Privacy Awareness: Consumers Taking Charge to Protect Personal Information

CISCO 2024 CONSUMER PRIVACY SURVEY

Table of Contents

Introduction

For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data. And this year, for the first time, a majority of respondents are not only aware of their local privacy laws, but also report feeling significantly more protected by these regulations. Notably, consumers in their 20s and 30s are leading the charge, not only by questioning data practices but also by switching providers when privacy standards are not met.

This consumer awareness coincides with the rapid advancement of artificial intelligence (AI) and its promise to reshape the way we live, work, and interact. As these novel technologies become increasingly embedded in our daily lives, they bring with them a new set of questions around privacy, safety, and trust.

Methodology

This report explores current trends, challenges, and opportunities in privacy and AI. It draws upon data gathered in the summer of 2024 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 comprised 2600+ adults (18 years and older) in 12 countries (5 Europe, 4 Asia, and 3 Americas).[1]

Respondents were asked about their awareness and attitudes regarding companies' use of personal data, privacy legislation, Generative AI (Gen AI), and data localization requirements. The findings from this research demonstrate the importance of privacy legislation, the increasing actions consumers are taking to protect their privacy, and the implications for organizations and governments that serve them.

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

"Privacy has grown from a compliance matter to a customer requirement. Understanding and adapting to a more privacy-active consumer base will be crucial for businesses aiming to maintain a competitive edge."

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

Key findings

1. For the first time, a majority of respondents are familiar with privacy laws in their countries. Consumers who are aware of local privacy laws are also more confident in their ability to protect their data.

2. Privacy practices impact buying decisions, with three-quarters of respondents saying they will not purchase from organizations they do not trust with their data.

3. Privacy laws continue to be viewed very positively around the world, and most respondents favor a US federal privacy law.

4. Regular users of Gen AI have nearly doubled in the past year but are still in the minority.

5. The majority of respondents think AI can be useful in improving lives and expect organizations to help ensure the technology is used ethically and responsibly.

Results

1. Privacy laws

a. Awareness and impact of privacy laws

There are now more than 160 countries with omnibus privacy laws in place. We have been tracking consumer awareness and reaction to these laws to better understand their value and impact. In 2019, only 36% of survey respondents were aware of their country's privacy laws, and this percentage has been steadily increasing.

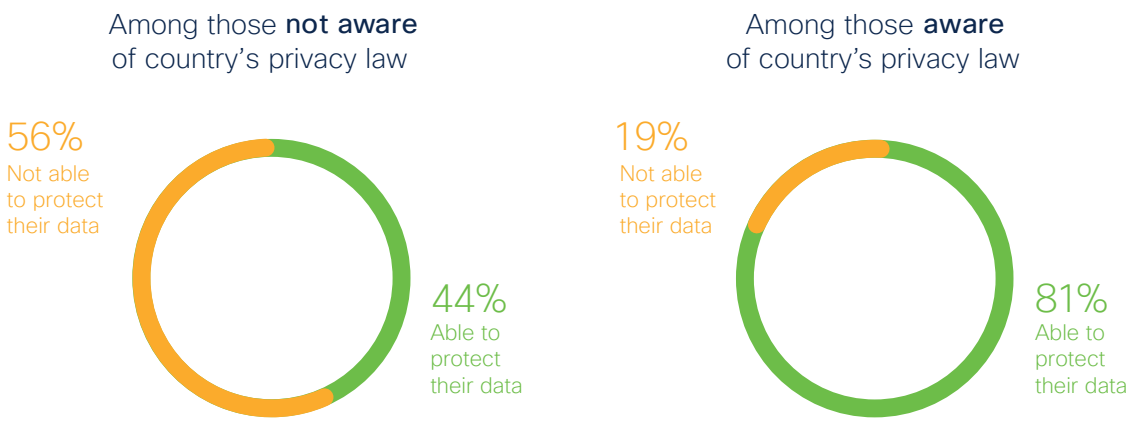
For the first time, in 2024, a majority of respondents (53%) said they were aware of their country's privacy laws. Since we started this research in 2019, the change from 46% in 2023 to 53% this year – an increase of 7 percentage points – is the largest awareness growth year over year. See Figure 1.

Figure 1. Awareness of privacy laws, 2019–24

Source: Cisco 2024 Consumer Privacy Survey

Awareness of privacy laws highly correlates with consumer confidence. Among respondents who were not aware of their country's privacy laws, only 44% said they are able to protect their personal data. By contrast, among those who are aware of these laws, 81% said they are able to protect their data. See Figure 2.

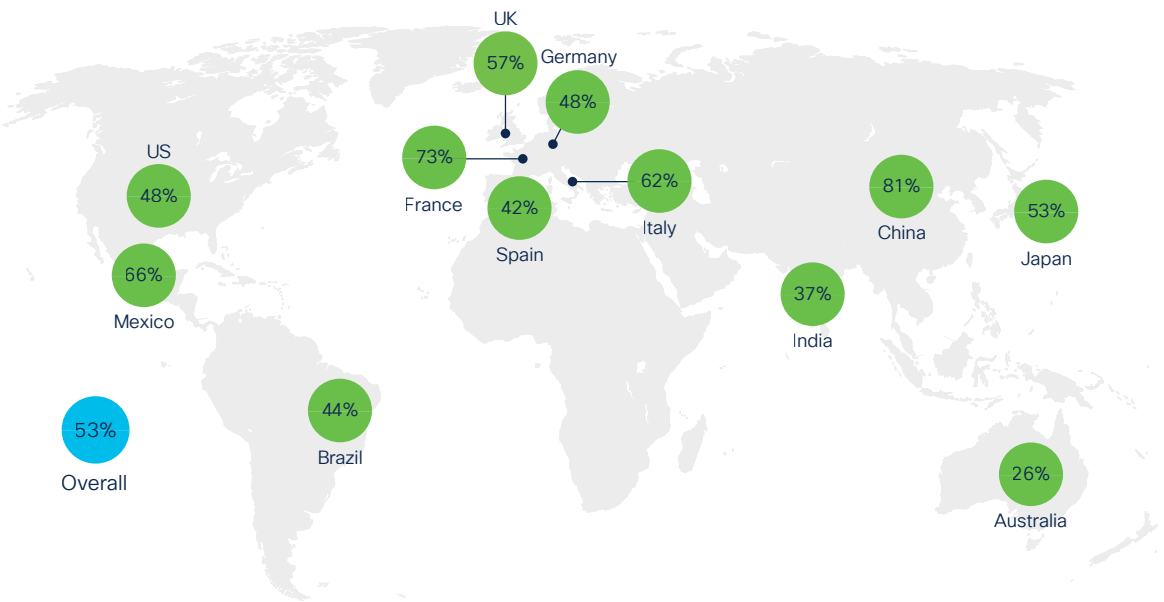
Figure 2. Awareness of privacy laws and ability to protect data



Source: Cisco 2024 Consumer Privacy Survey

Awareness of privacy laws varied significantly by country, with the highest percentages in China (81%) and France (73%), and the lowest percentages in India (37%) and Australia (26%). See Figure 3.

