



Protecting Data Privacy to Maintain Digital Trust

The Importance of Protecting Data Privacy
During the Pandemic and Beyond

Contents

Introduction	3
The Results	4
1. COVID-19 and remote working have created a set of new privacy challenges, but consumers continue to want their information to be protected and support only limited exceptions	4
2. One-Third of Consumers are Privacy Actives who have stopped doing business with organizations over Data Privacy concerns	7
3. Consumers expect their governments to take the lead in protecting their data, and residents of all countries surveyed view their privacy laws very favorably	11
4. Consumers want more transparency on how their data is being used	14
Recommendations for Organizations and Individuals	16
About the Cybersecurity Report Series	17

Introduction

Protecting one's data privacy has never been more critical as the COVID-19 pandemic has created dramatic changes to how we work, live, play and learn in 2020. Governments need personal health information to control the spread of the virus, and organizations need safe tools for remote working and learning. Consumers are often caught in the middle, wanting to participate and help, but are concerned that their interactions and personal information may not be protected and secure. This study, our second-annual look at consumer privacy concerns, explores these challenges for organizations that are trying to maintain digital trust with their customers, along with the evolving privacy landscape and its impact on consumers.

This report draws upon data gathered from a June 2020 survey where the respondents were not informed of who was conducting the study and respondents were anonymous to the researchers. Respondents included over 2600 adults (over age 18) in 12 countries¹ including five in Europe, four in Asia Pacific, and three in the Americas. Participants were asked about their attitudes and activities regarding protecting their personal data, the impact of the COVID-19 pandemic, their comfort level with potential new uses of their data, and the impact of privacy regulations.

The findings from this research, along with Cisco's previously published privacy research, demonstrate the growing importance of privacy to the individual and its implications on the businesses who serve them. Highlights of this report include the following:

1. COVID-19 and remote working have created new privacy challenges, but consumers continue to want their information protected and support only limited exceptions
2. One-third of consumers are "Privacy Actives" who have stopped doing business with organizations over data privacy concerns
3. Consumers expect their governments to take the lead in protecting their data, and residents of all countries surveyed view their privacy laws very favorably
4. Consumers want more transparency on how their data is being used

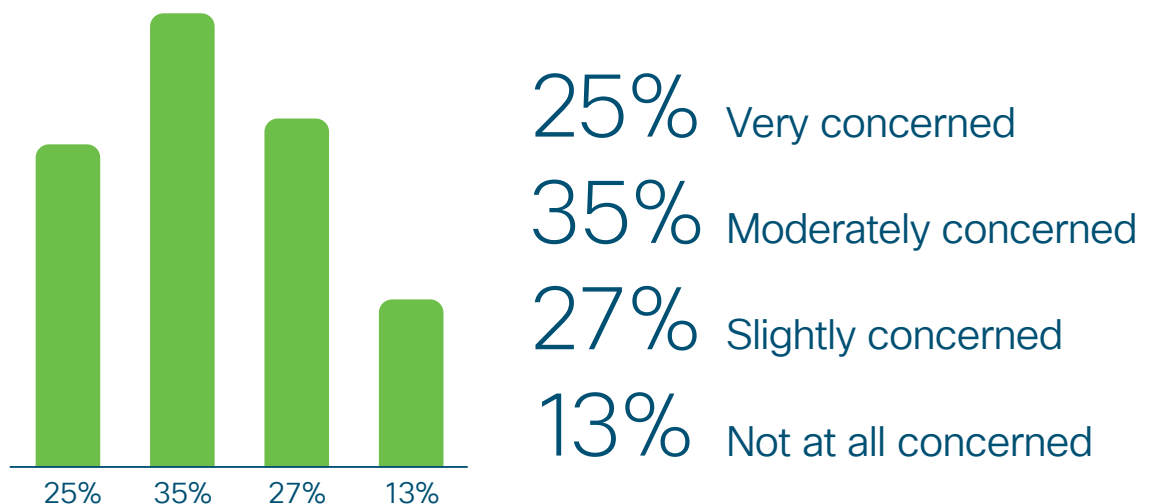
¹ *Australia, Brazil, China, France, Germany, Italy, India, Japan, Mexico, Spain, UK, and US.*

The Results

1. COVID-19 and remote working have created a set of new privacy challenges, but consumers continue to want their information to be protected and support only limited exceptions

