CISCO
SECURE

The bridge to possible

Building Consumer Confidence Through Transparency and Control

CISCO 2021 | CONSUMER PRIVACY SURVEY

Table of Contents

Introduction

Protecting privacy continues to be a critical issue for individuals, organizations, and governments around the world. Eighteen months into the COVID-19 pandemic, our health information and vaccination status are needed more than ever to understand the virus, control the spread, and enable safer environments for work, learning, recreation, and other activities. Nonetheless, people want privacy protections to be maintained, and they expect organizations and governments to keep their data safe and used only for pandemic response. Individuals are also increasingly taking action to protect themselves and their data. This report, our third annual review of consumer privacy, explores current trends, challenges, and opportunities in privacy for consumers.

The report draws upon data gathered from a June 2021 survey where respondents were not informed of who was conducting the study and respondents were anonymous to the researchers. Respondents included 2600 adults (over the age of 18) in 12 countries (5 Europe, 4 Asia Pacific, and 3 Americas).[1] Participants were asked about their attitudes and activities regarding companies' use of their personal data, level of support for COVID-19 related information sharing, awareness and reaction to privacy legislation, and attitudes regarding artificial intelligence (AI) and automated decision making.

The findings from this research demonstrates the growing importance of privacy to the individual and its implications on the businesses and governments that serve them. Key highlights of this report

1. Consumers want transparency and control with respect to business data practices – an increasing number will act to protect their data
2. Privacy laws are viewed very positively around the world, but awareness of these laws remains low
3. Despite the ongoing pandemic, most consumers want little or no reduction in privacy protections, while still supporting public health and safety efforts
4. Consumers are very concerned about the use of their personal information in AI and abuse has eroded trust

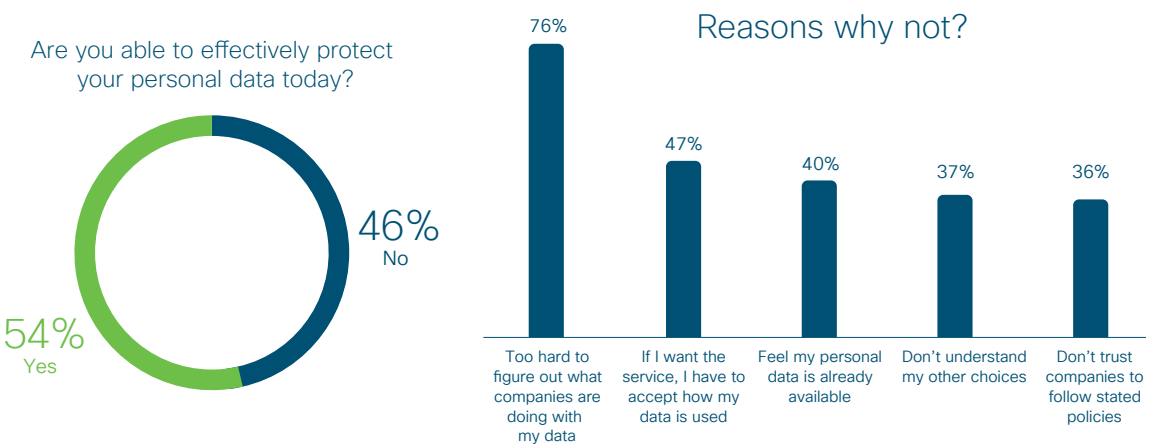
[1] *Australia, Brazil, China, France, Germany, Italy, India, Japan, Mexico, Spain, UK, and US*

The Results

1. Consumers want transparency and control with respect to business data practices – an increasing number will act to protect their data

Nearly half (46%) of our survey respondents feel they are unable to effectively protect their data today. This is despite having over 140 national and multinational privacy laws around the world, regulations requiring privacy notices and choice for consumers, and security technologies to help prevent unauthorized access. The main reason consumers don't feel safe is the lack of transparency and clarity with respect to business data practices. Seventy-six percent (76%) told us that it's too hard for them to understand what's going on and how their information is being used. What companies are actually doing with their data remains a mystery. See Figure 1.

Figure 1. Ability of Consumers to Protect Their Data.

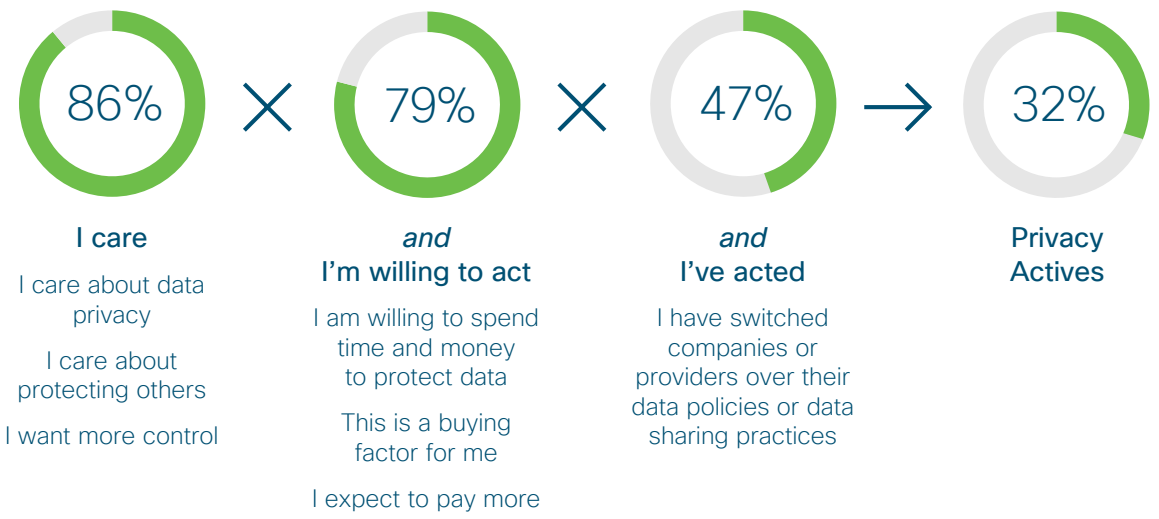


Source: Cisco Consumer Privacy Study - 2021

The Results

In response, more consumers are taking action to protect themselves and their data. Over the past three 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 over their data practices or policies. Among this year's respondents, we found that 32% met the test for Privacy Actives, up from 29% a year ago. See Figure 2.