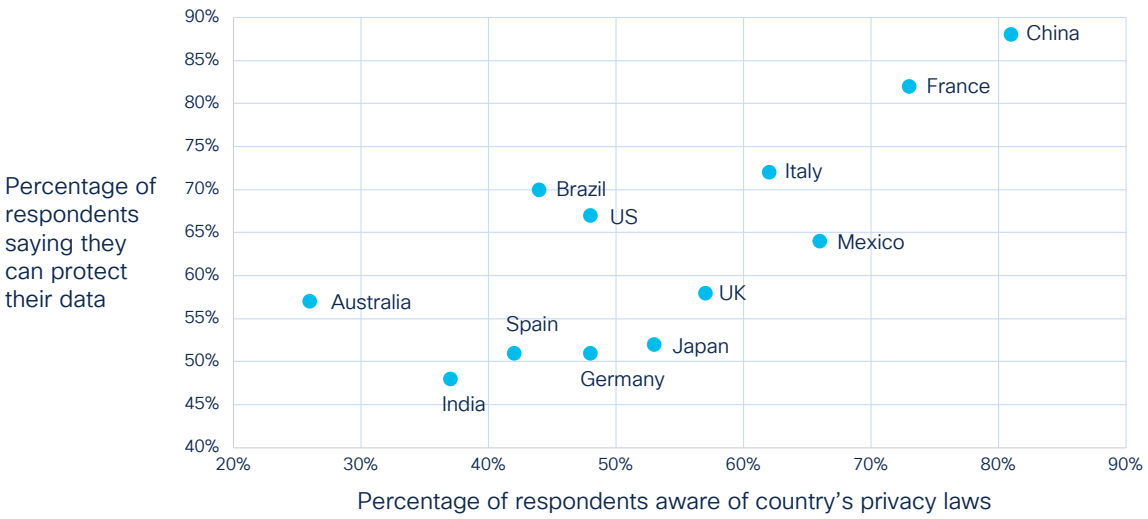
Figure 3. Awareness of privacy laws, by country



Source: Cisco 2024 Consumer Privacy Survey

There is a correlation between the respondents' awareness of their country's privacy laws and their ability to protect their data. See Figure 4.

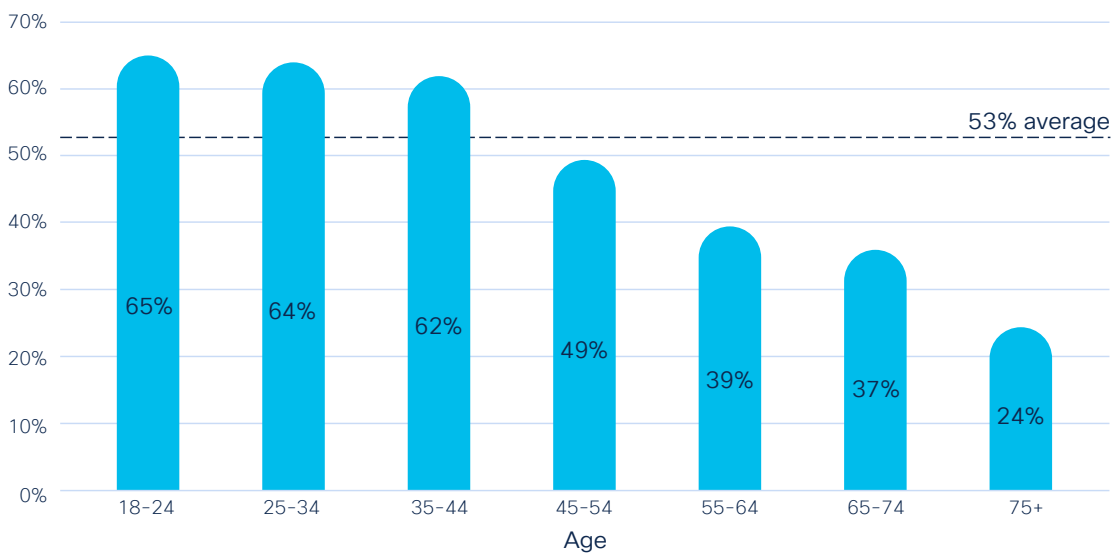
Figure 4. Awareness of privacy laws and ability to protect data, by country



Source: Cisco 2024 Consumer Privacy Survey

There was also a strong correlation between the age of respondents and their awareness of existing privacy laws. Younger consumers were much more likely to be aware of existing privacy laws. Sixty-five percent of respondents aged 18-24 were aware of their country's privacy laws, and this percentage steadily declined with age. Only 24% of respondents over age 75 were aware of the laws. See Figure 5.

Figure 5. Awareness of privacy laws, by age

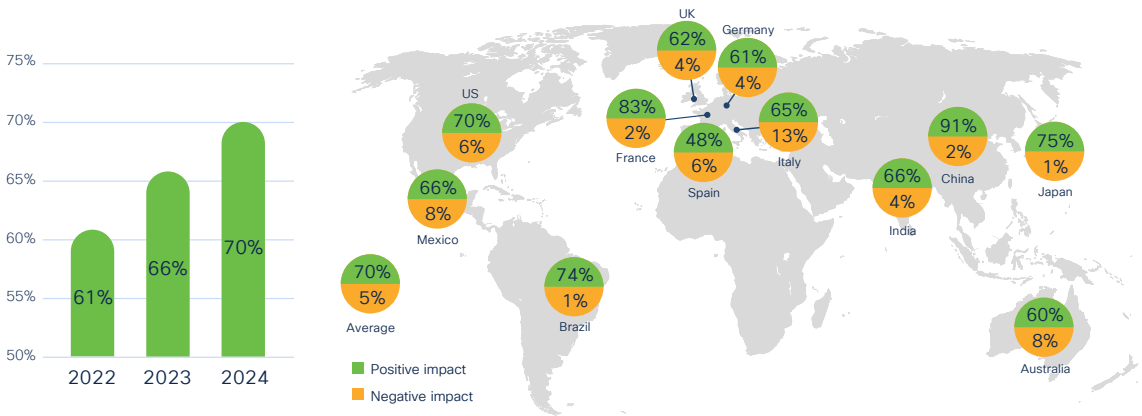


Source: Cisco 2024 Consumer Privacy Survey

b. Positive impact of laws

Consumers continue to view privacy laws very favorably. Among this year's respondents who were aware of the privacy laws, 70% felt privacy laws have had a positive impact, up from 66% last year and 61% two years ago. On average, only 5% of respondents felt they had a negative impact. See Figure 6.