The majority of people don't trust the digital tools they needed to use this year for remote interactions. The COVID pandemic has forced many changes on society, including a massive shift to remote working and an often-urgent need for personal health information to support and maintain public health. Among respondents in our June 2020 survey, a very large percentage (81%) indicated they were currently working or learning remotely. While some organizations had enabled remote interactions before the pandemic, many were challenged to find or develop the digital tools and scale needed to support this shift. People were asked to interact and share information remotely, and our survey indicates that they were not very confident that their data was properly protected. Specifically, among those who were working or learning remotely, 60% said they were moderately or very concerned about the privacy protections associated with the tools they were using to support these remote interactions. (See Figure 1.)

Figure 1. Level of Concern with Remote Working Tools. N=2115.

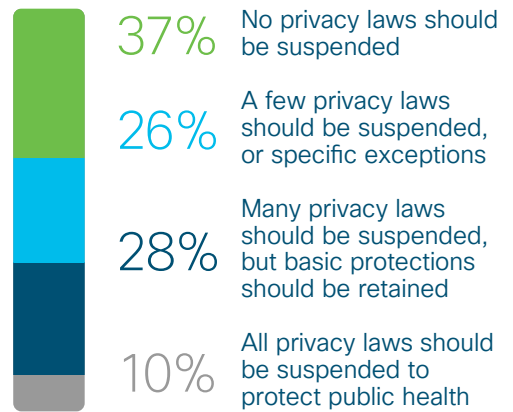


Source: Cisco Consumer Privacy Study - 2020

Consumers also have concerns about sharing their health information even during the pandemic.

Employers need personal health information to create a safe workplace, governments need this information to contain the disease, and researchers need this information to work on treatments and cures. In this year’s survey, we tested a number of propositions that weighed these needs against the need for data privacy, and most consumers want privacy laws maintained. More than a third of respondents said they wanted no relaxation of privacy laws due to the pandemic and another 26% supported only limited exceptions to privacy laws. Only 10% felt that privacy laws should take a back seat to the pandemic. (See Figure 2.)

Figure 2. Changes to Privacy Laws During Pandemic. N=2602.

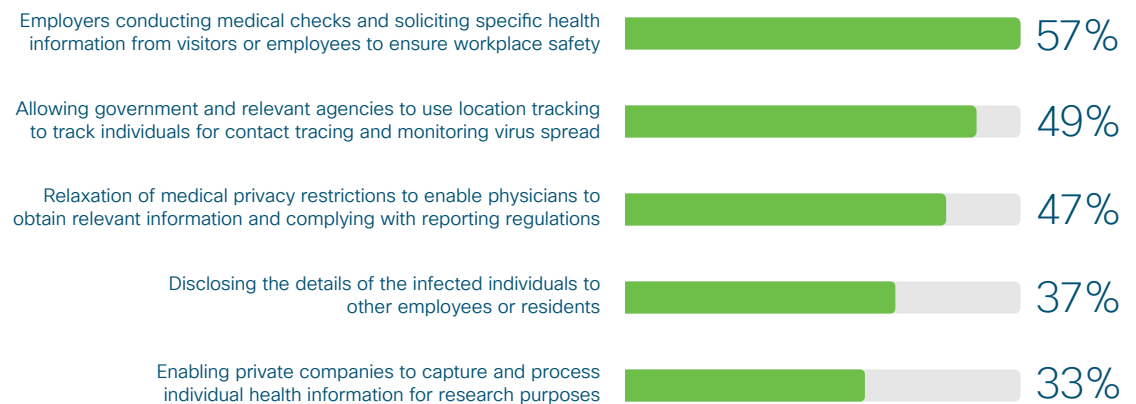


Source: Cisco Consumer Privacy Study - 2020

On specific and limited scenarios, consumers also had mixed feelings about sharing personal information even when it was needed for public health.

Over half (57%) supported employers requesting employee health information to ensure a safe workforce. However, slightly under half supported location tracking, only 37% supported disclosing information about infected individuals, and only a third supported sharing information with private companies for research purposes. (See Figure 3.)