Figure 2. The Privacy Actives Segment

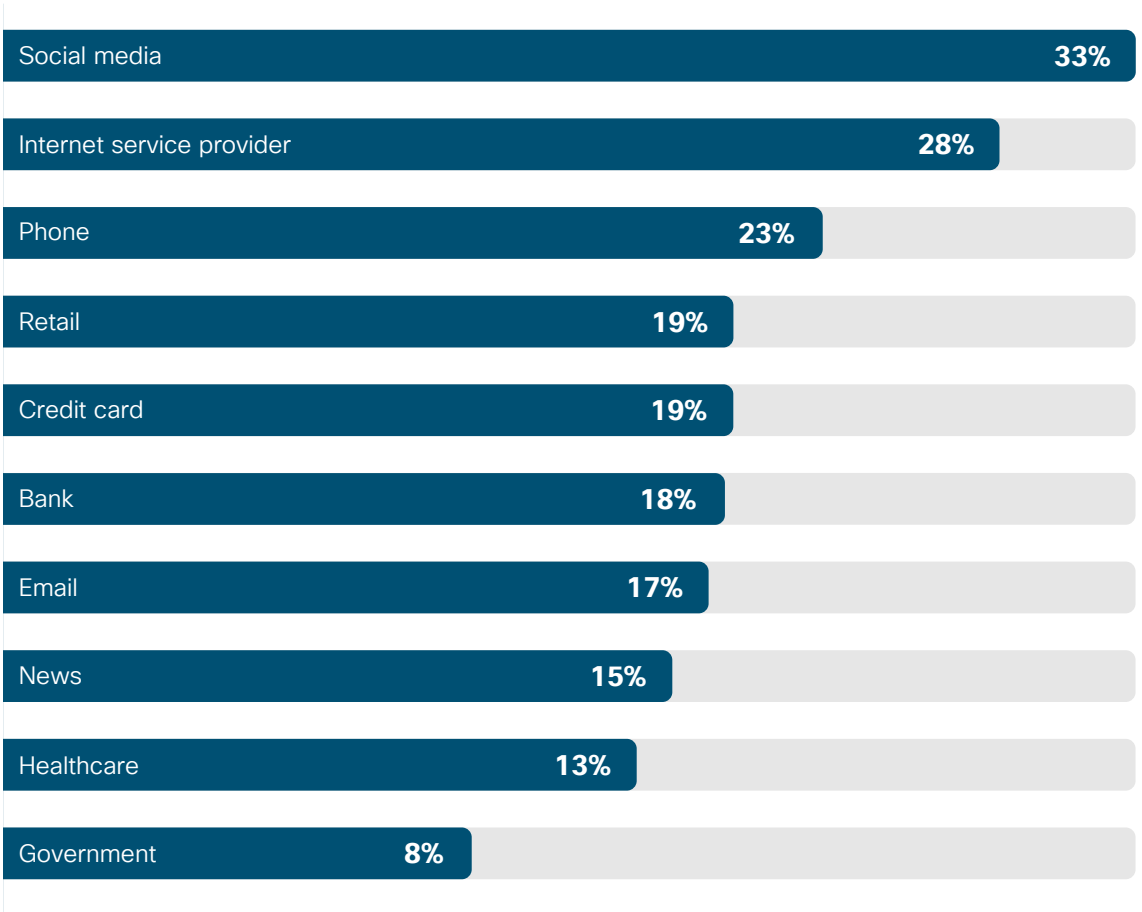


Source: Cisco Consumer Privacy Study - 2021

The Results

These consumers have terminated relationships with both online and traditional companies over data privacy concerns. A third (33%) left social media companies and 28% left Internet Service Providers (ISPs), but they also left other types of companies. Nineteen percent terminated a relationship with a retailer, 19% with a credit-card provider, and 18% with a bank or financial institution. See Figure 3. It is also interesting that nearly half (47%) of these consumers left relationships that were "significant" (defined by its breadth and/or length of time the individual had been a customer). Consumer's concerns seem to be extending to any company that makes use of their data, even to those they have known for years.