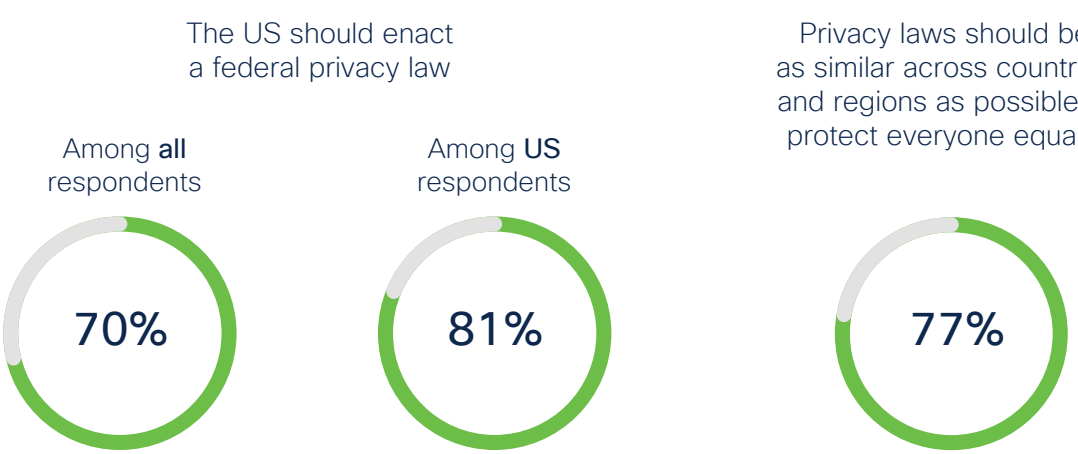
Figure 6. Impact of country's privacy laws



Source: Cisco 2024 Consumer Privacy Survey

Consumers were also supportive of the potential enactment of US federal privacy law. Seventy percent of all respondents, and 81% of US respondents, believe that the US should implement a nationwide privacy law. The vast majority (77%) also preferred consistency in privacy legislation across jurisdictions, suggesting a recognition of the global nature of data and the need for interoperable requirements and consistent protections. See Figure 7.

Figure 7. Future of privacy laws



Source: Cisco 2024 Consumer Privacy Survey

2. Consumer actions to protect their privacy

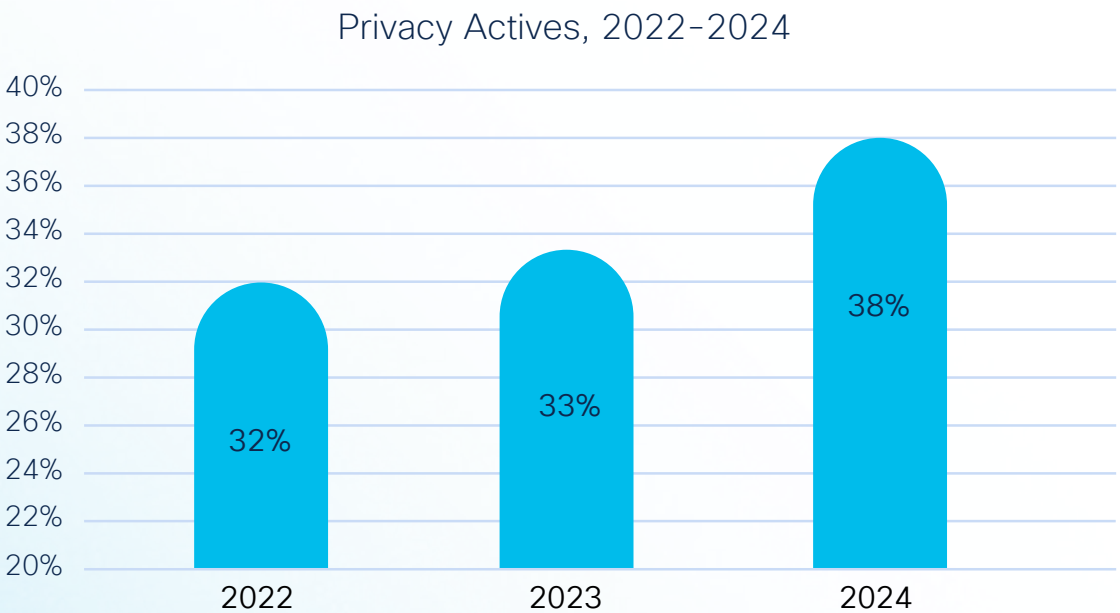
a. Privacy Actives segment

For the past six 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 taken action by switching companies or providers over their data policies or data-sharing practices. Among this year's respondents, 38% qualified as Privacy Actives, up significantly from 32% in 2022 and 33% in 2023. See Figure 8.

Figure 8. 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	

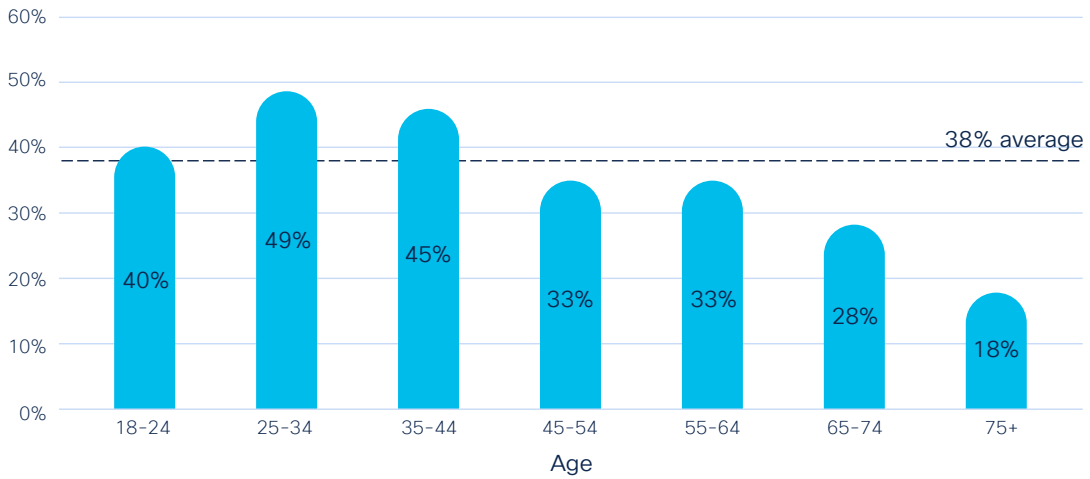
Note: The 83% and 51% are based on the relevant subset, not necessarily the overall respondent pool.
Source: Cisco 2024 Consumer Privacy Survey