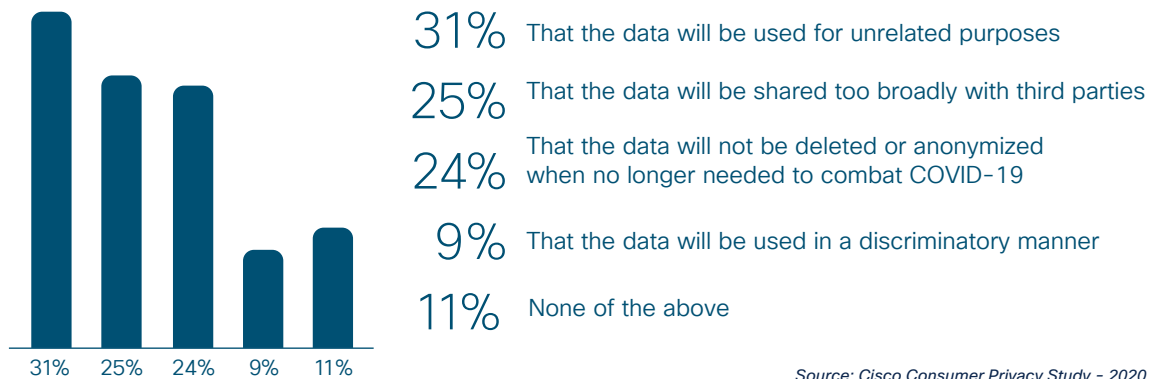
Figure 3. Level of Support for Data Sharing During Pandemic. N=2602.



Source: Cisco Consumer Privacy Study - 2020

Across all these scenarios, consumers expressed concern that their data would be used only for necessary and limited purposes. Specifically, their top concerns were that the data would be used for other unrelated purposes (31%), that the data would be shared too broadly with third parties (25%), and that the data would not be deleted or anonymized when it was no longer needed for this specific use (24%). (See Figure 4.) It is interesting to consider what protections or regulations might make consumers more confident in these scenarios; a topic for future research.

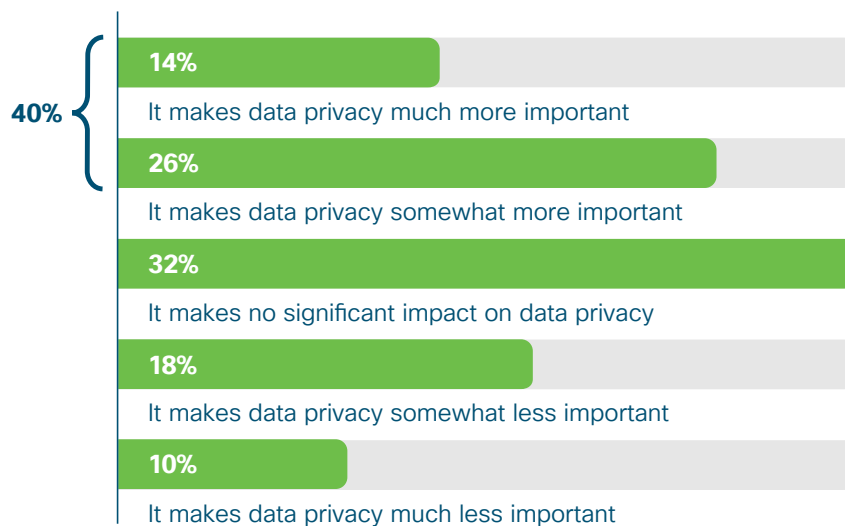
Figure 4. Top Privacy Concern About Data During Pandemic. N=2602.



Source: Cisco Consumer Privacy Study - 2020

It also appears that COVID’s impact on privacy may be long-lasting, as many responders felt the pandemic would make privacy even more important after the pandemic is over. Forty percent felt that the pandemic would strengthen the importance of privacy, compared with 32% who said it would stay about the same, and 28% who said it made privacy less important in the future. (See Figure 5.)

Figure 5. Long Term View of the Impact of the Pandemic on Privacy. N=2602.



