional areas of the business. In a highly fluid, data-driven business environment, decision makers and workers need more opportunities to discuss what data security should look like across the organization going forward from financial, operational, and ethical perspectives.

Bottom line: Implications and recommendations

The data collection and usage practices many companies currently employ largely are not aligned with the current consumer priorities.

A number of Adtech and Martech companies have solutions that enable companies to track user activities across web pages and platforms by supplying deterministic identifiers, such as emails and phone numbers, which mitigates the risk of exposure or leaks.

Specifically, these companies are establishing consortiums through which users can verify or view the contents of web pages free of charge without providing personal information. These solutions benefit both businesses and consumers as they deliver improved engagement with transparent and secure data sharing.

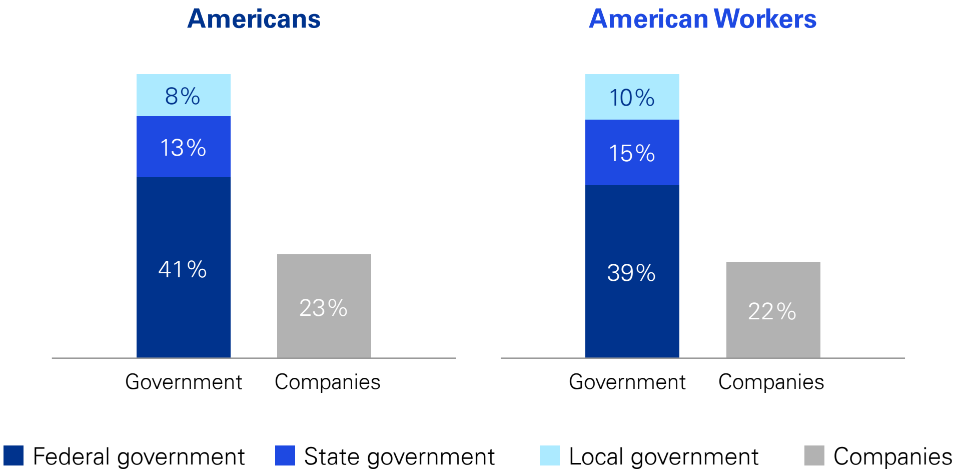
Security and privacy policies can be a competitive differentiator. It should not just be an exercise in regulatory compliance, but simply good business.

Government should set the standards, but companies must take active responsibility for data policies

New technologies are leading American consumers and workers to call for more regulation of data collection and usage

The majority of Americans believe local, state, or federal government—not corporate America—should establish rules and regulations for data security and privacy as it relates to new technologies. In short, there's a desire for uniformity and structure around how data is managed. As we've learned, Americans largely don't trust large corporations right now, but they acknowledge the need to establish the guardrails to help ensure that their data is secure and their privacy is respected, particularly with the proliferation of technologies such as AI, blockchain, and quantum computing.

Americans believe government is most capable of establishing data-related rules in connection with new and emerging technologies



Source: KPMG, 2022 Corporate Data Responsibility survey.

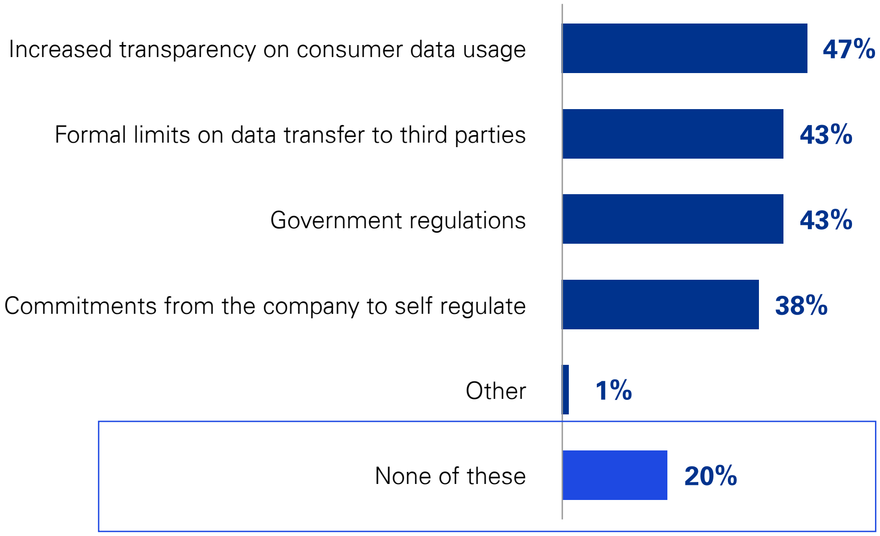
All respondents want more rules, more protections, a clear framework, and guidance that ensures all involved are on the same page. Simply put, it appears American consumers don't want companies policing themselves when it comes to their personal data. Of course, the challenge here is the time it may take for government at any level—federal, state, or local—to achieve consensus, gain approval, and put a plan in place.

