Generation Privacy:

Young Consumers Leading the Way

CISCO 2023 CONSUMER PRIVACY SURVEY

Table of Contents

Introduction

During the past five years, consumers – especially younger consumers, roughly those in their 20s and 30s – have become more aware of privacy laws governing the use of their personal information. Today, they are playing a greater role in ensuring their information remains safe. Under many privacy laws, consumers have the right to ask about the data organizations collect about them, and many are doing so. They are not only inquiring about their data but are also switching providers over privacy practices. If organizations are not transparent about how they use customers' personal data or how they make data-driven decisions, consumers more willingly take action to protect their data and themselves.

This report, Cisco's fifth annual review of consumer privacy, explores current privacy trends, challenges, and opportunities for consumers. It draws upon data gathered in June 2023 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 2,600 adults (18 years and older) in 12 countries (5 Europe, 4 Asia, 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.

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

"As governments pass laws and companies seek to build trust, consumers must also take action and use technology responsibly to protect their own privacy."

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

Key highlights

1. More consumers are taking action to protect their privacy, particularly younger generations.

2. Consumers want their governments to take the lead role on privacy, and privacy laws continue to be viewed very positively around the world.

3. Consumers are split on the value of data localization requirements, with many indicating that local data storage may not be worth the added costs.

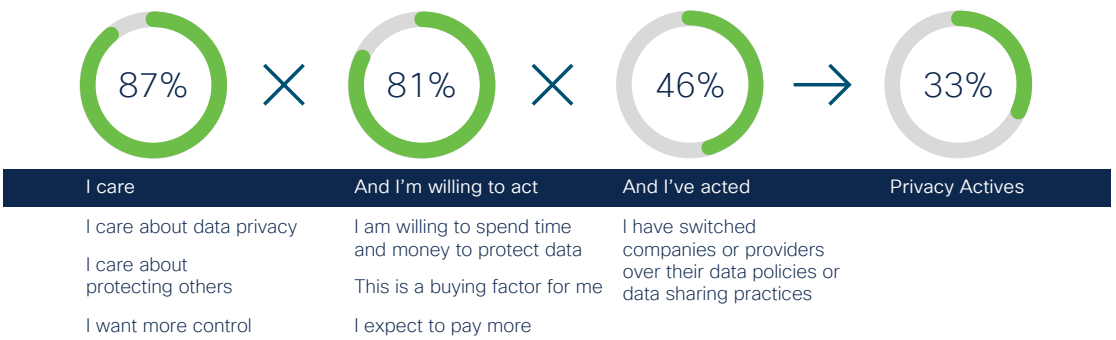
4. Consumers are very concerned about the use of their personal information in AI, and organizations must take additional steps to earn and build their confidence and trust.

5. Regular users of Generative AI are generally aware of the risks these applications pose, but only about half of them are taking action; the other half seem to have accepted the risk.

1. “Privacy Actives” and the role of the younger generations

During the past five years, we have been tracking a segment of consumers called “Privacy Actives.” This segment consists of people who say they care about privacy, are willing to act to protect it, and most importantly, have already taken action by switching companies or providers over their data policies or data-sharing practices. Among this year’s respondents, we found that 33% qualified as Privacy Actives, up from 32% in last year’s survey, and 29% three years ago. See Figure 1.

Figure 1. The “Privacy Actives” Segment

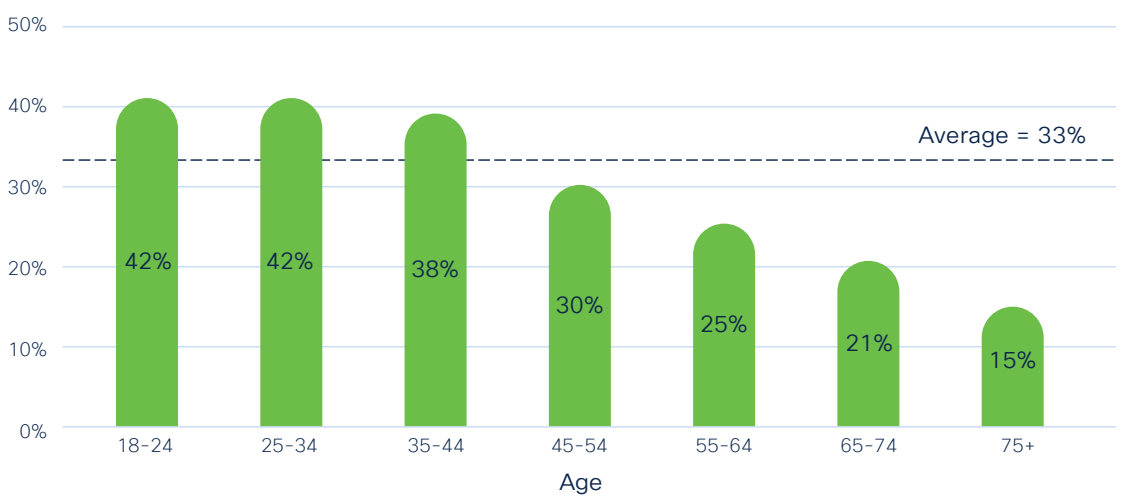


Note: The 81% and 46% are based on the relevant subset, not necessarily the overall respondent pool.

Source: Cisco 2023 Consumer Privacy Survey

Interestingly, survey results indicate that younger consumers are the most willing to take action when it is necessary to protect their privacy. Forty-two percent of consumers aged 18-34 are Privacy Actives and that percentage steadily decreases with age. Among consumers who are 75 years and older, only 15% are Privacy Actives. See Figure 2.