Source: Cisco Consumer Privacy Study - 2020

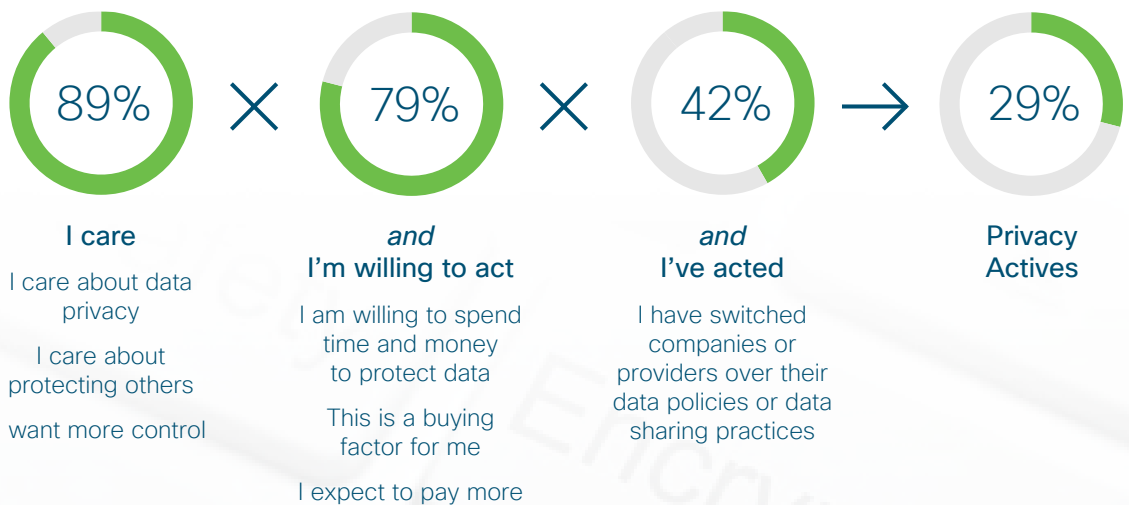
2. One-Third of Consumers are Privacy Actives who have stopped doing business with organizations over Data Privacy concerns

Until recently, many consumers felt they had little control over their personal information and little recourse against companies who were not protecting it.

The European Union's (EU) General Data Protection Regulation (GDPR) gave individuals greater rights to know what data companies had about them and, in some cases, the ability to get it modified or deleted. Many countries began considering and adopting their own privacy regulations, and today over 120 jurisdictions have privacy laws, often providing consumers with greater rights and the ability to protect their personal information.

Many consumers are also taking matters into their own hands. Over the past two years, we have been tracking a segment of consumers we called "Privacy Actives" – those who say they care about privacy, are willing to act to protect it, and have already acted by switching companies or providers over their data policies or practices. Among this year's respondents, we found that 29% of respondents met the test for Privacy Actives, confirming our similar result from a year ago.² (See Figure 6.)

Figure 6. The Privacy Actives Segment. N=2602.

