CISCO
SECURE

CISCO
The bridge to possible

Data Transparency's Essential Role in Building Customer Trust

CISCO 2022 CONSUMER PRIVACY SURVEY

Table of Contents

© 2022 Cisco and/or its affiliates. All rights reserved.

Introduction

Even with privacy laws enacted in more than 130 countries around the world, consumers are not confident that their personal data is safe. While the laws and regulations provide helpful oversight, consumers still want organizations to be more transparent about how their personal data is being used. In addition, evolving and innovative technologies are making it even harder for consumers to trust the companies with whom they share their data. In response to these challenges, many consumers are taking action to better protect themselves and their data.

This report, our fourth annual review of consumer privacy, explores current trends, challenges, and opportunities in privacy for consumers. It draws upon data gathered in June 2022 from a double-blind survey where the respondents did not know who was conducting the study and individual respondents were similarly unknown to the researchers. Respondents included 2600 adults (18 years and older) in 12 countries (5 Europe, 4 Asia Pacific, and 3 Americas).[1]

Participants were asked about their attitudes and activities regarding companies' use of personal data, and awareness and reaction to privacy legislation, artificial intelligence (AI), and data localization requirements. The findings from this research demonstrate the growing importance of consumer privacy and highlight what this means for the businesses and governments that serve them.

Key highlights:

1. Transparency is an essential element of trust, and consumers rank transparency as the most important thing organizations can do to build and grow trust when it comes to dealing with their personal data.
2. Consumers are taking action to protect their personal privacy and data, including changing providers, inquiring about the data organizations have about them, and regularly turning off home listening devices.
3. Consumers are very concerned about the use of their personal information in AI applications, but organizations that apply and use AI can still take steps to earn and build their trust.
4. Privacy laws continue to be viewed very positively by consumers around the world, but awareness of these laws and the protections they afford remain low.
5. Consumers are split on the value of data localization requirements with many indicating that local data storage may not be worth the added costs.

[1] Australia, Brazil, China, France, Germany, Italy, India, Japan, Mexico, Spain, the United Kingdom, and the United States

© 2022 Cisco and/or its affiliates. All rights reserved.

Results

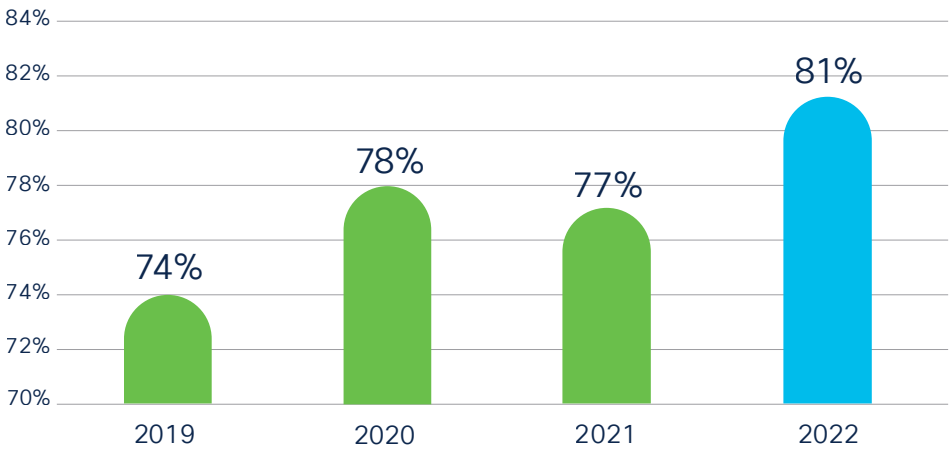
Section 1: Transparency's role in consumer trust and confidence

Consumers often need to provide their personal data to organizations to access goods and services. Consumers look to these organizations to be truthful and transparent about their data practices and expect the organizations to treat their personal data responsibly—all essential elements of trust. In this year's survey, 76 percent of respondents said they would not buy from a company who they do not trust with their data. In addition, 81% of respondents agreed that the way an organization treats personal data is indicative of how it views and respects its customers. This year's percentage is the highest since we began tracking it in 2019. See Figure 1.

Figure 1: Treating Personal Data Properly

"I believe the way a company treats my personal data is indicative of the way it views me as a customer."

Percentage of respondents who agree



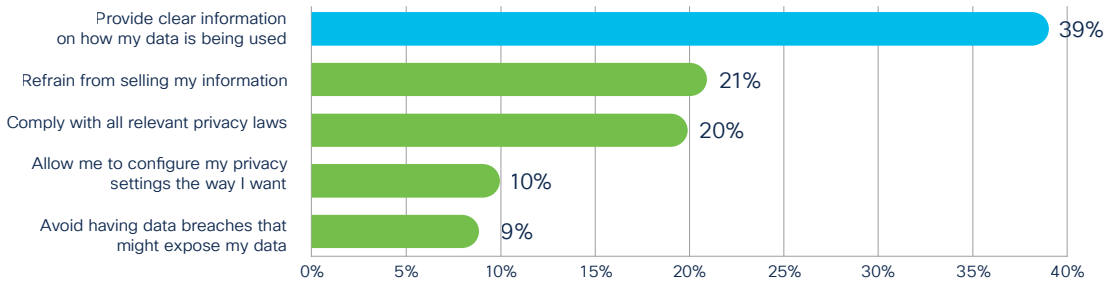
Source: Cisco 2022 Consumer Privacy Survey

© 2022 Cisco and/or its affiliates. All rights reserved.