Figure 2. Privacy Actives, by Age

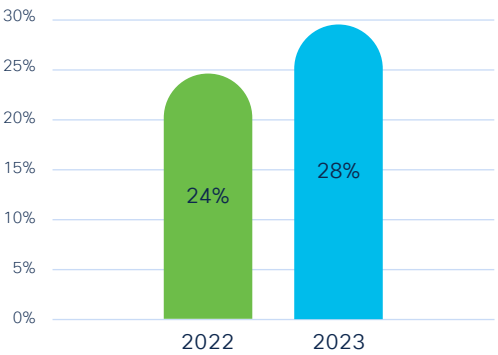


Source: Cisco 2023 Consumer Privacy Survey

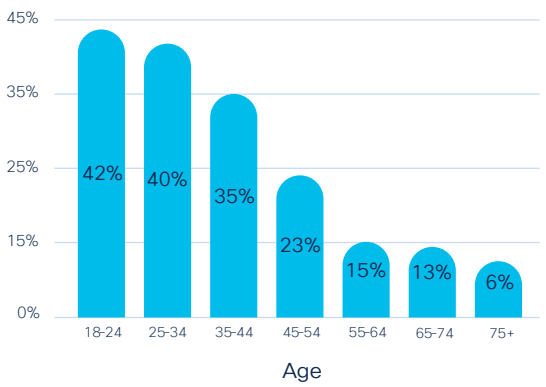
There are several actions consumers can take to try to understand and possibly correct the data that organizations have about them. Under many privacy laws, consumers have Data Subject Access Rights (DSAR), enabling them to inquire about their data and, in some cases, to request that their data be changed or deleted. Among survey respondents, 28% indicated they exercised their rights to inquire about data, up from 24% last year. Amongst those exercising DSAR, younger consumers are more active with 42% of consumers aged 18-24 doing so, compared with just 6% for consumers 75 years and older. See Figure 3.

Figure 3. Consumers Exercising Data Subject Access Rights (DSAR)

Percent exercising DSAR (2022-2023)



Percent exercising DSAR, by age (2023)

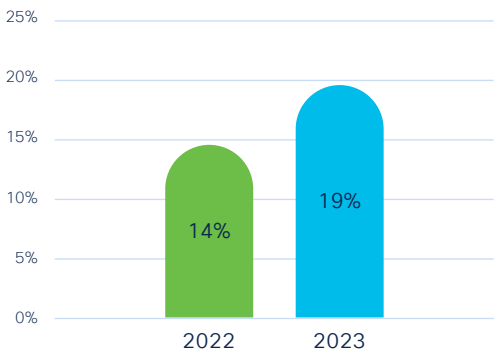


Source: Cisco 2023 Consumer Privacy Survey

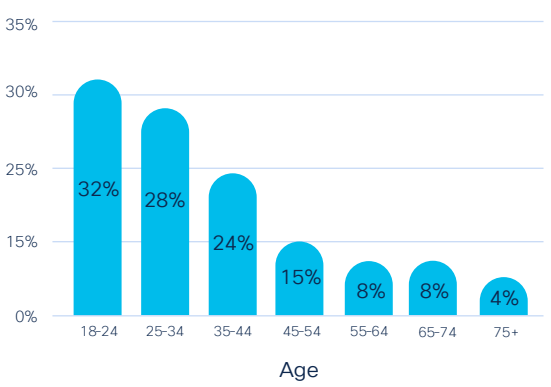
When it comes to requesting data changes or deletions, the percentage of consumers making these requests rose to 19%, up from 14% last year. Again, this is highly correlated with age, with 32% of consumers aged 18-24 making data changes or deletion requests compared to only 4% of the oldest consumers. See Figure 4.

Figure 4. Consumers Making Data Changes or Deletion Requests

Percent requesting data changes or deletion (2022-2023)



Percent requesting data changes or deletion, by age (2023)



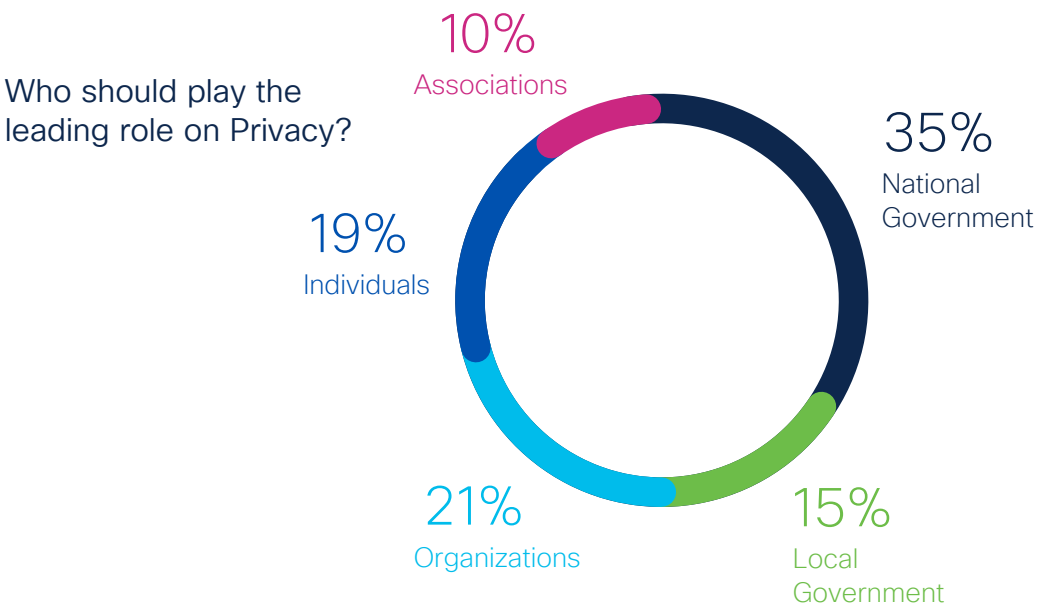
Source: Cisco 2023 Consumer Privacy Survey