Figure 3. Types of Companies Left by Privacy Actives

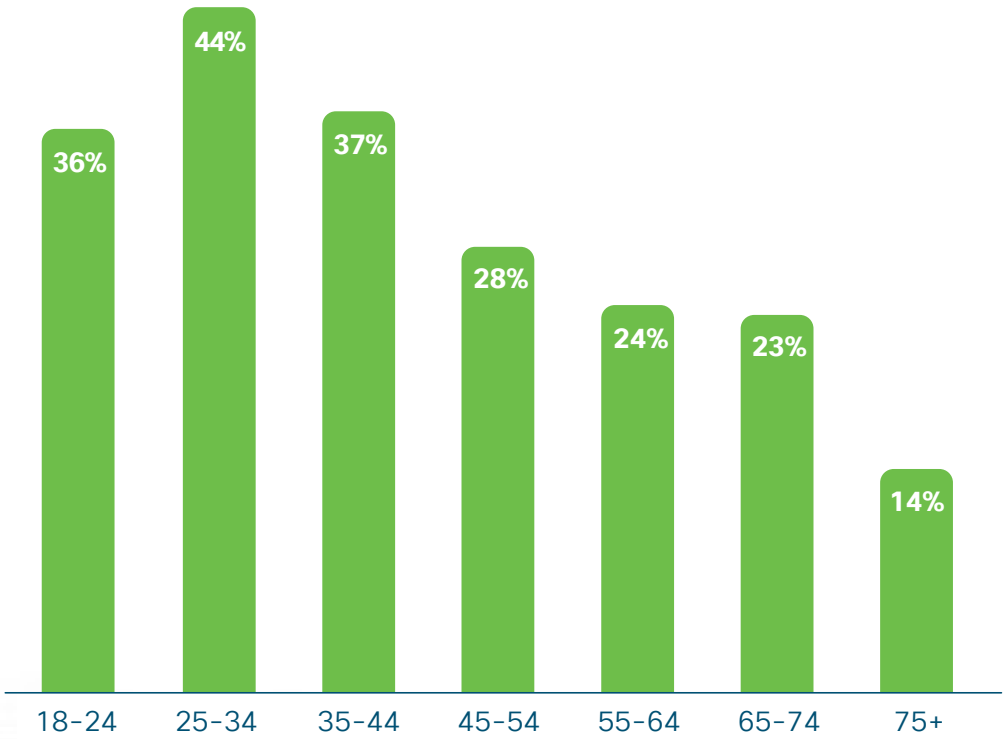


Source: Cisco Consumer Privacy Study - 2021

The Results

From a generational perspective, the Privacy Actives segment makes up an even larger share of younger consumers, including 44% of those between the ages of 25 and 34, declining to only 14% of those over age 75. See Figure 4. If these consumers continue their behaviors in the coming years, we can expect to see a steady increase in the number who are willing to act to protect their privacy over time..

Figure 4. The Privacy Actives Segment, by Age

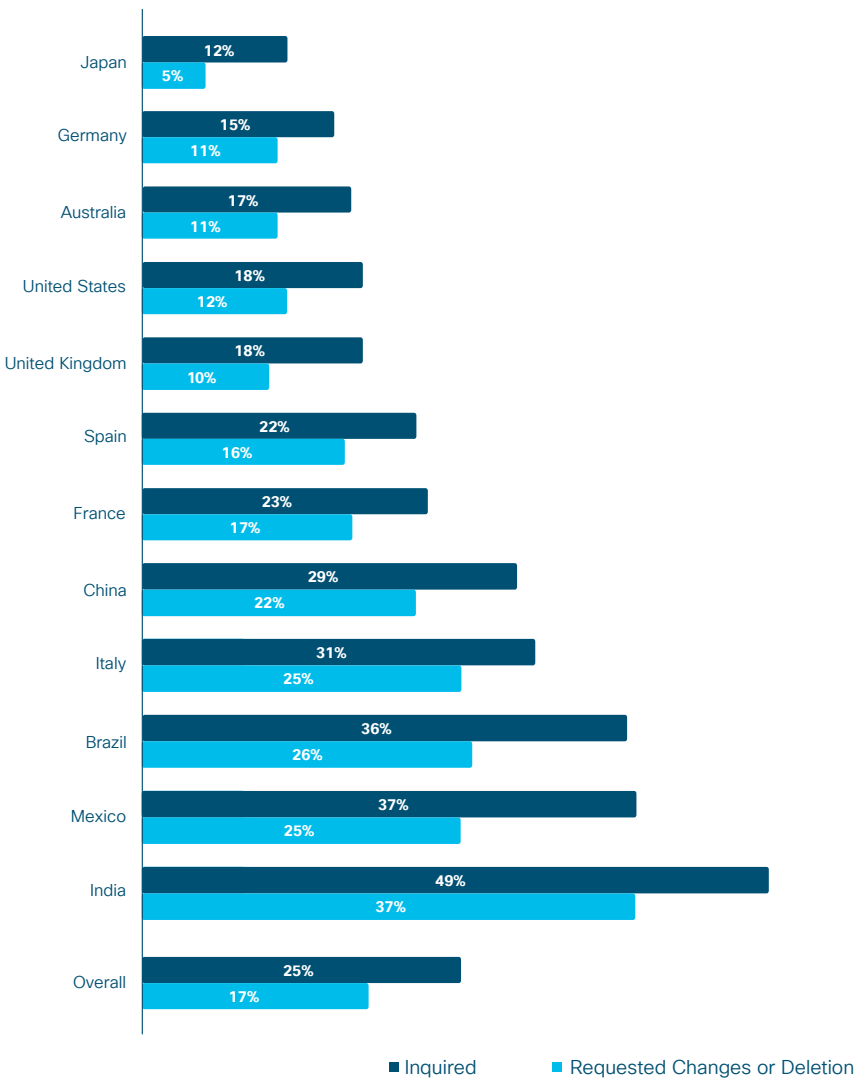


Source: Cisco Consumer Privacy Study - 2021

The Results

Another area where consumers are acting to protect their data is in inquiring about the data companies have about them, and potentially getting the data corrected or deleted. The European Union's (EU's) General Data Protection Regulation (GDPR) has received the most attention over the years and set forth a framework for data subject access requests (DSAR). Many privacy laws today have similar requirements around transparency and individual control that enable consumers to take such actions. Among all survey respondents, 25% said they have made such an inquiry and 17% said they have also requested the data be changed or deleted. These laws vary by country, and it is interesting that India had the largest percentage of respondents who had made inquiries into their data (49%), followed by Mexico (37%) and Brazil (36%). See Figure 5.