Source: Cisco 2024 Consumer Privacy Survey

Younger consumers are much more likely to be Privacy Actives. Forty-nine percent of respondents aged 25-34 are Privacy Actives and that percentage steadily decreases with age. Among respondents who are between 45-64, 33% are Privacy Actives, and for those 75 years and older, the percentage drops to 18%. See Figure 9.

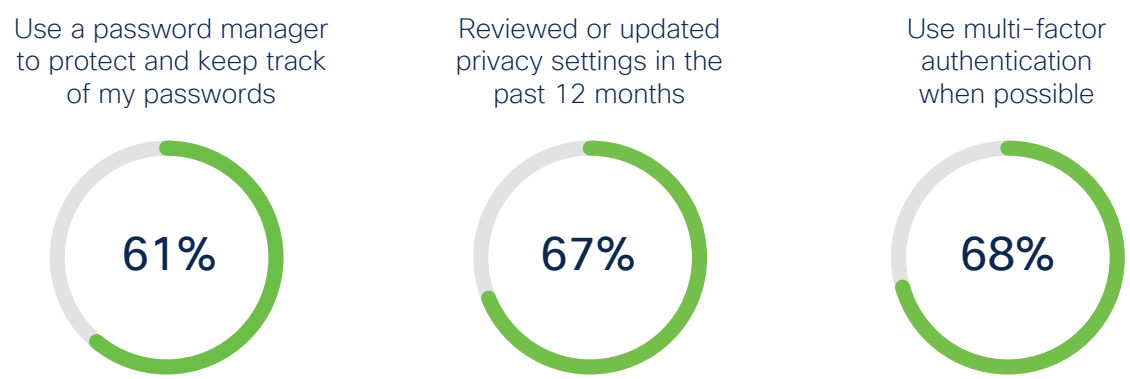
Figure 9. Privacy Actives, by age



Source: Cisco 2024 Consumer Privacy Survey

Consumers aren't solely relying on organizations to protect their privacy. They are taking actions into their own hands to protect their personal information. Sixty-one percent said they have used a password manager to protect and keep track of passwords. And two-thirds of respondents have reviewed or updated their privacy settings in the past 12 months, and use multi-factor authentication respectively. See Figure 10.

Figure 10. Consumers' actions to protect privacy

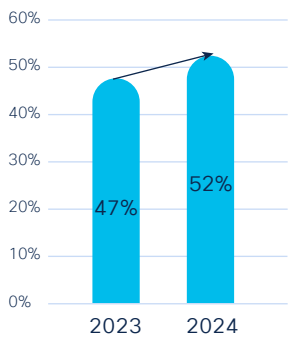


Source: Cisco 2024 Consumer Privacy Survey

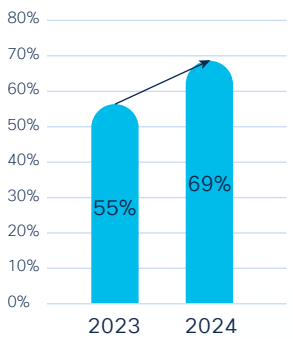
Consumers taking active steps to protect their information is a growing trend, with increases year over year in both turning off home assistants and managing cookie preferences. Notably, consumers are using their purchasing power to emphasize privacy. Seventy-five percent of respondents said they would not purchase from an organization they do not trust with their data. See Figure 11.

Figure 11. Consumers' actions to protect privacy

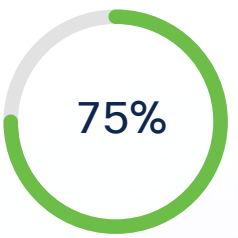
I turn off my home assistant at times to protect my privacy



I manage my cookie preferences and don't automatically accept all



I will not purchase from organizations I don't trust with my data

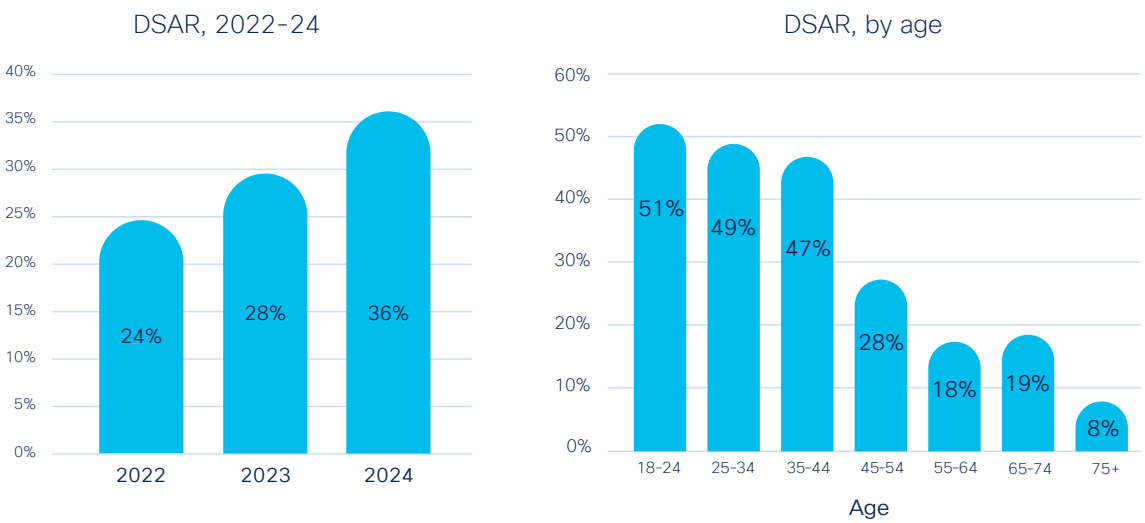


Source: Cisco 2024 Consumer Privacy Survey

b. Data Subject Access Request rights

There are several actions consumers can take to try to understand and manage the data that organizations have about them. Under many privacy laws, consumers have Data Subject Access Request (DSAR) rights, enabling them to inquire about their data and, in some cases, to request that their data be changed or deleted. Among survey respondents, 36% indicated they have exercised their rights to inquire about data, up from 28% this past year and 24% two years ago. Here again, younger consumers are leading the way. Fifty-one percent of respondents aged 18-24 have exercised a DSAR, compared with just 8% for respondents 75 years and older. See Figure 12.