2. Impact and awareness of privacy laws

A. Governments' role

While governments, organizations, and individuals all have roles to play in protecting personal data, survey respondents were asked which should have the primary role. Half (50%) said national or local government should be primary, 21% said organizations, including private companies, and 19% said the individuals themselves should be primarily responsible for protecting their own data. See Figure 5.

Figure 5. Consumers' Views on Privacy Leadership



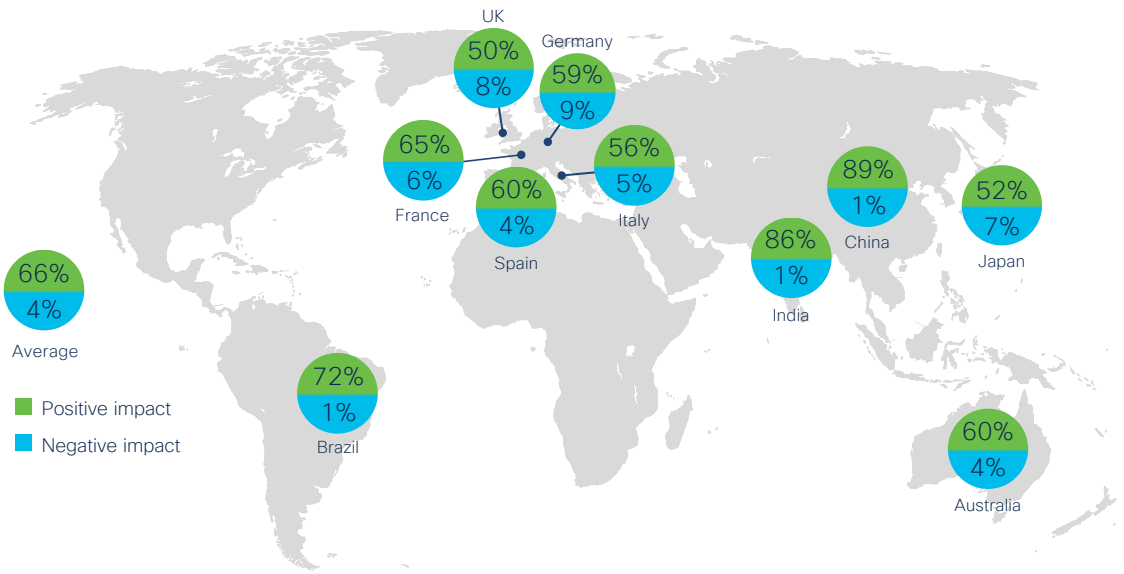
Source: Cisco 2023 Consumer Privacy Survey

Many consumers don't trust private companies to be responsible for protecting personal data on their own. However, consumers also feel they have limited power to safeguard their personal data. Thus, they look to the government to set the standard of care and enforce privacy protections. Perhaps for this reason, consumers continue to look at their country's privacy laws very favorably.

In this year's survey, we tested reactions to the General Data Protection Regulation (GDPR) among European Union (EU) respondents, as well as specific privacy laws in other countries, including Australia's Privacy Act 1988, Personal Information Protection Law in China, Lei Geral de Proteção de Dados Pessoais in Brazil, Japan's Personal Information Protection Act, and the draft Personal Data Protection Bill in India.

Among respondents in these countries who were aware of their country's laws, 66% felt the laws have had a positive impact, up from 61% last year and 53% three years ago. Only 4% felt they have had a negative impact. All of the individual countries had strong positive responses, with China (89% positive, 1% negative) and India (86% positive, 1% negative) the most strongly in favor. Remarkably, no country had more than 9% of respondents believing that their laws have had a negative reaction. See Figure 6.

Figure 6. Impact of Country's Privacy Laws

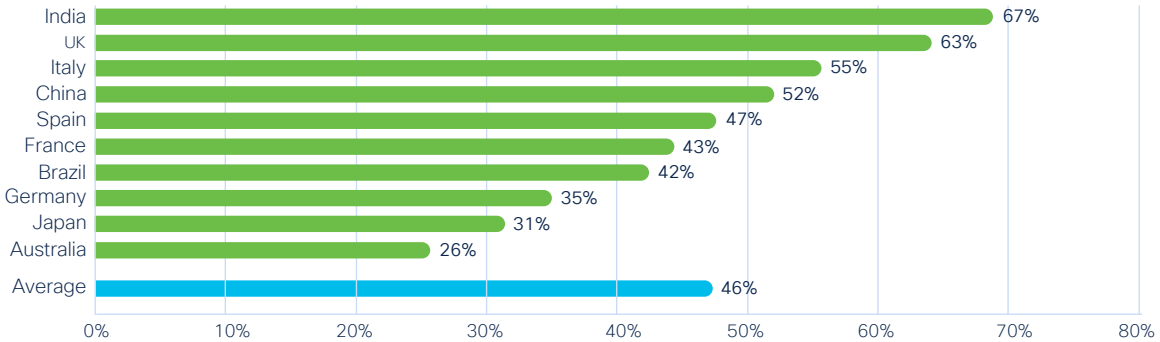


Source: Cisco 2023 Consumer Privacy Survey

B. Awareness of privacy laws

Public awareness of privacy laws continues to be relatively low but has increased in the past year. Overall, 46% of respondents were aware of their country's privacy law, up from 43% last year, with the highest awareness percentages in India (67%), the UK (63%), and Italy (55%). One reason for India's high awareness may be that their privacy law has been frequently in the news and was passed by Parliament in August 2023. See Figure 7.