Organizations can perform a variety of activities to fulfill this expectation and earn and build customer trust. These include complying with all applicable privacy laws and regulations, refraining from selling the customer's personal information, avoiding data breaches that might expose personal data, allowing the customer to configure his or her privacy settings, and providing clear information on how the customer's personal data is being used. When asked to rank these activities in order of importance for building trust with customers, 39% of respondents selected having "clear information on how data is used" (i.e., transparency) as their top priority. This was nearly twice as many as the next most popular options. See Figure 2.

Figure 2: Consumer Priorities for Organizations

Most important activity organizations can do to build trust with customers, regarding their data



Source: Cisco 2022 Consumer Privacy Survey

"Organizations need to explain their data practices in simple terms and make them readily available so that customers and users can understand what is going on with their data. It is not just legally required; trust depends on it."

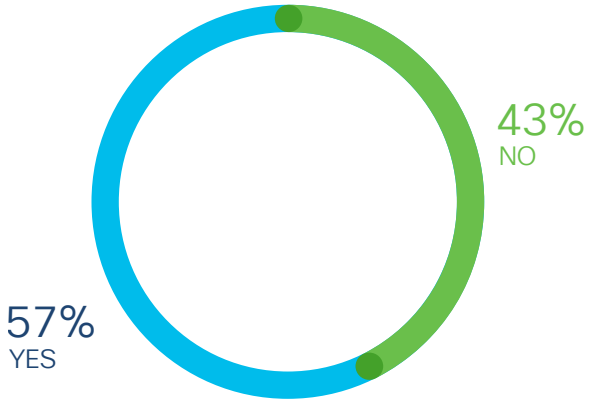
– Harvey Jang, Cisco Vice President, Deputy General Counsel and Chief Privacy Officer

© 2022 Cisco and/or its affiliates. All rights reserved.

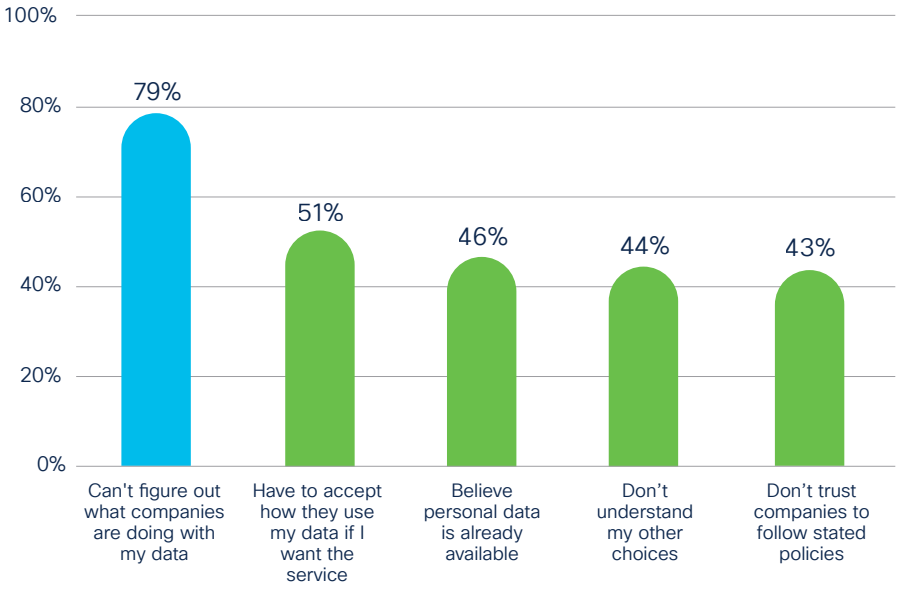
Despite it being a top priority, many consumers today believe they are not getting enough transparency from organizations with whom they share their data. Forty-three percent of respondents said they are unable to protect their data effectively. The main reason–cited by 79%–is that it's too hard for them to know and understand how companies are using their data. See Figure 3.

Figure 3: Ability of Consumers to Protect Their Data

Are you able to effectively protect your personal data?



Reasons why not?



Source: Cisco 2022 Consumer Privacy Survey

© 2022 Cisco and/or its affiliates. All rights reserved.

Section 2: Actions consumers take to protect their privacy

During the past four years, we have been tracking a segment of consumers called "Privacy Actives"—those who say they care about privacy, are willing to act to protect it, and most importantly, have already acted by switching companies or providers to better protect their privacy. Among this year's respondents, we found that 32% qualified as Privacy Actives (same result as in last year's survey and up from 29% two years ago). See Figure 4.