Figure 12. Data Subject Access Request (DSAR)



Source: Cisco 2024 Consumer Privacy Survey

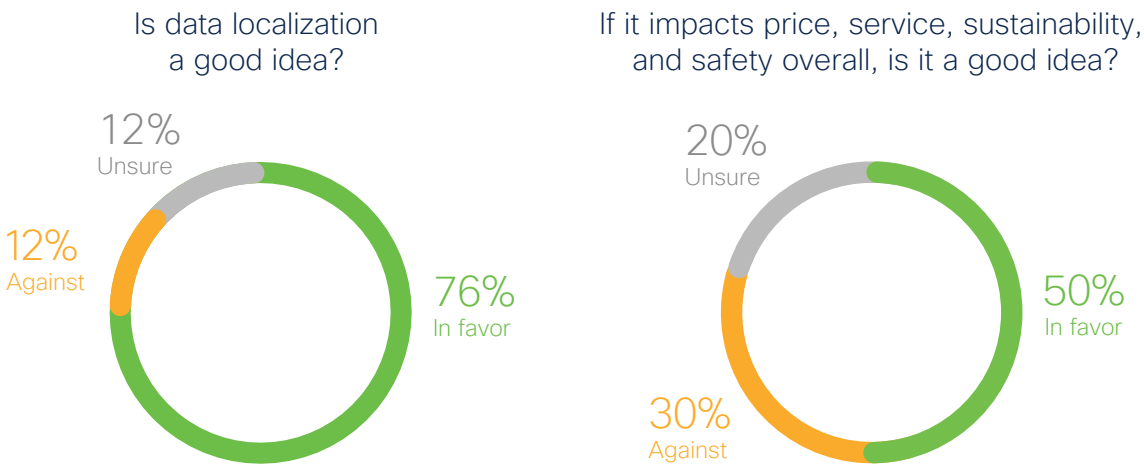
Younger consumers are more aware of the laws, more active in taking steps to protect their privacy, and more confident that their data is adequately protected. Therefore, it is important to also consider what can be done for older consumers who may be less privacy aware, less active, and less confident that their data is safe. Everyone should feel comfortable participating in the digital economy, which often includes sharing personal data with organizations when and where it is safe to do so.

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. Seventy-six percent of respondents initially indicated 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, with 12% initially against it.

However, when asked to factor in potential price increases, service reductions, sustainability, and service implications, they were far less supportive, with only 50% saying localization is a good idea and 30% opposed. Data localization does, in fact, add cost, and the Cisco 2024 Data Privacy Benchmark Study reported that 85% of surveyed organizations were experiencing significant additional operational costs due to data localization requirements. See Figure 13.

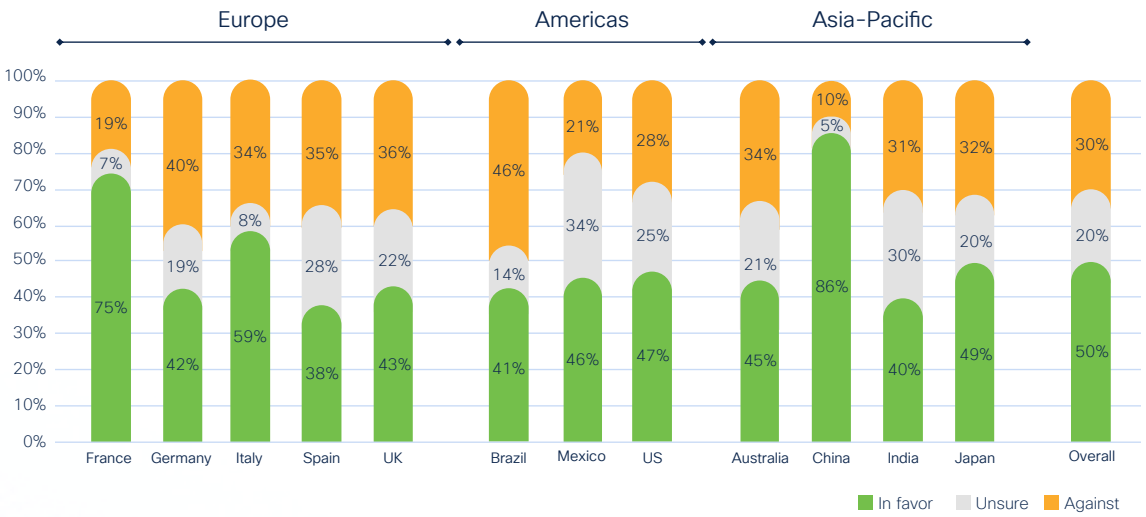
Figure 13. Data localization



Source: Cisco 2024 Consumer Privacy Survey

Support for data localization requirements varies by region and even among countries within a region. Europe generally has strong support for data localization policies, particularly in France (75%) and Italy (59%). The Americas show more variation, with Brazil more significantly against localization than the US, where opinion is more divided. The Asia-Pacific region is led by overwhelming support in China (86%). See Figure 14.

Figure 14. Reaction to data localization, by country



Note: Amounts may not sum and percentages may not recalculate due to rounding.
Source: Cisco 2024 Consumer Privacy Survey

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

Even in the early days of AI, the power and potential of leveraging data to create more efficient and personalized experiences for consumers is seemingly limitless. Sixty-three percent of survey respondents agreed that AI can be useful in improving their lives – from shopping to streaming services to healthcare and beyond. And more than half of the respondents (53%) said they were willing to share their anonymized health and medical information for AI to help improve healthcare for others. They believe that the potential benefits outweigh the risk, assuming proper anonymization techniques are applied. At the same time, most respondents (78%) believe that organizations should only use AI in an ethical manner. See Figure 15.