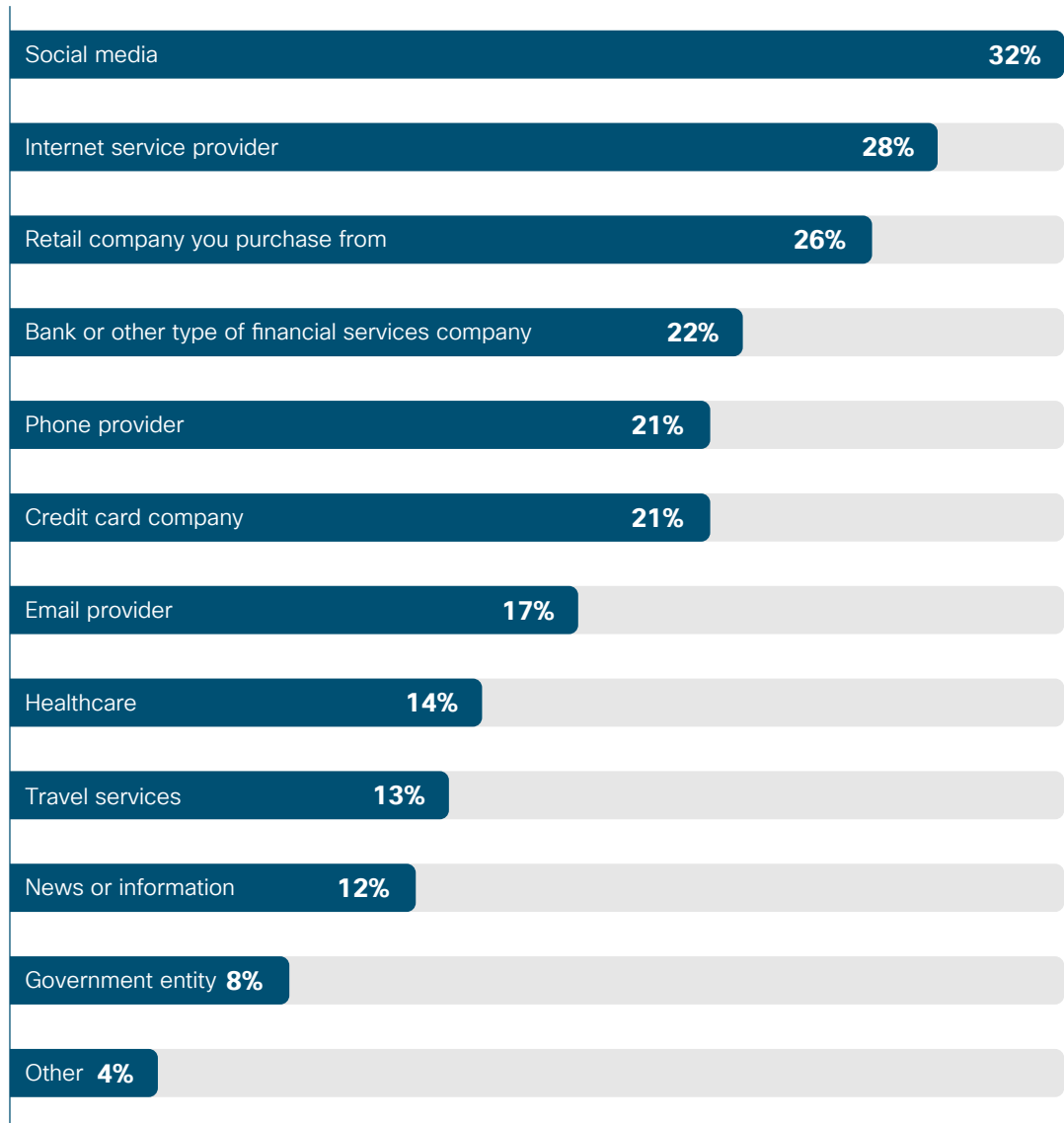


Source: Cisco Consumer Privacy Study - 2020

² Privacy Actives were 32% of respondents in last year's survey.

Interestingly, these consumers have stopped using both online and traditional companies over data privacy concerns. Thirty-two percent of Privacy Actives have left social media companies and 28% have left Internet Service Providers (ISPs), but many other businesses were impacted as well. Twenty-six percent of the Privacy Actives left retail companies, 22% left banks or other financial institutions, 21% left a phone provider, and 21% left a credit card company. (See Figure 7.)

Figure 7. Type of Companies "Left" by Privacy Actives. N=760.