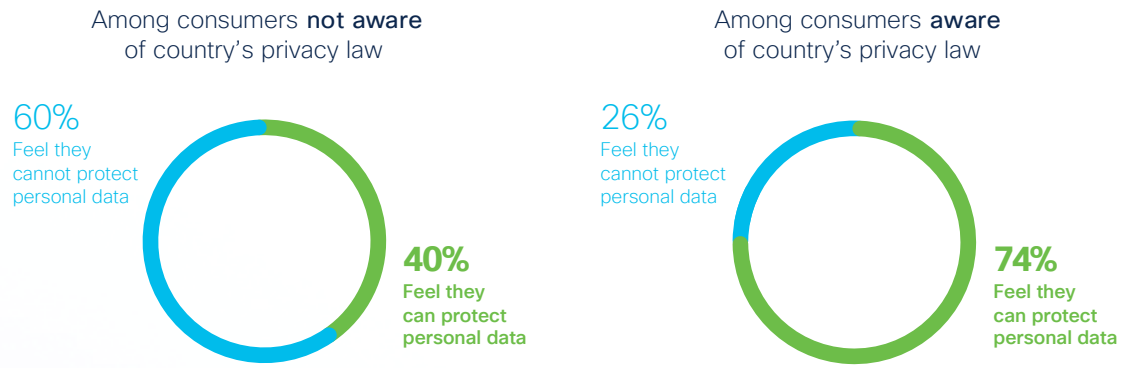
Figure 7. Awareness of Country's Privacy Law



Source: Cisco 2023 Consumer Privacy Survey

Awareness of the law seems to be an important factor when it comes to consumer confidence. Those that are aware of the law are more likely to feel they can adequately protect their data. In this year's survey, only 40% of respondents who were not aware of their country's law felt they could adequately protect their data. However, among those who were aware of these laws, 74% of respondents felt they could adequately protect their data. Governments have a responsibility not only to enact privacy laws, but also to build confidence that they are governing for their constituents' best interests. It is also important that they help ensure citizens are aware of the law and educated about their rights under the law. See Figure 8.

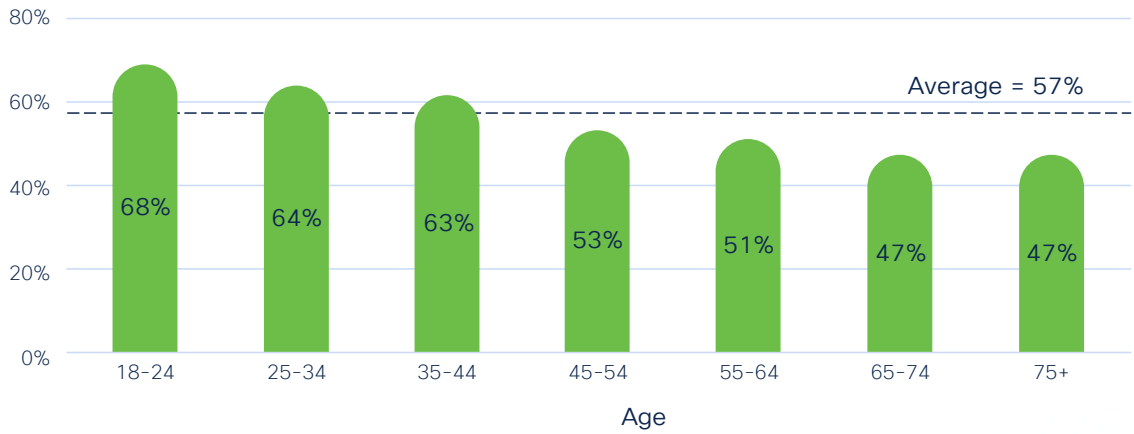
Figure 8. Consumers' Awareness of Privacy Law and Their Ability to Protect Data



Source: Cisco 2023 Consumer Privacy Survey

As described above, younger consumers are taking a more active role in protecting their privacy. They are also more aware of the privacy laws, and this translates into higher confidence when it comes to protecting their own data. Overall, 57% of consumers feel they can protect their data, with higher percentages for the younger generations. Sixty-eight percent of consumers aged 18-24 feel they can protect their data, and it gradually declines to only 47% of consumers over age 65 saying so. See Figure 9.