Figure 5. Consumers Who Inquired or Requested Changes or Deletion to their Data, by Country

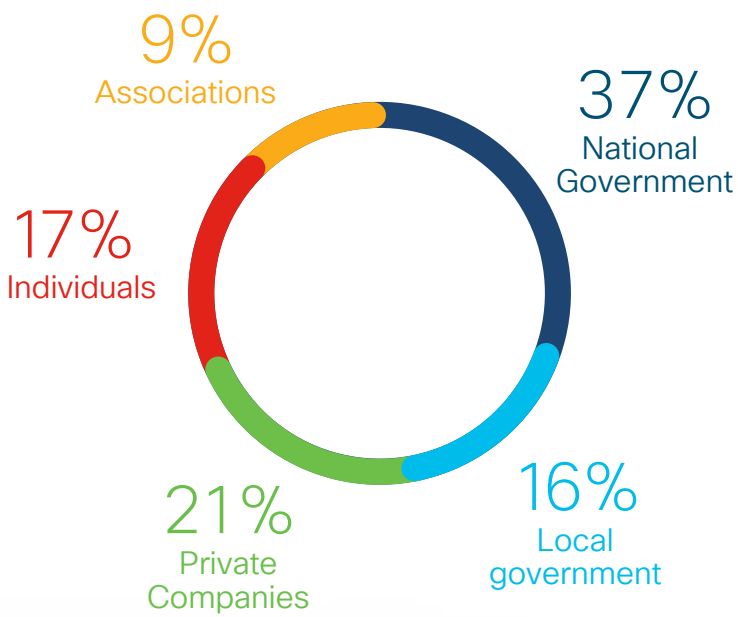


Source: Cisco Consumer Privacy Study - 2021

2. Privacy laws are viewed very positively around the world, but awareness of these laws remains low

Survey respondents were asked how much responsibility various entities (e.g., federal government, local government, companies, industry associations, or the individuals) should have for protecting individuals' personal data. Over half (53%) said national or local government should play the primary role, 21% said private companies should play this lead role, and 17% said the individuals themselves should be primarily responsible for protecting their data. See Figure 6. Many consumers don't trust private companies to follow their own policies and treat data responsibly, so they look to the government to provide enforcement and protections. While consumers may accept responsibility for doing what they can, they also recognize that their power is limited.

Figure 6. Entities Who Should Have Lead Responsibility for Protecting Data Privacy

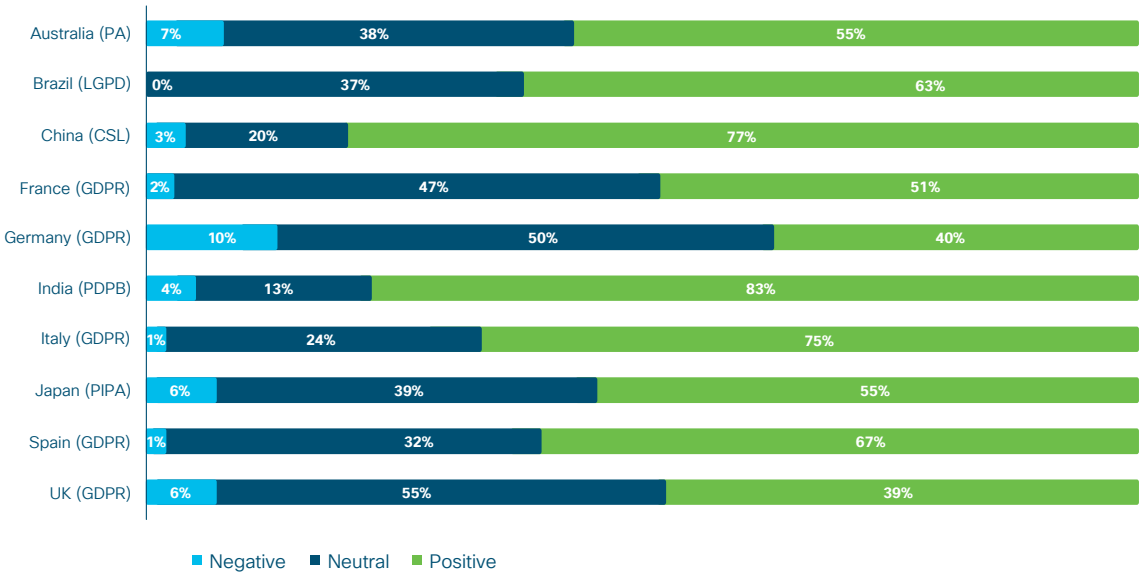


Source: Cisco Consumer Privacy Study - 2021

The Results

Given the desire for a strong governmental role in protecting personal data, consumers view privacy laws and regulations very favorably. In this year's survey, we tested reactions to GDPR (among EU respondents) as well as the specific privacy laws in other countries: the Privacy Act 1988 (PA) in Australia, Cyber Security Law (CSL) in China, the Personal Data Protection Bill (PDPB) in India, Lei Geral de Proteção de Dados Pessoais (LGPD) in Brazil, and Personal Information Protection Act (PIPA) in Japan. Among respondents in these countries who were aware of the laws, 60% felt they had a positive impact, up from 53% last year. Only 4% felt they had a negative impact, down from 6% last year. Across each of the individual countries, the sentiment was quite positive, including India (82% positive, 4% negative) and China (77% positive, 3% negative). Among the European countries, the percentage of positive responses for GDPR ranged from 40% (Germany) to 75% (Italy). See Figure 7.