Figure 4: The "Privacy Actives" Segment

I care	And I'm willing to act	And I've acted	Privacy Actives
I care about data privacy I care about protecting others I want more control	I am willing to spend time and money to protect data This is a buying factor for me I expect to pay more	I have switched companies or providers over their data policies or data sharing practices	

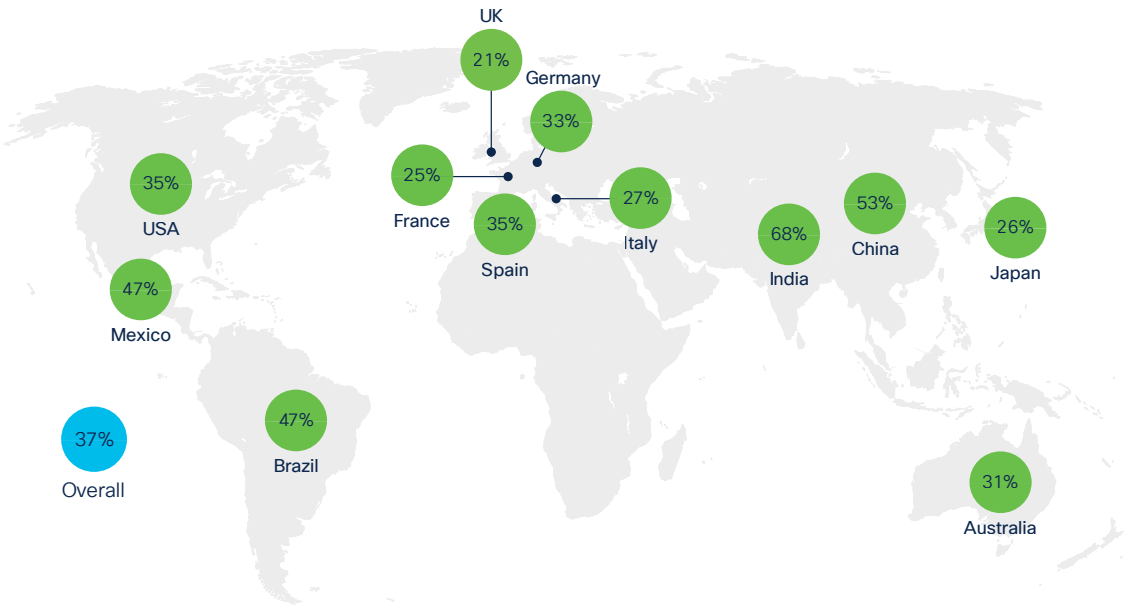
Note: The 82% and 44% are based on the relevant subset, not necessarily the overall respondent pool

Source: Cisco 2022 Consumer Privacy Survey

© 2022 Cisco and/or its affiliates. All rights reserved.

Overall, 37% of respondents in this year's survey indicated they had indeed switched providers (similar to last year and up from 34% two years ago). By country, interestingly, the lowest percentages of those who switched are from Europe, including the UK (21%), France (25%), and Italy (27%). Surprisingly, India (68%) and China (53%) had the highest percentage of respondents in nations that changed providers. See Figure 5.

Figure 5: Percentage of Consumers Who Have Switched Companies/Providers



Source: Cisco 2022 Consumer Privacy Survey

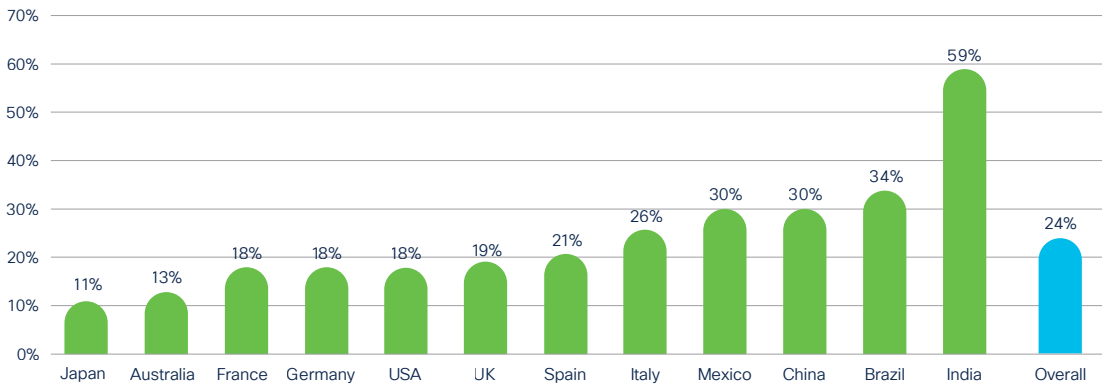
© 2022 Cisco and/or its affiliates. All rights reserved.

Perhaps strong privacy laws—like the European Union's (EU) General Data Protection Regulation (GDPR)—drive a more consistent level of protection from organizations operating in Europe, so switching providers isn't useful or helpful to improve privacy. Since India has yet to pass an omnibus privacy legislation, consumers are left to fend for themselves and protect their privacy by more carefully selecting the organizations they engage with and are more willing to switch when unsatisfied with how organizations protect their data.