Figure 9. Percentage Indicating They Can Adequately Protect Their Data, by Age



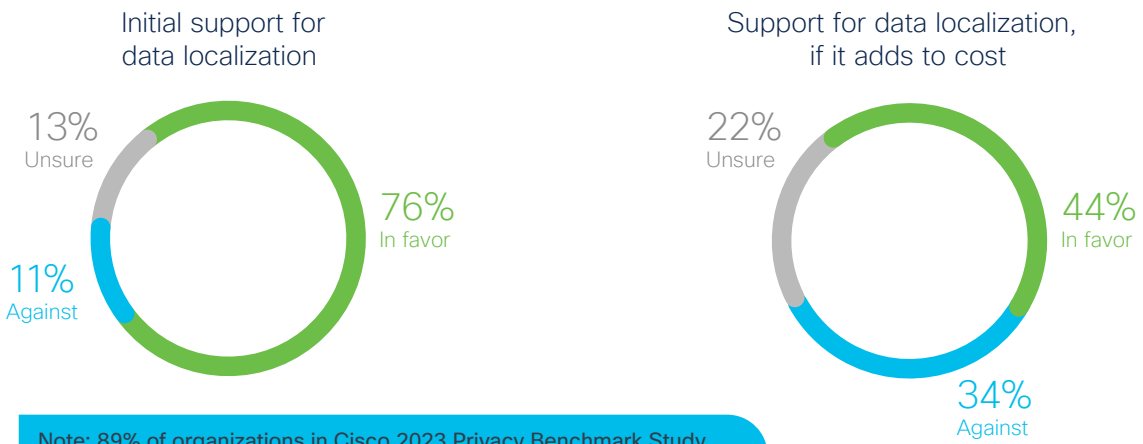
Source: Cisco 2023 Consumer Privacy Survey

C. Data localization

As governments and organizations continue to demand protections on data transferred outside of their national borders, more are putting in place data localization requirements to force data to be physically stored in the country where it was collected or other approved locations. Most consumers have heard about these requirements, and 76% of respondents indicated initially that 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 and told localization would make the products and services they buy more expensive, they were far less supportive, with only 44% in favor of localization. Of course, data localization does add cost. The Cisco 2023 Data Privacy Benchmark Study reported that 89% of surveyed organizations were experiencing significant additional operational costs due to data localization requirements. See Figure 10.

Figure 10. Data Localization



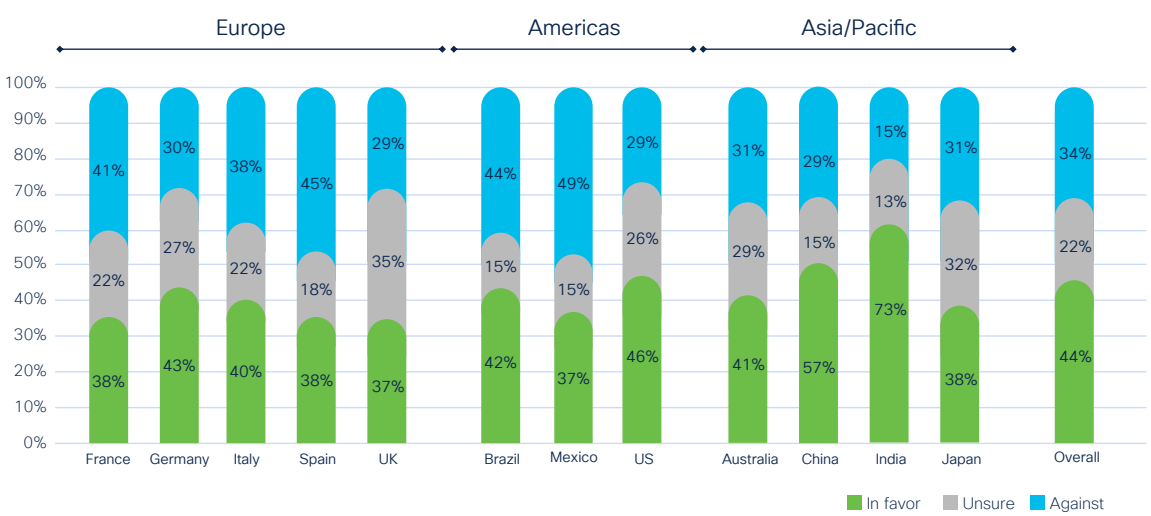
Note: 89% of organizations in Cisco 2023 Privacy Benchmark Study said data localization adds significant cost to their operation.

Source: Cisco 2023 Consumer Privacy Survey

The cost of data localization may be more than merely a financial burden. When keeping data local to their country, organizations may be forced to select less sophisticated or capable, in-country providers and partners who are unable to rapidly deploy new features, functionality, or security updates to disparate, local instances of applications, and may be resource constrained to deliver redundant services and capabilities in multiple geographies.

There are significant differences across geographies and overall the results are mixed. In Europe, three countries – Germany, Italy, and the UK – had more respondents in favor, and two countries – France and Spain – had more respondents against. In the Americas, the US had more respondents in favor, but the two other countries surveyed – Brazil and Mexico – had more respondents against. Respondents from the four Asian countries were positive on localization, including respondents from India who were 73% in favor and 15% against. See Figure 11.