Figure 7. Impact of Privacy Laws, by Country

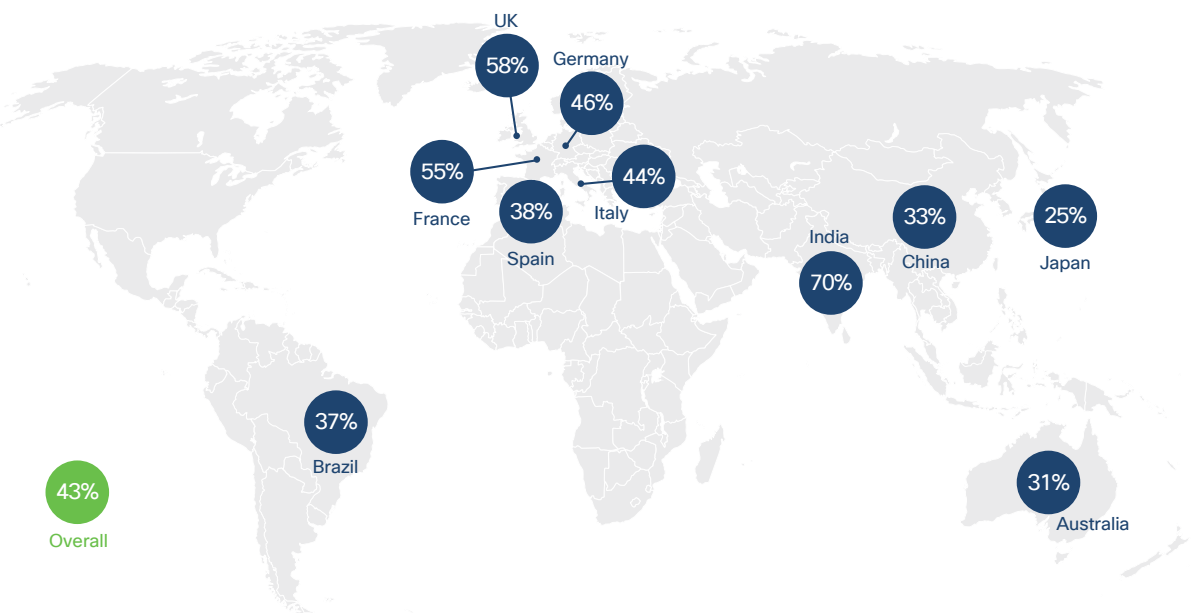


Source: Cisco Consumer Privacy Study - 2021

The Results

Unfortunately, public awareness of these laws continues to be relatively low. Overall, only 43% of respondents in the countries with national or multinational privacy laws were aware of these laws. GDPR has been in place for over three years and awareness ranges only from 38% (Spain) to 58% (UK). Awareness in other countries with national privacy laws (Japan, Brazil, Australia, and China) is similarly low, ranging from 25% to 33%. The clear leader, and notable exception, is India where 70% of respondents are aware of the PDP Bill. See Figure 8.

Figure 8. Awareness of National or Multi-National Privacy laws, by Country



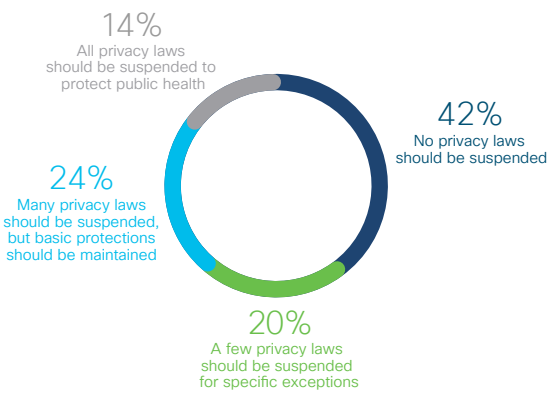
Source: Cisco Consumer Privacy Study - 2021

Awareness of privacy laws has several benefits beyond compliance. First, it builds consumer confidence. 69% of survey respondents who were aware of privacy laws felt they can adequately protect their data today, versus only 44% of those who were unaware of these laws. In addition, 51% of those aware of the privacy laws said they were comfortable sharing their data with companies or services they use, versus 37% of those who were unaware. Finally, knowledgeable consumers take a more active role in protecting their data. 47% of those aware of the privacy laws have inquired about their personal data at companies, versus only 10% of those who were unaware of the laws. Given these results, it would be beneficial to governments, companies, and individuals if more people would be made aware of the privacy laws and protections that are already in place today.

3. Despite the ongoing pandemic, most consumers want little or no reduction in privacy protections, while still supporting public health and safety efforts.

The COVID-19 pandemic has brought new challenges to privacy during the past 18 months. The rapid shift to remote working challenged organizations to provide tools that keeps data safe, and the ongoing need for personal health, location and proximity information, and contacts has forced organizations and governments to try to balance the need to control the virus and keep people safe while respecting privacy. Consumers believe safety can be achieved, but with little or no relaxation of privacy protections. Among survey respondents, 42% indicated they want no reduction in privacy protections despite the pandemic, and another 20% indicated they want only limited reductions. See Figure 9.