Another way that consumers can act to protect their data is by inquiring about the data companies have about them and potentially getting the data corrected or deleted. Many privacy laws have a framework for data subject access requests (DSARs), granting individual rights of access and control over their own data. Among all survey respondents, 24% said they have made a data inquiry of at least one provider, and 14% of all respondents said they have also requested some of their data be changed or deleted.

These laws vary by country, and it is interesting to note that India (59%) had the largest percentage of respondents who had made inquiries into their data, followed by Brazil (34%), China (30%), and Mexico (30%). The GDPR countries, on the other hand, had relatively lower percentages of respondents making DSAR inquiries. See Figure 6.

Figure 6: Percentage of Consumers Exercising Data Subject Access Rights (DSAR)

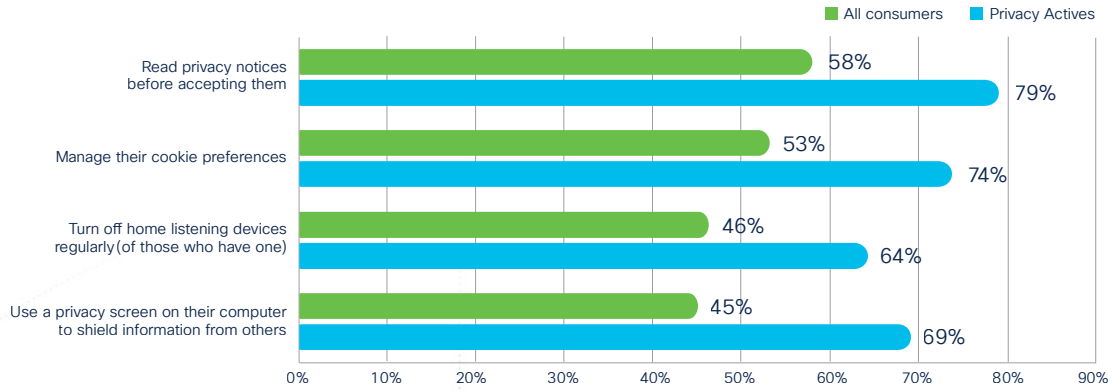


Source: Cisco 2022 Consumer Privacy Survey

© 2022 Cisco and/or its affiliates. All rights reserved.

We also asked respondents about other actions they take to help protect their data. Fifty-eight percent of respondents say they read privacy notices before accepting them, and 53% say they manage their cookie settings before accepting all cookies from a website. Forty-six percent of those with a home listening device say they turn it off regularly to protect their privacy. Forty-five percent use a privacy screen on their computer to help shield information from others. Not surprisingly, in all these categories, the percentage of "Privacy Actives" who do these activities is much higher than in the general population. See Figure 7.

Figure 7: Consumer Privacy Behaviors



Source: Cisco 2022 Consumer Privacy Survey

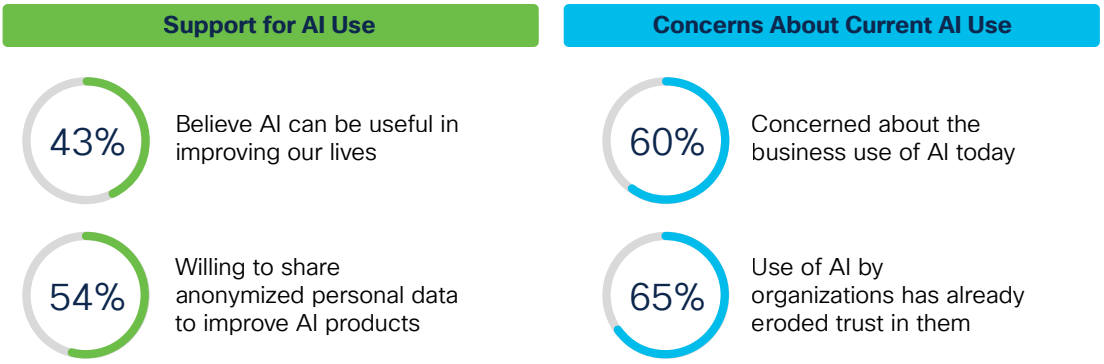
© 2022 Cisco and/or its affiliates. All rights reserved.

Section 3: Artificial Intelligence and automated decision-making using personal data

Artificial Intelligence has the potential to use customer data in ways that create more efficient and personalized experiences for consumers. Forty-three percent of survey respondents (up from 40% last year) recognize that AI can be useful in improving their lives—from shopping to streaming services to healthcare. Interestingly, in a new question in this year's survey, the majority of respondents (54%) said they are even willing to share their anonymized personal data to help improve AI products and decision-making. They believe that the potential benefits outweigh the risk, assuming proper anonymization and de-identification techniques are employed.

Some AI applications use personal data for automated decision-making, and the vast majority of organizations (92%[2]) as well as consumers (77%) agree that organizations must act responsibly in this area. However, there is a disconnect on how well this is working today. Eighty-seven percent of organizations[3] believe they already have processes in place to ensure automated decision-making is done in accordance with customer expectations. Nonetheless, 60% of consumers in our survey expressed concern about how organizations are using their personal data for AI today, with 65% saying that they have already lost some trust in organizations as a result of their AI use. See Figure 8.