Figure 15. Artificial Intelligence

Source: Cisco 2024 Consumer Privacy Survey

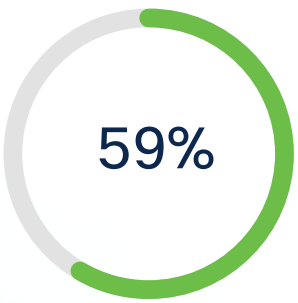
"With the growing role of AI in daily life, the spotlight is on its safe and responsible application. Companies should prioritize ethical AI to preserve customer trust."

Dev Stahlkopf, Cisco Executive Vice President, Chief Legal Officer

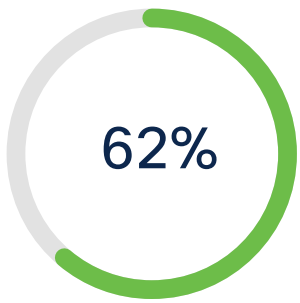
Fortunately, there are steps governments and organizations can take to reduce the potential negative impact their applications and use of AI may have on customer trust. Fifty-nine percent of respondents indicated that having strong privacy laws makes them more comfortable using AI applications, and a similar number (62%) said the same about strong AI laws. See Figure 16.

Figure 16. Impact of privacy and AI laws

Having strong **privacy laws** makes me more comfortable sharing my information in AI applications



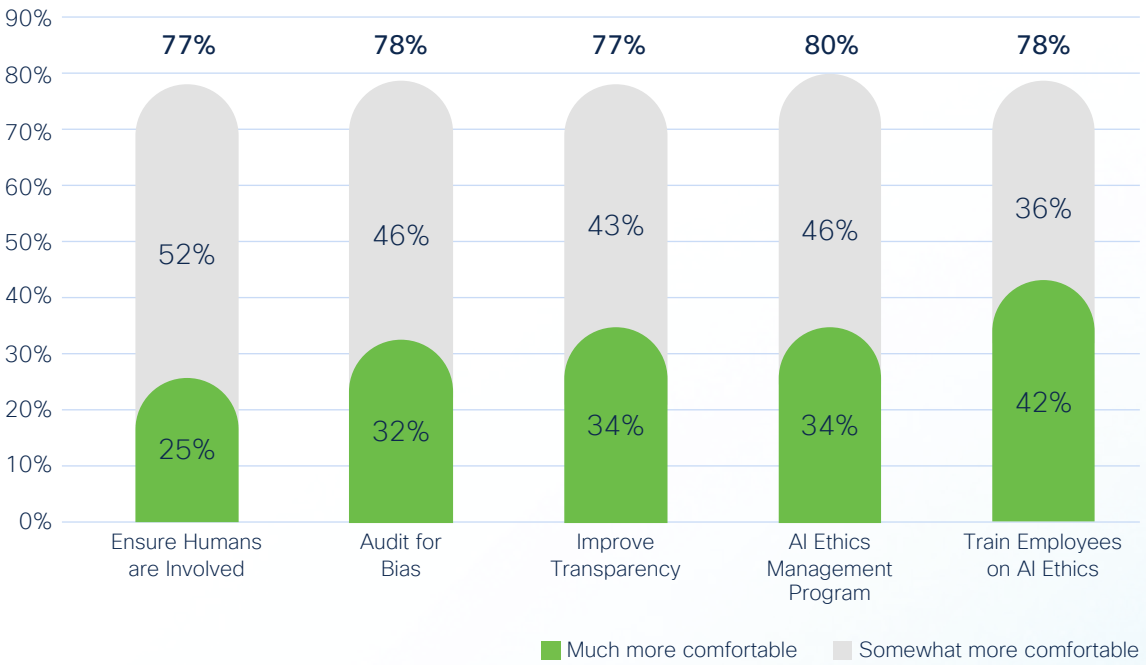
Having strong **AI laws** makes me more comfortable sharing my information in AI applications



Source: Cisco 2024 Consumer Privacy Survey

Organizations have a variety of options for earning and building customer trust when it comes to AI, including having a human involved, auditing for bias, improving transparency, instituting an AI Ethics Management Program, and training employees on AI Ethics. All of these options were viewed positively by respondents, with 77%–80% saying these steps would make them "somewhat more" or "much more" comfortable with the organization's AI use. Interestingly, the action that had the most impact on making respondents much more comfortable was training employees on AI Ethics (42%). These results can help guide organizations to make the investments necessary to foster comfort and confidence with their customers when it comes to AI. See Figure 17.

Figure 17. Organization actions that make consumers more comfortable with AI use

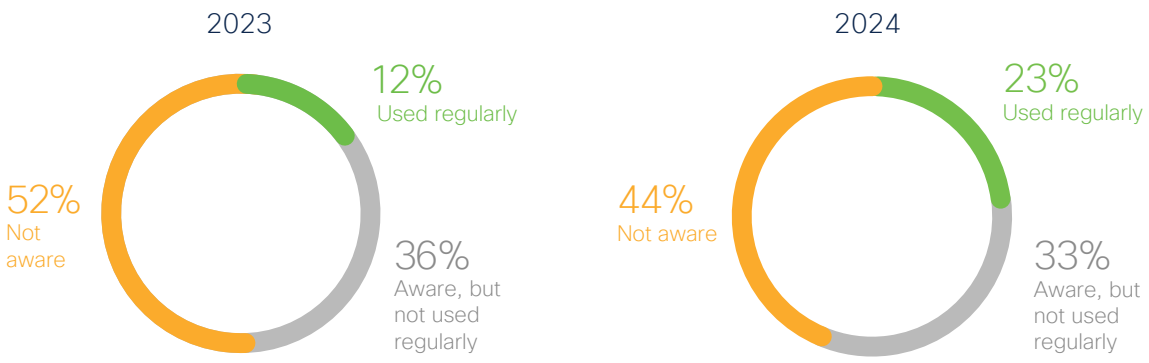


Source: Cisco 2024 Consumer Privacy Survey

4. Generative AI

Today's Generative AI (Gen AI) applications 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 during the past 18 months, and survey results from this year and last provide an early snapshot of its use and some of the potential risks and challenges. As of June 2024, when our survey was conducted, 23% of respondents described themselves as regular users of Gen AI, almost double compared to last year. See Figure 18.