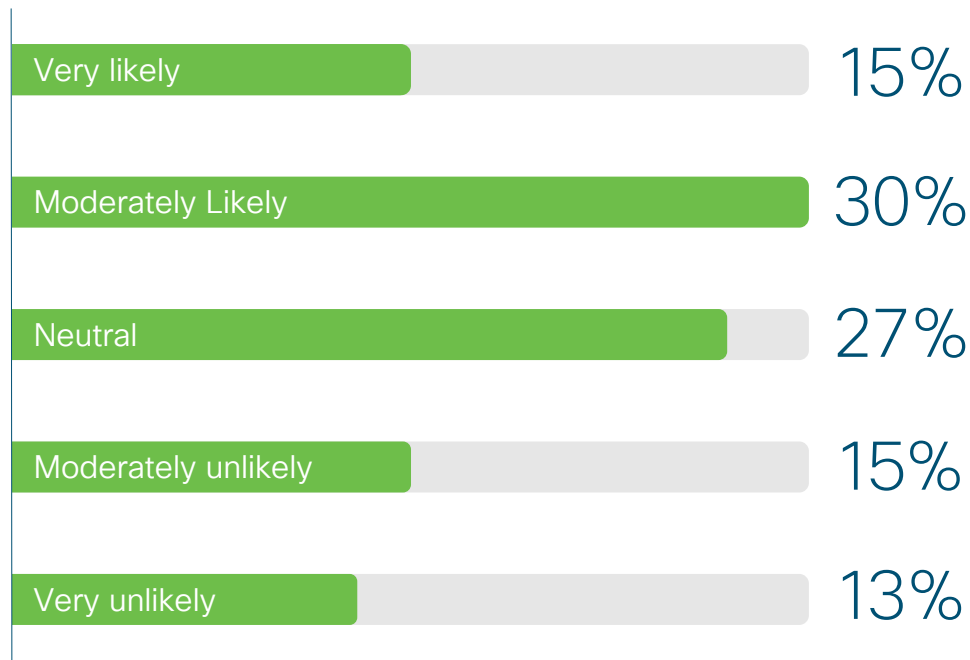


Source: Cisco Consumer Privacy Study - 2020

Not respecting privacy can cause consumers to terminate even long-standing, important business relationships. Nearly half (45%) of the Privacy Actives indicated the relationship terminated was of high significance (defined by its breadth and/or length of time the individual had been a customer), 37% indicated it was of moderate significance, and only 18% indicated it was of low significance. With many consumers ending significant business relationships over privacy concerns, we know privacy has become a very important factor in consumer decision making.

Interestingly, these broken relationships can sometimes be repaired. We asked these former customers if they would be willing to return as a customer if the organization's data privacy practices were improved, and most said yes. Nearly half (45%) of the former customers indicated it was very or moderately likely they would work with the company again if the data privacy issues were fixed. But 28% said it was very or moderately unlikely they would ever return. (See Figure 8.) **While fixing privacy problems can attract a portion of the lost customers, some are probably never giving the company a second chance.**

Figure 8. Likelihood of Former Customer to Return if Data Privacy Were Improved. N=760.

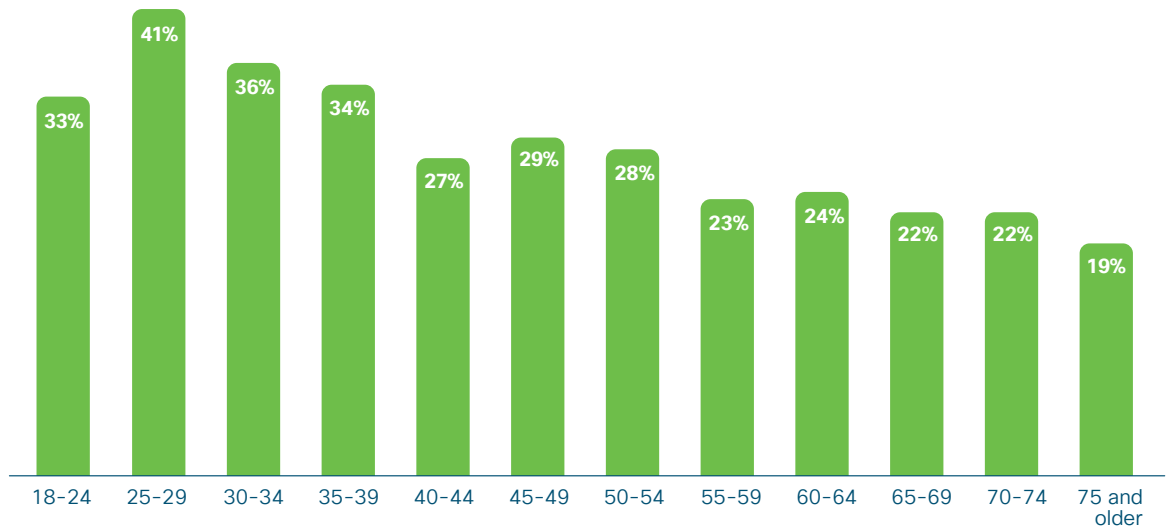


Source: Cisco Consumer Privacy Study - 2020

Finally, there are generational differences in the makeup of Privacy Actives. Contrary to the popular notion that younger people don't care about privacy, **we found stronger privacy awareness and activity among younger consumers.** The highest concentration of Privacy Actives is with the population under age 40, including 41% of the consumers between the ages of 25 and 29, and is somewhat lower among older consumers. (See Figure 9.)

These consumers already see privacy as an essential part of the customer experience and brand for the companies from which they choose to buy. Ninety percent of Privacy Actives said they won't buy from a company that they don't trust with their data, and 92% said they believe that "the way a company treats my data is indicative of the way it views me as a customer." As companies are thinking about their investments in privacy, they cannot ignore the impact it has on their current and potential customers. See the discussion in Section 3 below on the generation differences on awareness of privacy regulations.

Figure 9. Age Distribution of Privacy Actives. N=760.