Figure 8: Support and Concerns About the Use of Personal Data in AI



Source: Cisco 2022 Consumer Privacy Survey

[2,3] Cisco 2022 Data Privacy Benchmark Study

© 2022 Cisco and/or its affiliates. All rights reserved.

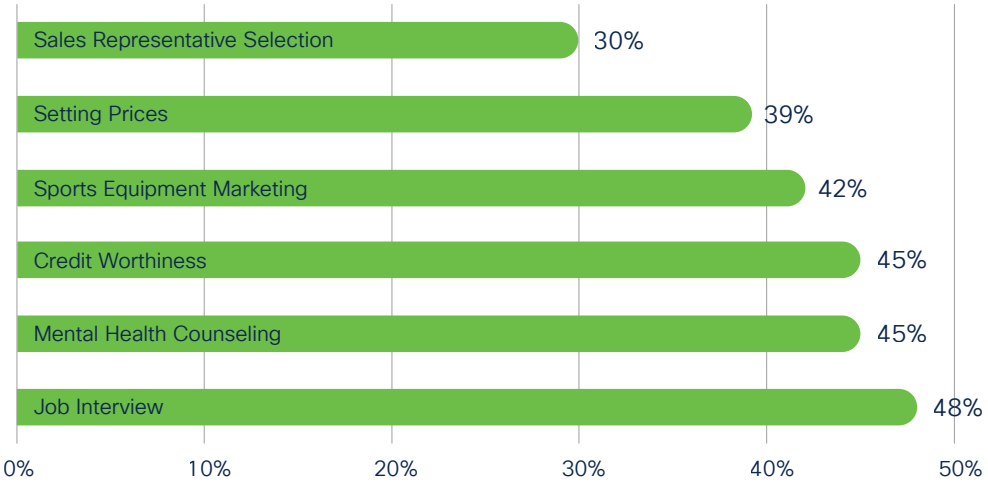
To explore further this potential loss of trust, we tested six common AI business applications, including matching the consumer with a sales representative, determining credit worthiness, setting prices, and qualifying for a job interview. As expected, consumers had the most concern with the most sensitive applications. Yet, in all of the applications tested, 30% or more of respondents indicated they would trust a company less that uses AI for automated decision-making in these areas. For example, 48% said they would trust a company less that used AI to determine who qualified for a job interview. And 30% said they would trust a company less that used AI to automatically select a sales representative. See Figure 9.

Figure 9: AI Use Cases and Loss of Trust

Use cases tested to

- Better match a sales representative to you when you call or visit their store
- Set the prices for their products and services
- Infer whether you participate in sports and market sports equipment to you
- Infer your credit-worthiness and decide whether to grant you a loan
- Infer your mental health status and recommend counseling services to you
- Infer your work ethic and decide whether to select you for a job interview

Percentage who would trust a company less who made these decisions using AI



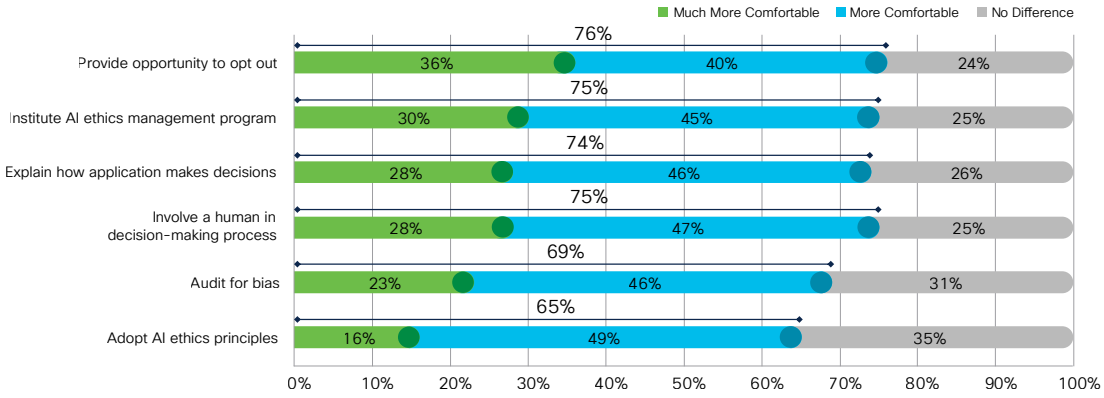
Source: Cisco 2022 Consumer Privacy Survey

© 2022 Cisco and/or its affiliates. All rights reserved.

These results suggest that any AI applications that affect individuals directly may be problematic for organizations trying to earn and build customer trust (and human involvement is legally required in some jurisdictions when the AI is making a legal or significant impact).

Fortunately, there are steps organizations can take to reduce reticence and the potential negative impact their AI applications have on customer trust. These include adopting Responsible AI principles, instituting a Responsible AI methodology and governance framework, auditing their AI use for unintended bias, involving a human in the decision-making process, and explaining at a high level how their AI application works (i.e., what factors are considered and how decisions are automatically made), or giving consumers the opportunity to opt-out. Roughly two-thirds of respondents (65% to 76% range) said each of these steps would help make them more comfortable with an organization's AI applications and use. Not surprisingly, the most powerful step is to give consumers choice and the opportunity to opt-out of the AI application altogether—76% said that would make them more comfortable. See Figure 10.