Figure 11. Reaction to Data Localization, by Country



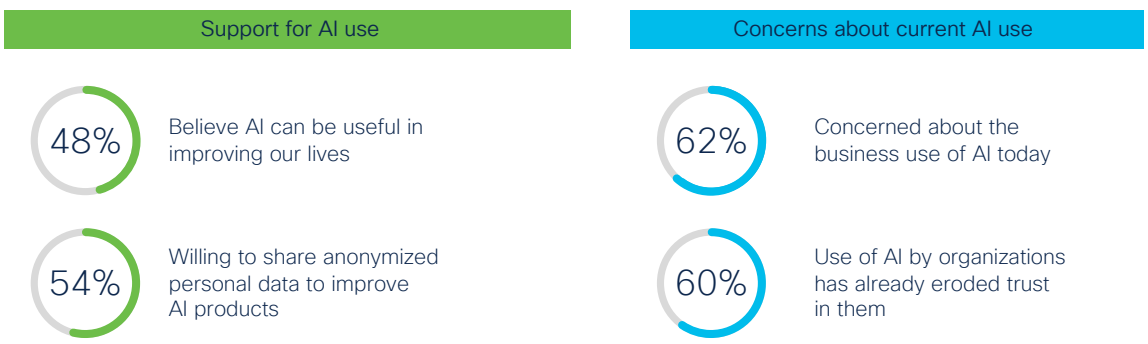
Source: Cisco 2023 Consumer Privacy Survey

3. Artificial Intelligence and automated decision-making using personal data

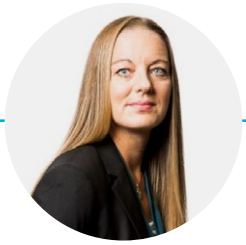
Artificial Intelligence has the potential to use customer data in ways that create more efficient and personalized experiences for consumers. Forty-eight percent of survey respondents agree (23% disagree) that AI can be useful in improving their lives – from shopping to streaming services to healthcare and beyond. And a majority of respondents (54% agree, 29% disagree) said they are 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 uses personal data for automated decision-making, and most consumers (77%) believe that organizations must be careful and act responsibly in this area.

Consumers are quite concerned about how organizations train, implement, and use AI. Sixty-two percent of consumers in our survey expressed concern about how organizations are using their personal data for AI today, with 60% saying that they have already lost some trust in organizations because of their AI use. See Figure 12.

Figure 12. Consumers Support AI Use, but Are Also Concerned



Source: Cisco 2023 Consumer Privacy Survey



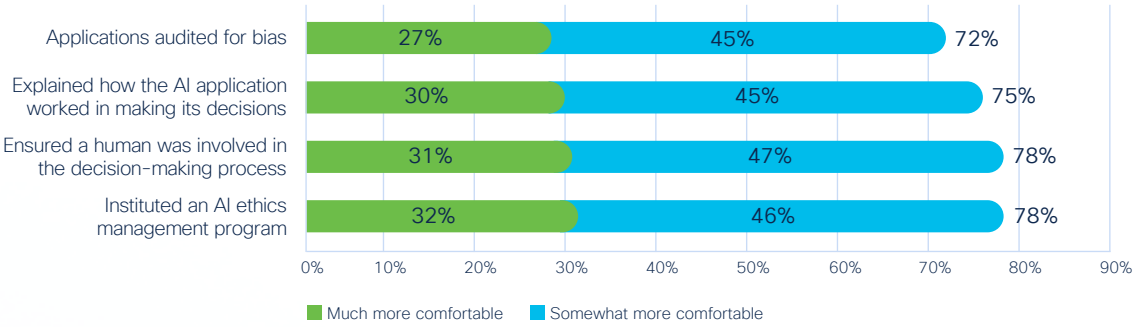
"Transparency is key to trust. Consumers want clarity about how companies are integrating AI into their products and services."

Dev Stahlkopf, Cisco Executive Vice President, Chief Legal Officer

Fortunately, there are steps organizations can take to reduce the potential negative impact their AI may have on customer trust. Seventy-two percent of respondents indicated that having products and solutions audited for bias would make them "somewhat" or "much more" comfortable with AI. Other steps, such as being more transparent and explaining how the AI works, ensuring human involvement, and instituting an AI ethics management program would make 75%+ of respondents more comfortable with the AI. These results can help guide organizations to make the investments necessary to maintain trust with their customers when it comes to AI. See Figure 13.

Figure 13. Steps Organizations Can Take to Build Trust in AI

Percentage of consumers saying they would be more comfortable with AI if organizations took this specific action



Source: Cisco 2023 Consumer Privacy Survey

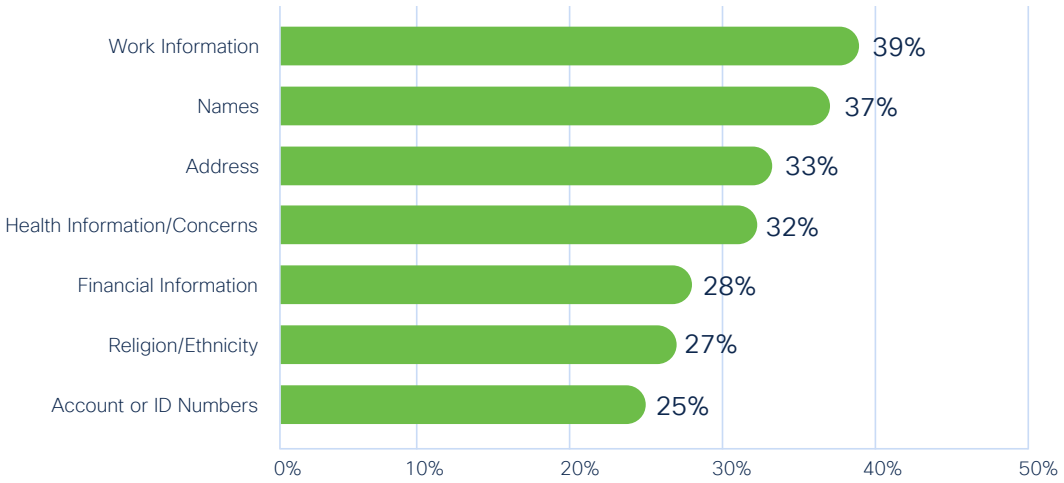
4. Generative AI

Generative AI (Gen AI) applications, such as ChatGPT and DALL-E, have the power to use AI and machine learning to create new content based on user prompts, including text, music, images, 3D rendering, video, and code. Many consumers learned about Gen AI over the past few months, and their survey responses regarding Gen AI provide an early snapshot of its use and some of the potential risks and challenges.