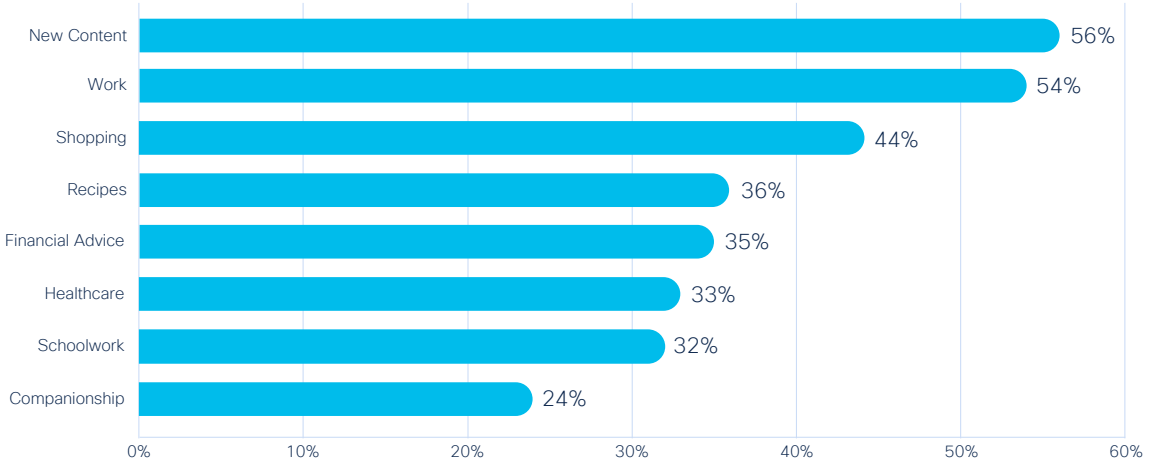
Figure 18. Awareness and Gen AI use



Source: Cisco 2024 Consumer Privacy Survey

For these regular users, the top Gen AI applications were creating new content (56%) and work-related tasks (54%), followed by shopping, recipes, and financial advice. See Figure 19.

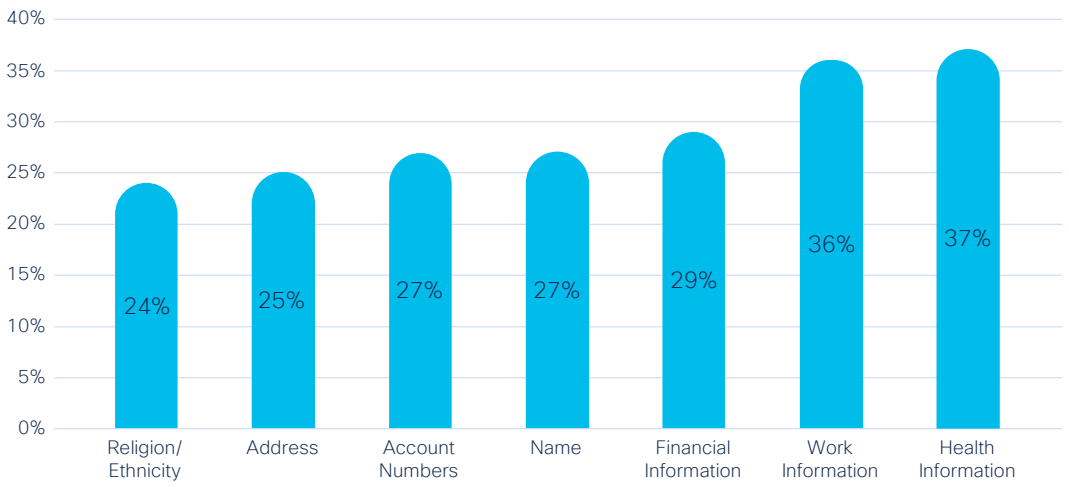
Figure 19. Top Gen AI uses



Source: Cisco 2024 Consumer Privacy Survey

In terms of the type of data they are entering, 37% of respondents said they have submitted health information, 36% have entered work information, and 24% to 29% of users have provided financial information, account numbers, and religion/ethnicity. These categories of data could include personal or confidential information that would be problematic if the Gen AI applications were to share the data publicly or with competitors. This is also the type of personal data consumers are taking actions to protect when used outside of Gen AI applications. See Figure 20.

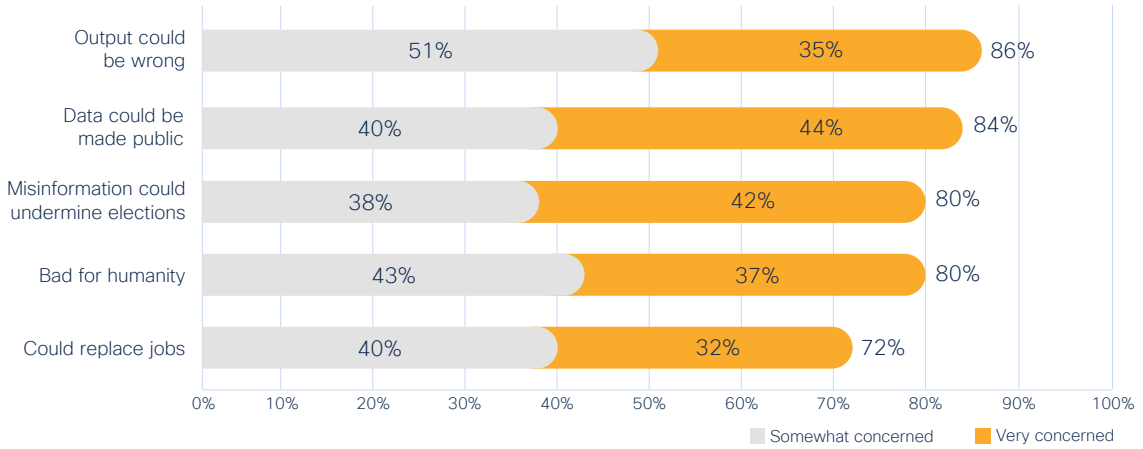
Figure 20. Information types entered in Gen AI tools by users



Source: Cisco 2024 Consumer Privacy Survey

Gen AI users seem to be highly aware of the individual and societal risks of this innovative technology if it is not used with appropriate controls and protections. Eighty-six percent of respondents said they would be "Somewhat Concerned" or "Very Concerned" the data could be wrong, and 84% were concerned their data could be shared. In addition, 80% were concerned about Gen AI potentially being bad for humanity, and 72% were concerned that Gen AI would replace jobs currently done by humans. See Figure 21.

Figure 21. Risk concerns with Gen AI



Source: Cisco 2024 Consumer Privacy Survey

There are a variety of ways to minimize the risks of Gen AI, and many of the regular Gen AI users in our survey indicated they were taking action. Fifty-one percent said they check other sources of information to be sure the Gen AI output is correct. Forty-five percent indicated they use a safe Gen AI tool (perhaps supplied by their employer) where the information would not be shared publicly, and the same percentage said they refrain from entering personal or confidential information into Gen AI applications. See Figure 22.