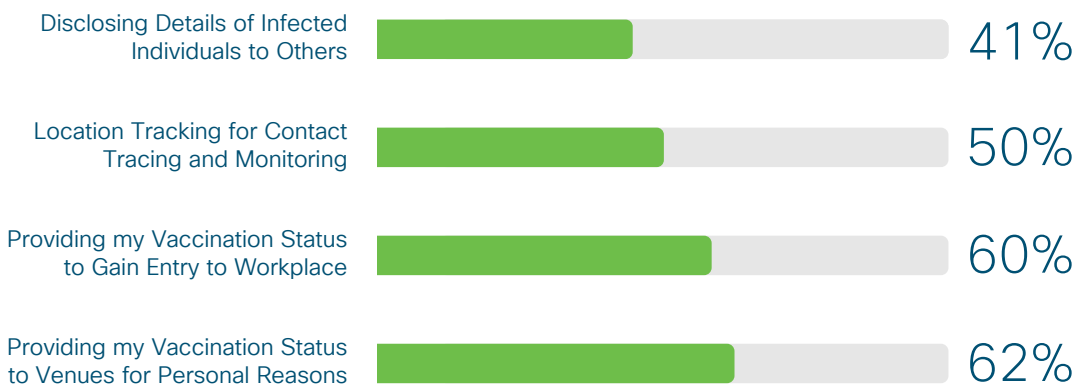
Figure 9. Changes to Privacy Laws During Pandemic or National Emergency



Source: Cisco Consumer Privacy Study - 2021

In considering various policies that might help control the virus and create safe environments for work, education, recreation, and other activities, consumers offer mixed support. Only 41% support disclosing any information about infected individuals and 50% support location tracking for contact tracing to help people know if they might have been exposed. When it comes to requiring vaccination status to gain entry to work or social venues, consumers are more supportive (60% and 62%, respectively). See Figure 10.

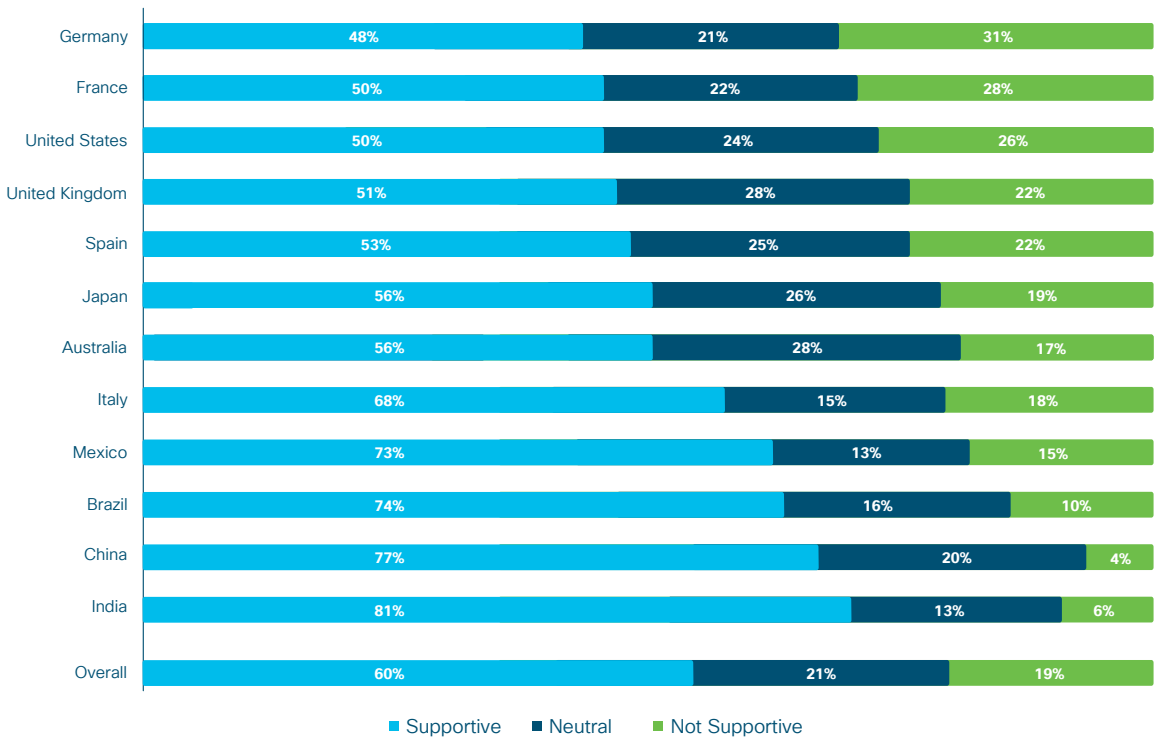
Figure 10. Support for Covid-Related Sharing of Personal Information



Source: Cisco Consumer Privacy Study - 2021

As employers grapple with "back-to-office" requirements, it is interesting to see how this support for requiring vaccination status varies around the world. Many of the European countries, along with the United States, were the least supportive. This includes Germany (48% in favor, 31% against) and France (50% in favor, 28% against). At the other end of the spectrum were a few of the countries in Asia Pacific, including India (81% in favor) and China (77% in favor). See Figure 11

Figure 11. Support for Sharing Vaccination Status to Enter Workplace, by Country



Source: Cisco Consumer Privacy Study - 2021

4. Many consumers are concerned about the use of their personal information in Artificial Intelligence (AI) and automated decision making, and abuse has eroded trust

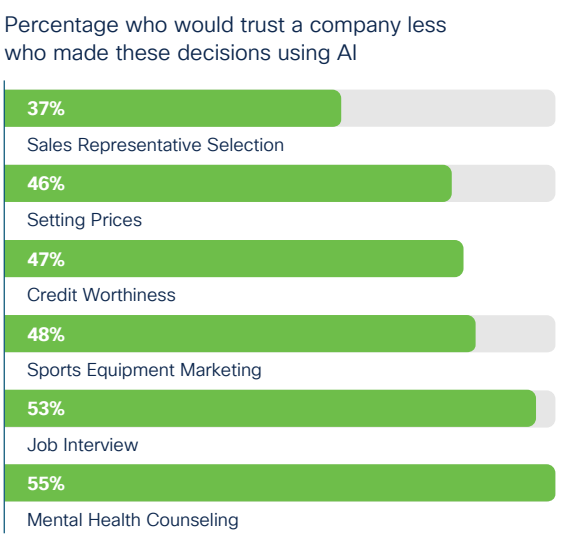
Artificial Intelligence has the potential to use customer data in ways that create more efficient and personalized experiences for consumers, and 40% of survey respondents recognize that AI can be useful in improving their lives – from shopping to healthcare. At the same time, the majority (72%) of respondents believe organizations have a responsibility to only use AI responsibly and ethically. While there may be differing views of what constitutes good ethical behavior, consumers value transparency in how their data is used (see Section 1 above).. Not surprisingly, over half (56%) of survey respondents are concerned about how businesses are using AI today. AI decision-making can be particularly hard for many to understand.