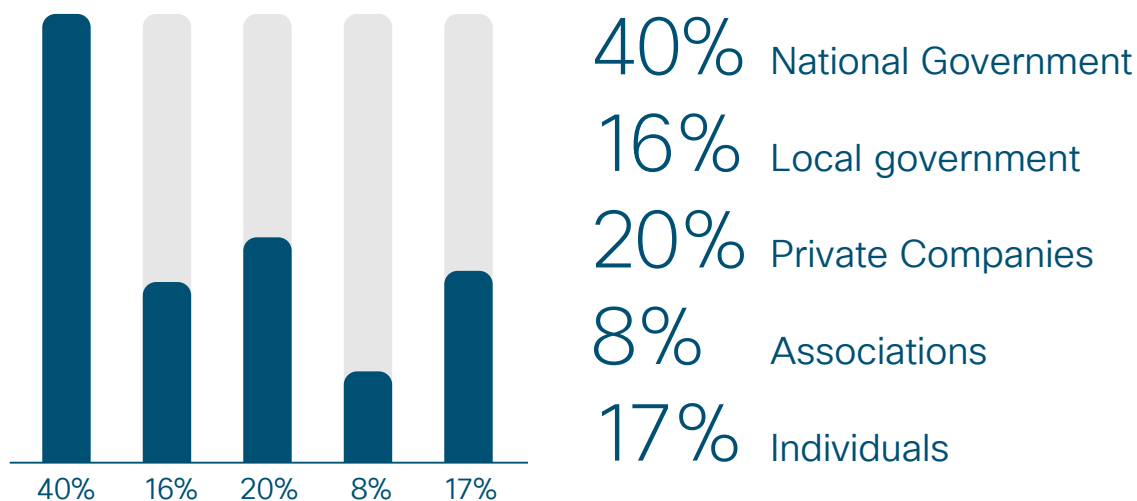
Source: Cisco Consumer Privacy Study - 2020

3. Consumers expect their governments to take the lead in protecting their data, and residents of all countries surveyed view their privacy laws very favorably

Survey respondents were asked how much responsibility various entities (e.g., federal and local government, companies, industry associations, or individuals) should have for protecting individuals' personal data, as each entity may have an important role to play. Companies request data from their customers and they can be transparent about how that data is being used. Governments can provide the regulation to ensure the companies are following stated policies and not misusing the data. Individuals can often choose what companies they want to work with, and what data they want to share.

Among survey respondents, **over half (56%) believe National or Local Government should play the primary role for protecting an individual's data**. 20% indicated private companies should play the lead role, and 17% said the individuals themselves should be primarily responsible. (See Figure 10.)

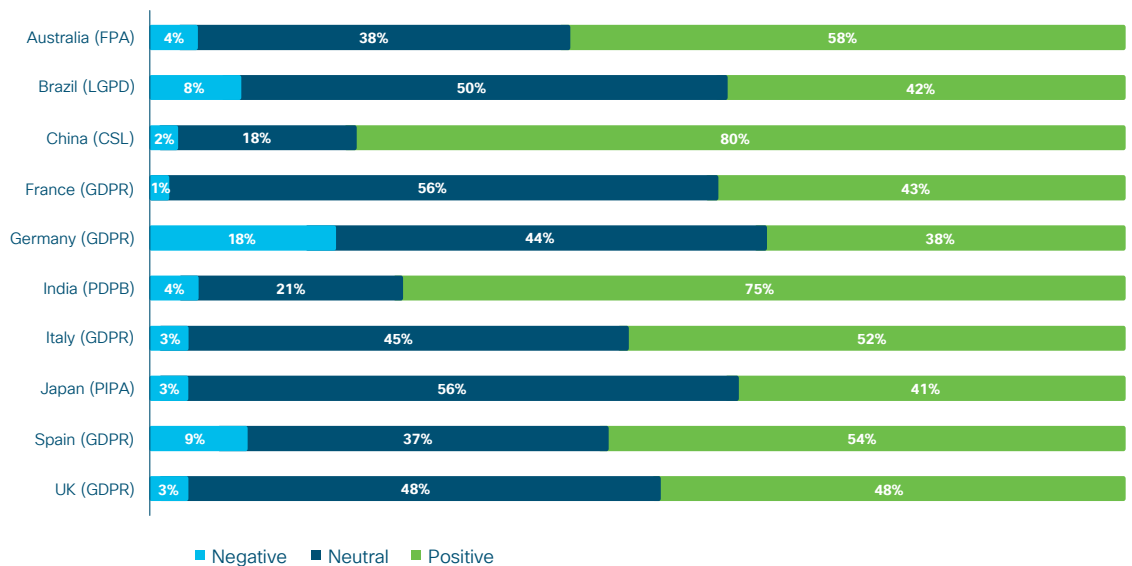
Figure 10. Entities Who Should Be Responsible for Protecting Data Privacy. N=2602.