Figure 22. Reducing risk when using Gen AI

Source: Cisco 2024 Consumer Privacy Survey

Conclusion and Recommendations

This shift towards a more privacy-conscious consumer base represents both a challenge and an opportunity for organizations looking to foster trust. As the digital landscape continues to evolve, understanding and adapting to these consumer trends will be crucial for businesses aiming to maintain a competitive edge.

With the strong correlation between consumer awareness of privacy laws and consumer confidence, transparency will continue to play an important role in building trust. Organizations should help educate individuals about privacy laws and their rights, share how and where consumers can get more information, and how they can take necessary action to protect their own privacy. And as the use of Gen AI becomes more pervasive, organizations can earn and build consumer confidence by enacting appropriate governance and controls.

While the percentage of Privacy Actives continues to grow, it sits well below half of the surveyed population. There are several steps consumers can take to play a more active role in protecting their privacy:

1. Learn about your privacy rights and the privacy laws in your country.

2. Understand how your data is being used and who it may be shared with when you provide it to organizations and ask questions if you need more information.

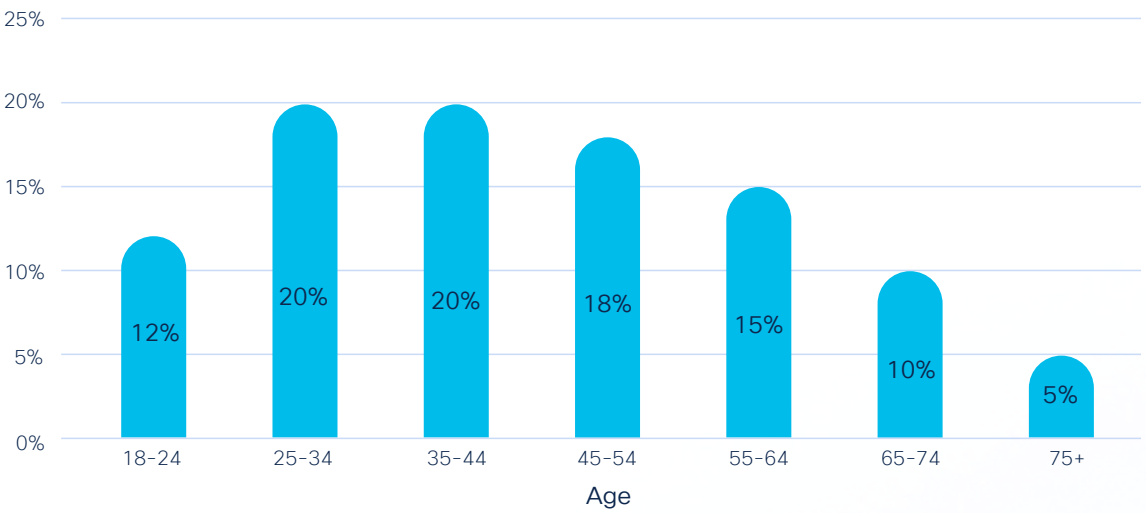
3. Take actions to protect your data by updating your privacy settings periodically, turning off home assistants, and using multi-factor authentication, among other noted actions.

4. Help those around you become Privacy Actives – notably older consumers who are less aware of their privacy rights – and understand how their data is being used and what measures they can take to protect themselves.

5. Be mindful when using Gen AI tools, understand the power and limitations of the tools being used, and refrain from entering personal or confidential information.

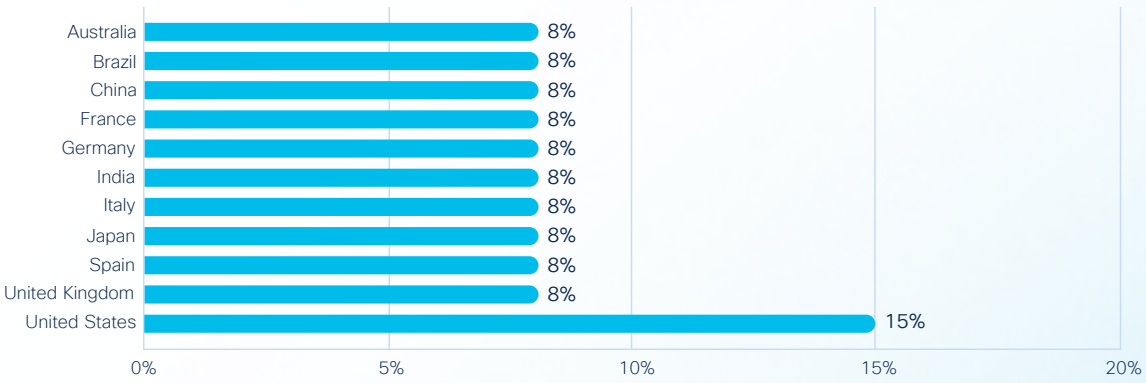
Appendix

Demographics of survey respondents, by age



Source: Cisco 2024 Consumer Privacy Survey

Demographics of survey respondents, by geography



Source: Cisco 2024 Consumer Privacy Survey

Helping organizations meet consumers' standards of trust

As customers set their standards of trust, Cisco continues to listen, learn, and evolve to meet those standards, prioritizing trustworthiness, transparency, and accountability throughout our holistic approach to security and privacy.

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, emerging and evolving technologies, and data regulations will impact privacy for organizations and consumers over time.

Cisco also publishes Privacy Data Sheets and Privacy Data Maps for its major products and services, enabling anyone interested to understand what personal data is used, who has access to it, and how long it is retained. Our Responsible AI Principles and Framework show how these principles and practices form our broad AI governance framework. And the Cisco Purpose Report and ESG Reporting Hub offer relevant resources related to how we prioritize trustworthiness, transparency, and accountability in our environmental, social, and governance (ESG) initiatives.

This research and other privacy and security-related content are available on the Cisco Trust Center.

About the cybersecurity report series

Cisco publishes a series of research-based, data-driven studies to inform, educate, and provide recommendations on security and privacy-related topics. 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 across the security industry, the reports include the Cisco Cyber Threat Trends Report, Security Outcomes Report, Duo Trusted Access Report, and Cisco Cybersecurity Readiness Index, and others published throughout the year.

For more information and to access all the reports, visit: www.cisco.com/go/securityreports.