We tested respondents' reactions to six different use cases where personal data could be involved in various types of automated decision-making that would impact the consumer. See Figure 12. For each use case, we asked whether consumers would trust a company less if they found out the company was using AI for this activity. At the high end, 55% said they would trust a company less who used AI to make mental health recommendations. Even at the low end, 37% said they would trust a company less who used AI to select a sales representative to assist them in the store or online. See Figure 12. These results suggest organizations should be particularly careful about any use of AI in decision-making that affects individuals directly. More work needs to be done to get consumers comfortable with AI technology and uses – starting with transparency.

Figure 12. AI Use Cases and Loss of Trust

Use cases tested

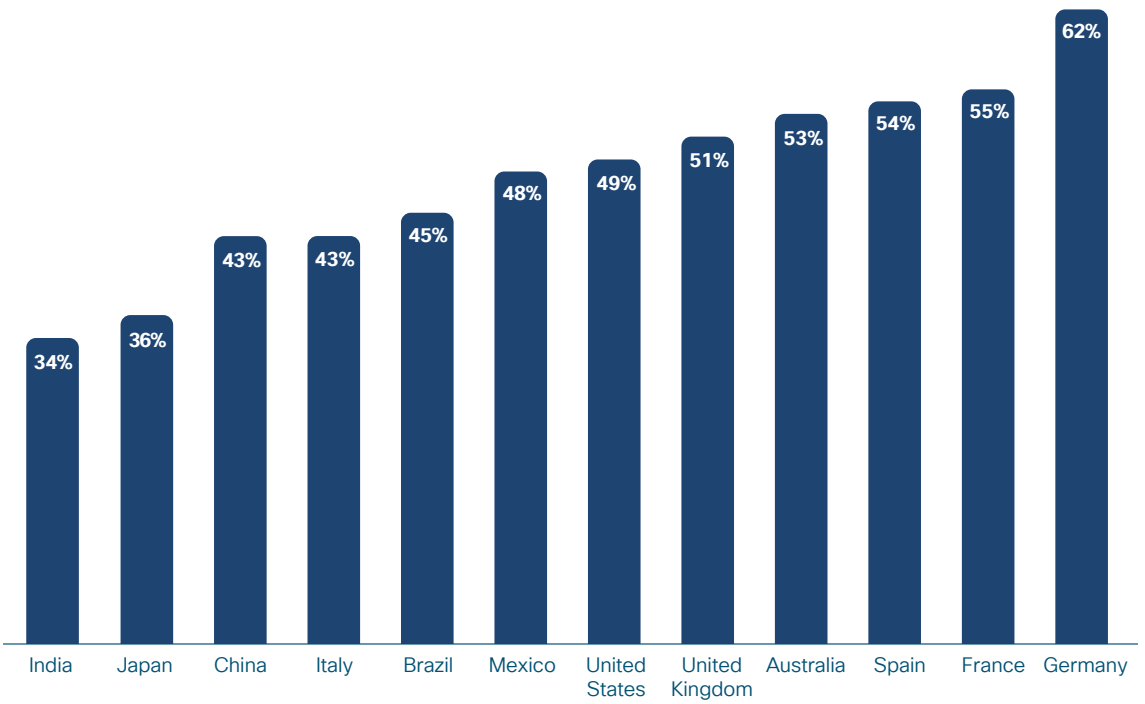
- To better match a sales representative to you when you call or visit their store
- To set the prices for their products and services
- To infer your credit-worthiness and decide whether to grant you a loan
- To infer whether you participate in sports, and market sports equipment to you
- To infer your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