In the interim, 87 percent of Americans agree that corporate America should take the lead in establishing corporate data responsibility plans as a way to fill the gap until clear government regulations are released. Not surprisingly, nearly all baby boomers (95 percent)—the generation most concerned about protecting personal data—also want companies to take greater responsibility. Even three-quarters of Gen Z, who are fairly relaxed compared to other generations when it comes to their personal data security, believe companies need to step up.

Finally, the survey also tells us that transparency can help allay American's concerns over how their data is being used and protected. The more Americans understand the process, the more transparent it feels, the more they believe that a company is being honest and open, the more cooperative they're likely to be. If they believe companies are trying to hide something, not only will they not share data, but they may turn their backs on those companies' products and services.

Whether it's on the metaverse or on augmented or virtual reality platforms, the more transparent corporate America can be about how they're managing data, the more they're likely to engender trust on the part of the American population.

Americans believe government—not corporations—should establish data-related rules in connection with new and emerging technologies



Source: KPMG, 2022 Corporate Data Responsibility survey.

In the end, companies can't go wrong being as fully transparent as possible without, of course, putting sensitive or proprietary information at risk. Transparency can only improve the trust Americans have in the companies with which they do business and may inspire consumers to continue to share their data with confidence.

Bottom line: Implications and recommendations

The takeaway is that companies must prioritize data privacy and security technology or risk falling behind the competition.

One strategy many companies are encouraged to explore with their Adtech and Martech partners is contextual targeting. This AI-powered solution enables companies to promote their products and services without having to open up access to their user database. The solution restricts data extraction without prior user consent, which not only builds trust, but also enables Adtechs to maintain regulatory compliance.

Contextual targeting doesn't just rely on matching keywords or categories to an ad, it leverages AI to analyze the context of the page and serve up the ads that are most relevant to the user. As a result, advertisers and marketers can reduce their dependency on search engines because contextual targeting doesn't rely on tracking third-party cookies.

Conclusion: Make data policy a competitive differentiator

There is no question that companies are going to continue collecting and using data to inform product development, marketing strategies, and customer experience. It is also clear, however, that they need to do it in a manner that consumers trust and that demonstrates the benefit: increased product choices, better pricing, personalized experiences, etc.

Companies must view their data collection processes not only through a regulatory compliance lens, but as a means for building business. An opportunity exists for companies to utilize their data privacy and data security protocols as a competitive differentiator and to build—and maintain— consumer trust.

This entails ensuring the various complementary, data-oriented roles align priorities. As Harvard Business Review writes, "Most large firms already suffer from a series of internal tensions over customer data."[1] Indeed, firms that collect consumer data are encouraged to actively acknowledge that data privacy and security issues are not just the responsibility of the CISO. They also need to be on the Chief Marketing Officer's radar.

Data policy is not solely about doing the things organizations have to do because they're being regulated or because other companies are doing it. Collectively, these processes can and should be a pillar of a firm's overarching operating model and, ultimately, a business enabler.

[1] Harvard Business Review, The New Rules of Data Privacy, February 25, 2022.

How KPMG can help

According to this year's survey, approximately 9 in 10 Americans are concerned about protecting their personal data. The same number wants companies to take their data responsibility seriously.

Eighty-six percent believe data privacy is a human right. Companies that collect consumer data should take note of these numbers.

To remain viable and competitive, organizations must build trust with their customers when it comes to data privacy and protection. To achieve this, they need to be transparent about how they're using customers' information to instill confidence in their data protection technology and data-handling practices.

Moreover, organizations that don't have full visibility into their data—where it is, how it's being used, who's using it, and for what purpose—risk not being able to protect it. This, in turn, damages customer trust. Most firms already possess the building blocks for achieving data visibility, but these resources are spread across their privacy, security, and information governance areas. These disparate efforts do not give a clear picture of the organization's data overall.

At KPMG, our data privacy specialists work with our clients to pull together data from different parts of the organization. We team with you to implement an integrated technology model that helps achieve visibility as well as data protection and trust.

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. Preconfigured 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.

Methodology

About the survey

There were two separate surveys, one covering a nationally representative audience of 2,008 U.S. adults, ages 18 and up, including a subset of 992 classified as "American workers," and one covering 255 business leaders, director level (or higher), with involvement in security/privacy/data decisions at companies with more than 1,000 employees. Total respondents for the two surveys combined was 2,263. The margin of error at the 95 percent confidence level is 2.19 percentage points for the U.S. general population and 3.11 percentage points for American workers. For the business leaders, the margin of error at the 95 percent confidence level is 6.14 percentage points. Both surveys were fielded from May 5, 2022, to May 17, 2022.

*Where denoted, the YoY findings indicate questions asked in prior years.

Contact us

Orson Lucas
Principal, Advisory
U.S. Privacy Services Leader
T: 813-301-2025
E: olucas@kpmg.com

Bret Sanford-Chung
Managing Director
U.S. Marketing Consulting
T: 212-758-9700
E: bsanfordchung@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

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.