As of June 2023, when our survey was conducted, Gen AI was still relatively new to most people. Over half (52%) of survey respondents said they were not aware of it, 36% said they were aware of Gen AI but were not regular users, and only 12% indicated they were regular users. We will focus on these regular users to better understand their practices and behaviors with Gen AI.

Sixty-three percent of these regular users said they were realizing significant value from Gen AI, with only 4% saying they were getting no value from it. In terms of the type of data they are entering, 39% said they have submitted work information, over 30% have entered names, addresses, or health information, and 25% to 30% of users have provided financial, religion/ethnicity, account or personal identification information. These categories of data could include personal or confidential information that could be problematic if the Gen AI applications were to share the data publicly or with competitors. See Figure 14.

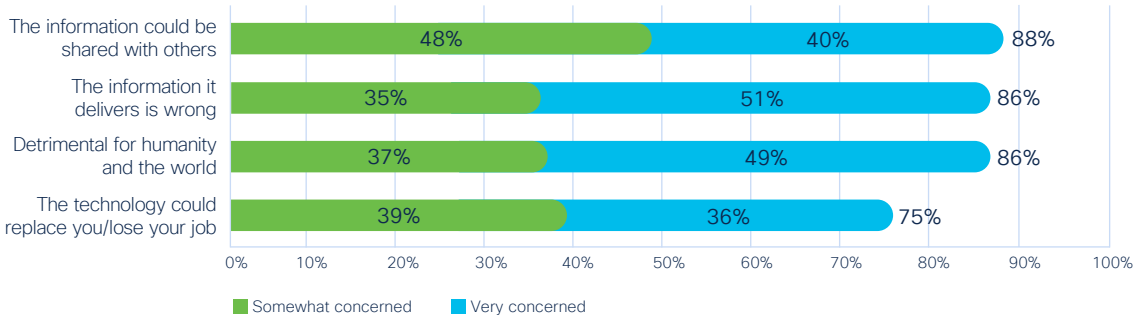
Figure 14. Type of Information Entered in Gen AI Applications



Source: Cisco 2023 Consumer Privacy Survey

Fortunately, most regular Gen AI users seem to be aware of the risks of this new technology. Eighty-eight percent said they would be "Somewhat Concerned" or "Very Concerned" if their data were to be shared. Eighty-six percent were concerned the information that they get from Gen AI could be wrong, and an equal percentage thought Gen AI could be detrimental for humanity or the world. Seventy-five percent were concerned they could lose their jobs or be replaced by Gen AI. See Figure 15.

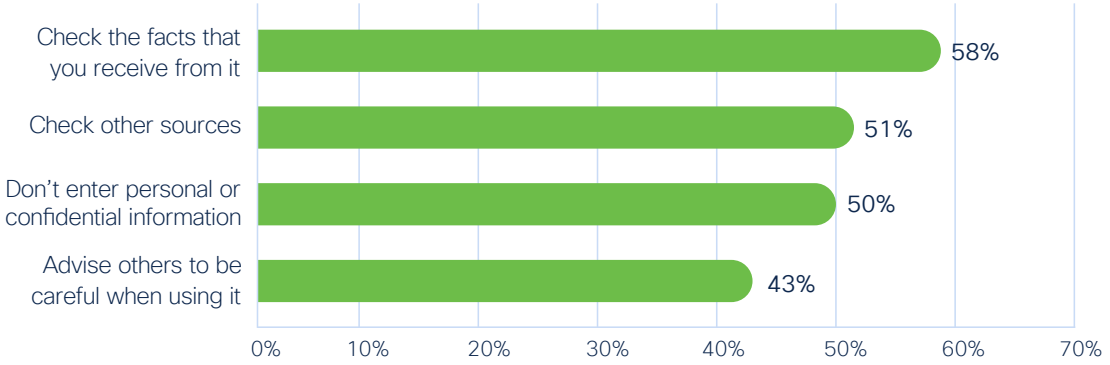
Figure 15. User Concerns about Risks with Gen AI



Source: Cisco 2023 Consumer Privacy Survey

There are a variety of ways one can minimize the risks of Gen AI, and many of the regular Gen AI users in our survey indicated they were taking action. Fifty-eight percent said they were checking the facts they received from Gen AI, and 51% said they were checking other sources of information. Half (50%) said they were refraining from entering personal or confidential information into Gen AI applications, but it is notable and worrisome that perhaps the other 50% are indeed entering personal or confidential information. See Figure 16.

Figure 16. User Steps to Reduce Risks with Gen AI



Source: Cisco 2023 Consumer Privacy Survey

As Gen AI is relatively new to most consumers, it will be helpful to track user behavior over time, especially on these dimensions. Are users aware of the risks of Gen AI? Are they taking actions to minimize the risks? In this year's survey, 82% were generally aware of and concerned about the risks and 53% of respondents indicated they were taking action to minimize the risks. Multiplied together, it means 44% of the regular Gen AI users can be considered "Concerned and Acting" users. We will see how this metric evolves in future research. See Figure 17.