Source: Cisco Consumer Privacy Study - 2021

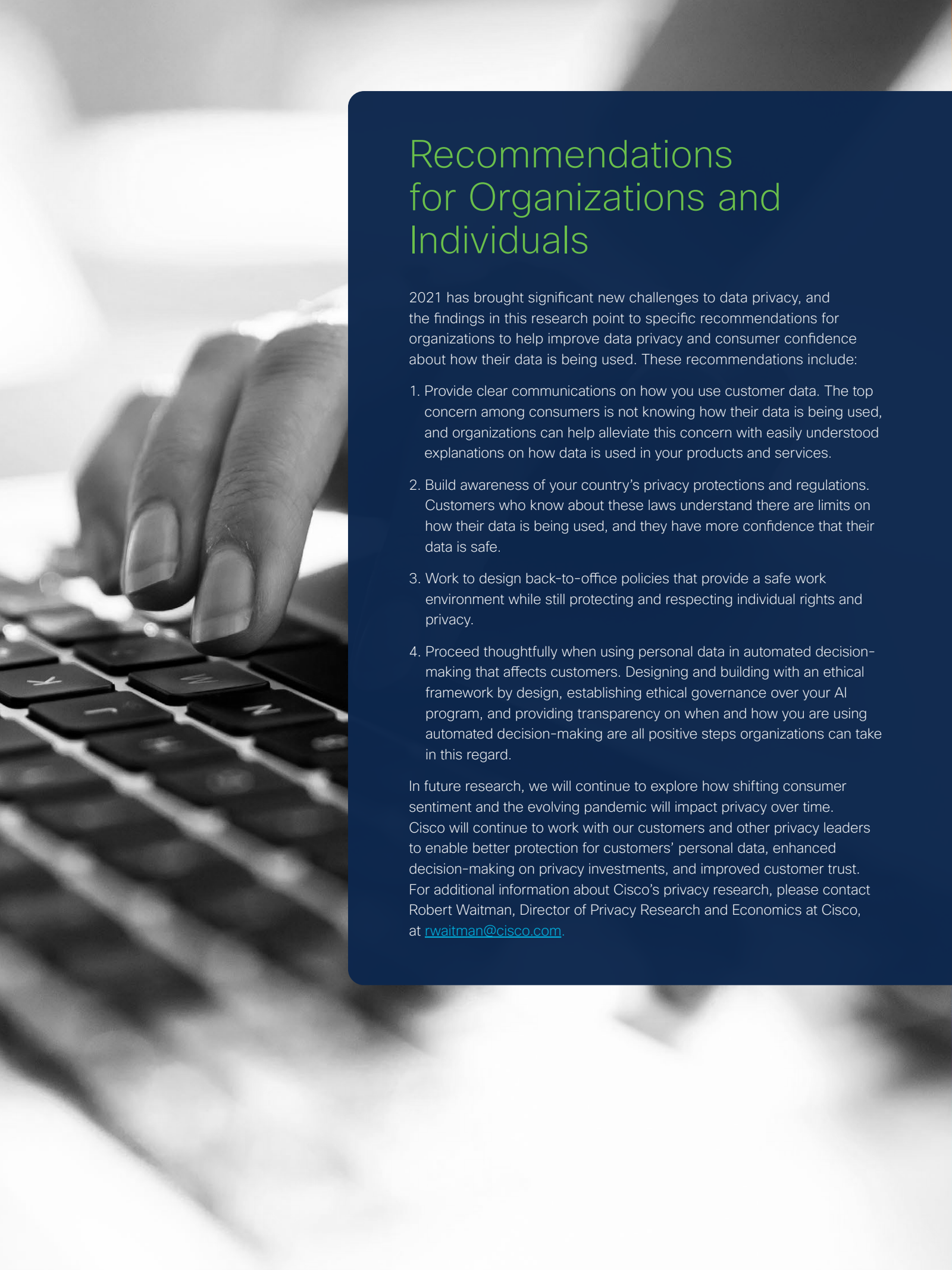
It is also interesting to see how this potential erosion of trust varies across different geographies. For each country, we looked at the percentage of respondents indicating they would trust the company less for each of the 6 use cases, and we averaged them. Among respondents in Germany, 62% on average indicated a loss of trust from the AI use cases. At the low end, only 34% of respondents on average in India indicated a loss of trust from the same use cases. See Figure 13. Organizations in all these countries should be careful about their use of AI, but especially where we see the higher numbers as in Germany, France, Spain, and Australia.

Figure 13. Average Loss of Trust from AI Use Cases, by Country



Source: Cisco Consumer Privacy Study - 2021

With customer trust at stake, organizations will need to consider deploying a variety of processes and tools to help customers better understand and be more comfortable with the use of AI-based decisions that affect them. Some examples include: developing and publishing easy-to-understand information regarding how AI tools are used, appointing a data ethics officer, requiring data ethics training for data scientists, adopting a set of data ethics principles to guide projects, and establishing internal or external data ethics advisory committees. An increase in transparency and accountability will likely increase consumers' comfort with how AI is used and minimize the potential negative impact on trust. We plan to explore these ideas further in future research.



Recommendations for Organizations and Individuals

2021 has brought significant new challenges to data privacy, and the findings in this research point to specific recommendations for organizations to help improve data privacy and consumer confidence about how their data is being used. These recommendations include:

1. Provide clear communications on how you use customer data. The top concern among consumers is not knowing how their data is being used, and organizations can help alleviate this concern with easily understood explanations on how data is used in your products and services.
2. Build awareness of your country's privacy protections and regulations. Customers who know about these laws understand there are limits on how their data is being used, and they have more confidence that their data is safe.
3. Work to design back-to-office policies that provide a safe work environment while still protecting and respecting individual rights and privacy.
4. Proceed thoughtfully when using personal data in automated decision-making that affects customers. Designing and building with an ethical framework by design, establishing ethical governance over your AI program, and providing transparency on when and how you are using automated decision-making are all positive steps organizations can take in this regard.

In future research, we will continue to explore how shifting consumer sentiment and the evolving pandemic will impact privacy over time. Cisco will continue to work with our customers and other privacy leaders to enable better protection for customers' personal data, enhanced decision-making on privacy investments, and improved customer trust. For additional information about Cisco's privacy research, please contact Robert Waitman, Director of Privacy Research and Economics at Cisco, at rwaitman@cisco.com.

About the Cybersecurity Report Series

Throughout the past decade, Cisco has published a wealth of definitive 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 organizational implications, as well as leading and proactive practices to defend against cyber crimimals. In our new approach to thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the banner Cisco Cybersecurity Series. 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 of threat researchers and innovators in the security industry, the reports in the 2021 series include the Data Privacy Benchmark Study, the Threat Report, and the Security Outcomes Study, with others published throughout the year. For more information, and to access all the reports and archived copies, visit www.cisco.com/go/securityreports

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published date here RPT_06_2020

cisco SECURE


cisco
SECURE