Figure 10: Impact of Approaches To Make Consumers More Comfortable, Given Use of AI Applications



Source: Cisco 2022 Consumer Privacy Survey

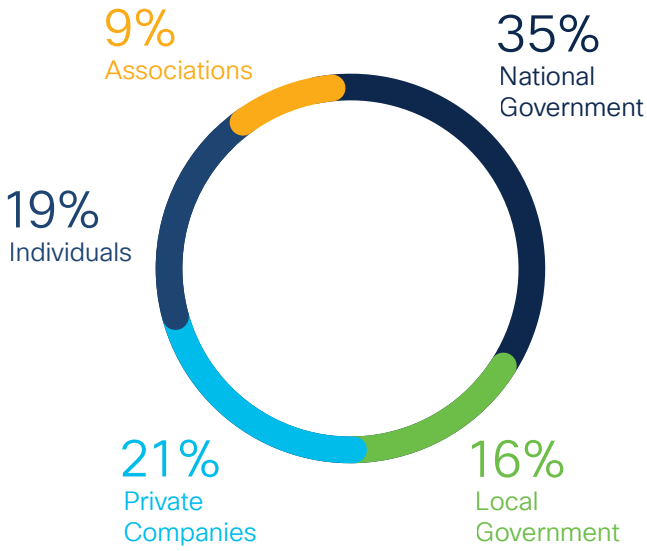
© 2022 Cisco and/or its affiliates. All rights reserved.

Section 4: Privacy laws and government's role in protecting data

Survey respondents were asked whether governments, organizations, or individuals should have a primary role in protecting personal data. More than half (51%) said national or local government should play the primary role, 21% said private companies should play this lead role, and 19% said the individuals themselves should be primarily responsible for protecting their own data. See Figure 11.

Figure 11: Privacy Roles

Who should have the primary role for protecting personal data?



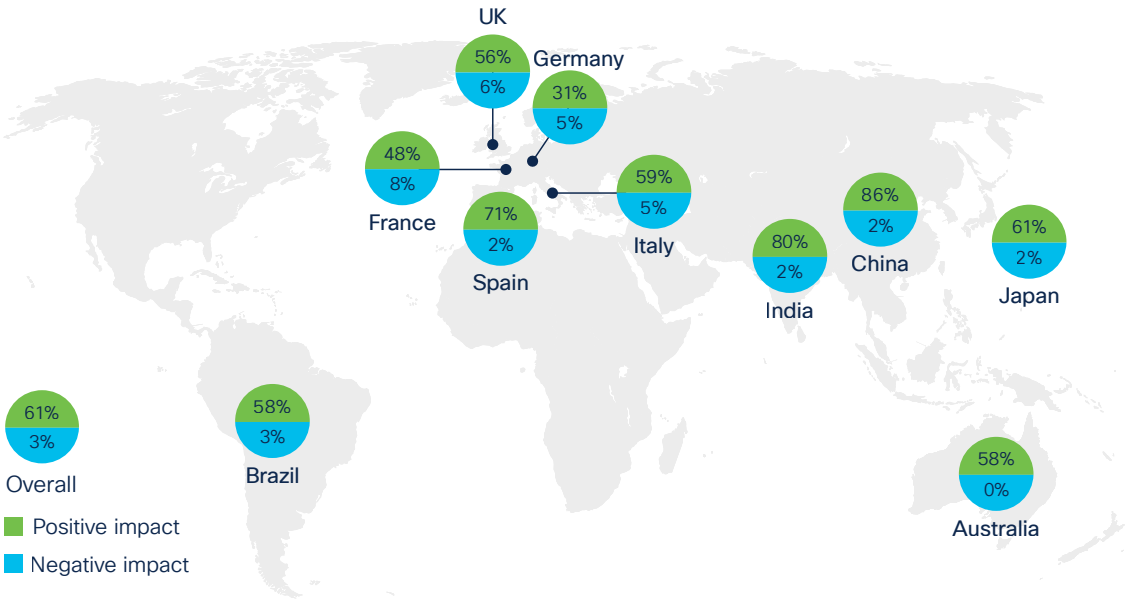
Source: Cisco 2022 Consumer Privacy Survey

Many consumers don't trust private companies to be responsible with personal data on their own accord. They look to the government to set the standard of care and enforce consumers' right to privacy. While consumers may accept responsibility for their data, given the lack of transparency, inability to exercise choice and control, and evolving technologies making things even more difficult, it is challenging for individual consumers to protect themselves. They believe they have limited power.

© 2022 Cisco and/or its affiliates. All rights reserved.