Figure 17: "Concerned and Acting" Gen AI Users

Source: Cisco 2023 Consumer Privacy Survey

Conclusion

Recommendations for organizations

Privacy attitudes and behaviors have evolved significantly over the past five years. Governments have passed many laws protecting privacy, organizations have established processes to try to earn and maintain trust with their customers over data use, and consumers are taking greater action and responsibility – where they can – to protect their personal data. The findings in this research point to specific recommendations for organizations to help improve data privacy and build consumer confidence:

Educate individuals about privacy and their rights.

There is a strong correlation between consumer awareness of privacy laws and their confidence that their data is protected. It is important that everyone understands the protections available to them and takes the necessary actions to protect their personal data. Broaden your customers' awareness and inform them of their rights to help improve their privacy and confidence.

Adopt measures for responsible data use, especially as it applies to AI.

Organizations can build and maintain consumer confidence by adopting a governance framework centered on respecting privacy, providing greater transparency on personal data use in AI, and implementing procedures to help eliminate bias and increase fairness and accountability.

Consider the costs, impact, and alternatives to data localization.

Data localization is not as attractive to consumers given the added costs, 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 or access, or economic protectionism.

Enact appropriate controls on the use of Gen AI.

Despite their awareness of the risks, many regular Gen AI users are entering work or personal data that could be problematic if it were to be shared. Controls and oversight are needed to protect privacy and confidentiality.

Learn more about consumer sentiment and trends regarding privacy on the Consumer Privacy Survey page and our annual review of key privacy issues and their impact on business on the Data Privacy Benchmark Study page. In future research, we will continue to explore how shifting consumer sentiment, evolving technology, and data regulations will impact privacy for organizations and consumers over time.

Additionally, Cisco publishes Privacy Data Sheets and Privacy Data Maps for its major products and services, enabling anyone interested to understand what data is used, who has access to it, and how long it is retained. This research and other privacy and security related content are available on the Cisco Trust Center.

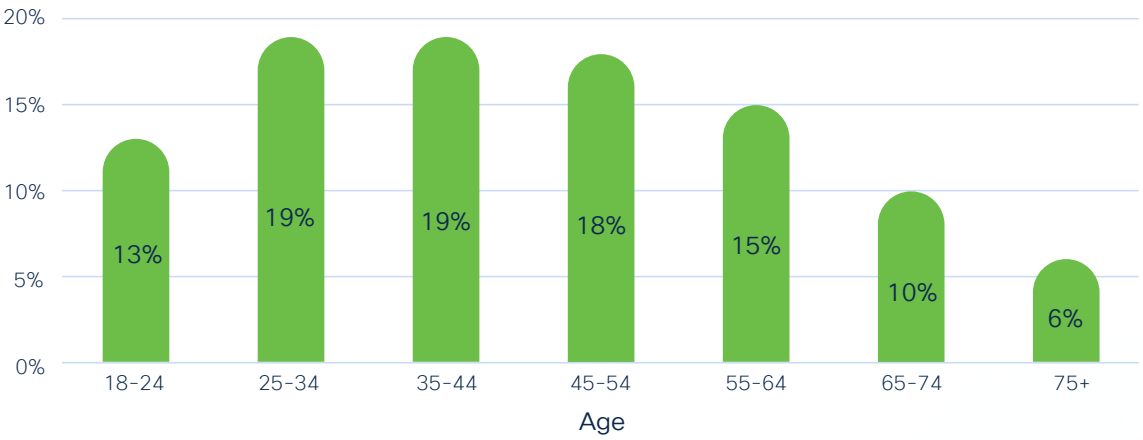
For additional information about Cisco's privacy research, contact Robert Waitman, Cisco Privacy Director, at rwaitman@cisco.com.

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 Report, 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.

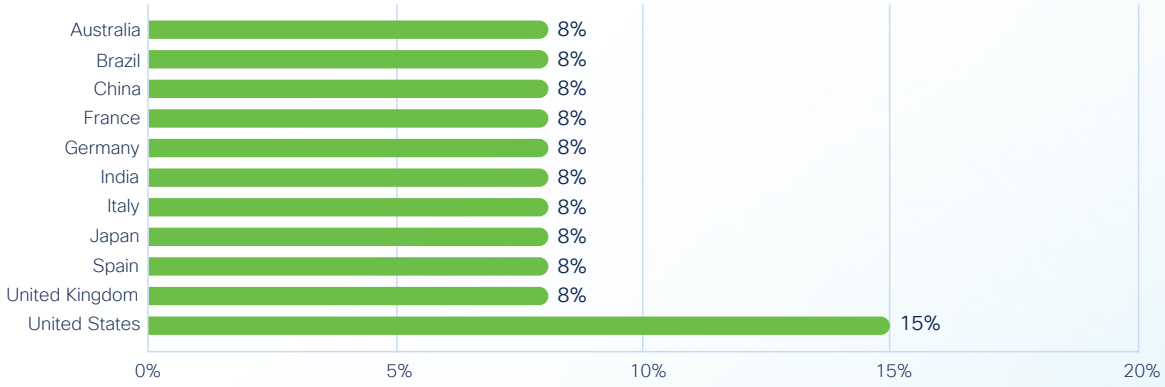
Appendix

Demographics of Survey Respondents, by Age



Source: Cisco 2023 Consumer Privacy Survey

Demographics of Survey Respondents, by Geography



Source: Cisco 2023 Consumer Privacy Survey