Given the desire for a strong regulatory role in protecting personal data, it is not surprising that consumers view their country's privacy laws and regulations very favorably. In this year's survey, we tested reactions to the GDPR among EU respondents, as well as several specific privacy laws in other countries, such as the Privacy Act 1988 (PA) in Australia, Personal Information Protection Law (PIPL) in China, Lei Geral de Proteção de Dados Pessoais (LGPD) in Brazil, Personal Information Protection Act (PIPA) in Japan, and the not-yet-adopted Personal Data Protection Bill (PDPB) in India. Among respondents in these countries who were aware of their country's laws, 61% felt the laws have had a positive impact, up from 60% last year and 53% two years ago. Only 3% felt they have had a negative impact, down from 4% last year and 6% two years ago. All of the individual countries had strong positive responses, with China (86% positive, 2% negative) and India (80% positive, 2% negative) the most strongly in favor. Remarkably, no country had more than 8% of respondents believing that their laws have had a negative reaction. See Figure 12.

Figure 12: Strong Support for National Privacy Laws

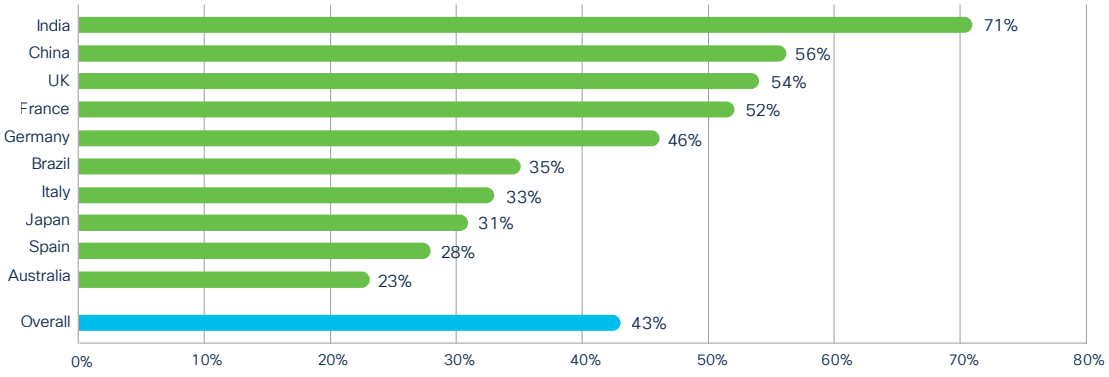


Source: Cisco 2022 Consumer Privacy Survey

© 2022 Cisco and/or its affiliates. All rights reserved.

While there has been growth in other areas, public awareness of these laws continues to be relatively low. Overall, only 43% of respondents (same as last year) in the countries with national privacy laws were aware of their country's laws. The GDPR has been enforceable for more than three years and awareness ranges only from 28% in Spain to 54% in the UK. One notable exception is in India, where 71% of respondents are aware of the draft PDPB Bill, which has been frequently in the news, but adoption continues to be delayed. See Figure 13.

Figure 13: Awareness of National Privacy Laws



Source: Cisco 2022 Consumer Privacy Survey

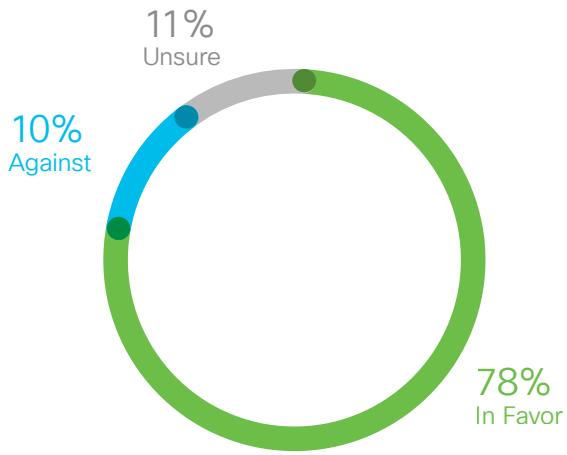
© 2022 Cisco and/or its affiliates. All rights reserved.

Section 5: Consumer views on the value of localization

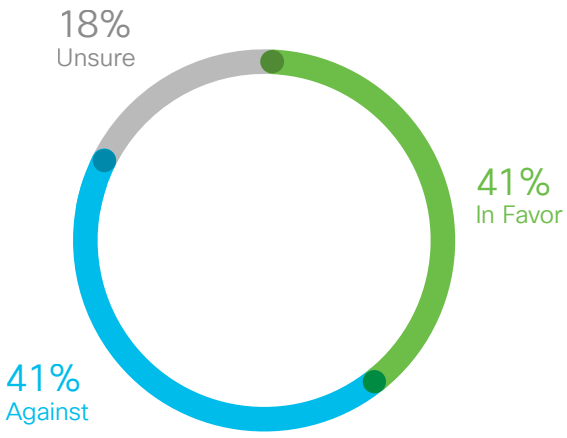
As governments and organizations continue to demand protections on data transferred outside their national borders, more are putting in place data localization requirements, that is, requiring data to be physically stored in the country where it was collected. Most consumers have heard about these requirements, and 78% of respondents indicated initially they thought data localization might be a good idea to help ensure their own country's laws and standard of care are applied to personal data. However, when respondents were asked the same question under the assumption that localization would make the products and services they buy more expensive, they were far less supportive, with only 41% in favor of localization. See Figure 14.

Figure 14: Data Localization

Support for data localization



Support for data localization, if it adds to cost



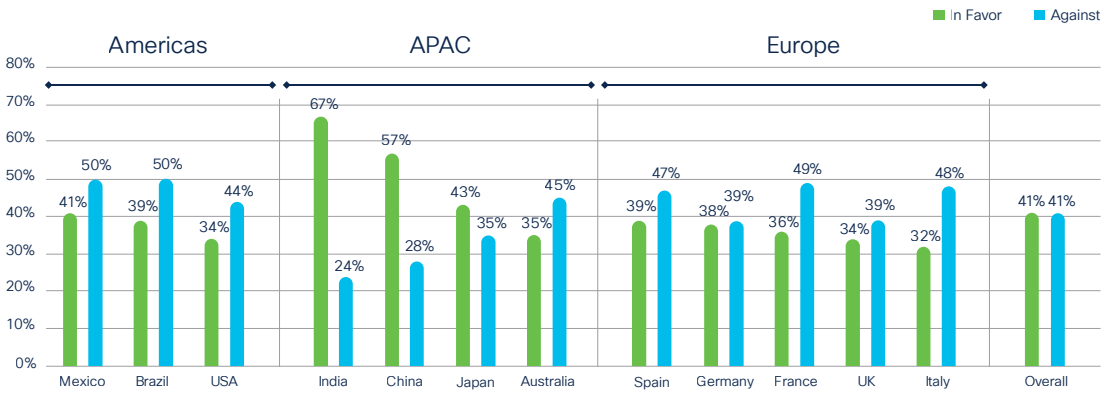
Source: Cisco 2022 Consumer Privacy Survey

© 2022 Cisco and/or its affiliates. All rights reserved.

Of course, data localization does add cost. The Cisco 2022 Data Privacy Benchmark Study reported that 88% of surveyed organizations were experiencing significant additional operational costs due to data localization requirements. Organizations may be forced to select less sophisticated or capable local, in-country providers and partners; unable to rapidly deploy new features, functionality, or security updates to disparate, local instances of applications; and resource constrained to deliver redundant services and capabilities in multiple geographies.

Focusing on the country results, it turns out that more respondents were against costly data localization in 9 of the 12 countries, including all of those surveyed in Europe and the Americas. For example, Italy's respondents were 48% against (32% in favor), France's were 49% against (36% in favor) and the US's were 44% against (34% in favor). The only 3 countries with more respondents in favor were India's 67% (24% against), China's 57% (28% against), and Japan's 43% (35% against). See Figure 15.

Figure 15: Support for Data Localization if it Adds Cost, by Country



Source: Cisco 2022 Consumer Privacy Survey

It will be interesting to better understand consumers' views on the various tradeoffs involved with data localization beyond cost–for example, quality, security, and agility–and we will plan to explore this in future research.

© 2022 Cisco and/or its affiliates. All rights reserved.

Conclusion: Recommendations for organizations and individuals

Protecting personal data requires governments, organizations, and consumers to each play an active role. The findings in this research point to these specific recommendations for organizations to help improve data privacy and consumer confidence:

1. **Invest in transparency.** Being open and transparent about how your organization manages data is not just a compliance exercise—transparency is key to earning and building consumer trust.
2. **Increase awareness of privacy laws and rights among individuals.** This can help everyone understand their rights and the protections available to them, as well as build confidence that their data is protected since the laws provide oversight for how organizations handle personal data.
3. **Adopt measures to ensure responsible use of data.** Designing, building, and implementing with a governance framework centered on respecting privacy; providing transparency on AI implementation, use, impact, and consequences; and providing consumers with a choice when the potential impact is significant are all positive steps organizations can take to engender consumer confidence.
4. **Consider the costs and legal alternatives, if any, to data localization requirements.** Data localization may not be worth its cost to many consumers, and it is still unclear if these regulations contribute to greater safety and protection of privacy, or if they serve other purposes, such as data sovereignty, national security, public interest, preventing foreign interference/access, or economic protectionism.

Cisco published its New Trust Standard as an industry benchmark for businesses to grow confidence and develop trusted digital relationships with their customers. This framework raises the bar for earning and building trust as work becomes more hybrid, more data is collected online, and cyber threats increase. To promote transparency, Cisco publishes Privacy Data Sheets and Privacy Data Maps for major products and services, enabling anyone interested to understand what data is used, why, who has access to it, and where it's stored. In future research, we will continue to explore how shifting consumer sentiment, evolving technology, and data regulations will impact privacy over time.

For additional information about Cisco's privacy research, contact Robert Waitman, Cisco Privacy Director, at rwaitman@cisco.com.

Over the past decade, Cisco has published a wealth of security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their effects on organizations, as well as best practices to defend against the adverse impacts of data breaches. In our new approach to thought leadership, Cisco Security is publishing a series of research-based, data-driven studies. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise from threat researchers and innovators in the security industry, the reports in each year's series include the Data Privacy Benchmark Study, the Security Outcomes Study, the Threat Report, and Prioritization to Prediction, with others published throughout the year. For more information, and to access all the reports, visit www.cisco.com/go/securityreports.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. PROJ 2062922 10/22