Source: Cisco Consumer Privacy Study - 2020

Given this belief that governments need to play a strong role in protecting data privacy, it is perhaps not surprising to see that **consumers view privacy regulation 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 Federal Privacy Act (FPA) in Australia, Cybersecurity Law (CSL) in China, the proposed 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. Globally, 53% of respondents who were aware of the regulations felt they had a positive impact versus only 6% who said they had a negative impact. The sentiment among the respondents in individual countries was all quite positive, including China (80% positive, 2% negative), India (75% positive, 4% negative), and Australia (58% positive, 4% negative). Among the European countries, the percentage of positive responses for GDPR ranged from 38% (in Germany) to 54% (in Spain). (See Figure 11.)

Figure 11. Impact of Privacy Laws, by Country. N=2001.

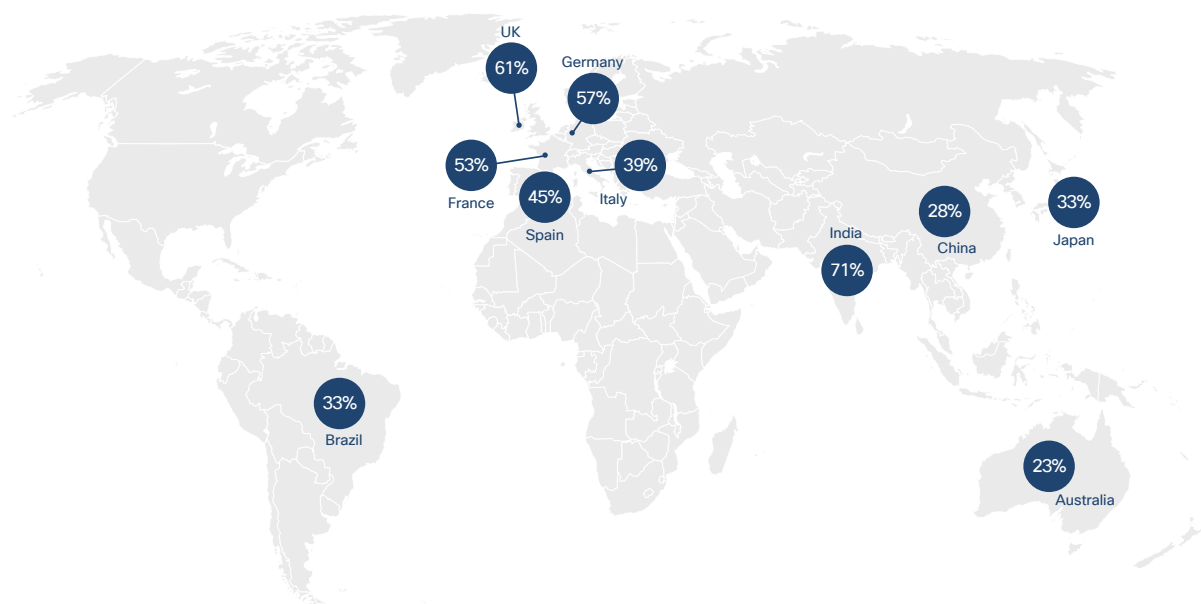


Source: Cisco Consumer Privacy Study - 2020

Even though consumers derive confidence from their country's privacy laws, public awareness of these laws continues to be challenging in most countries.

Overall, only 40% of respondents in the countries with national or multinational privacy laws were aware of these laws. GDPR has been in place for over two years and awareness ranges only from 39% (in Italy) to 61% (in UK). Among Australia, China, Japan, and Brazil respondents, awareness of their national privacy laws ranges from 23% to 33%. The notable exception is India, where 71% of respondents were aware of the proposed PDPB law. (See Figure 12.)

Figure 12. Awareness of National or Multi-national privacy laws, by Country. N=2001.

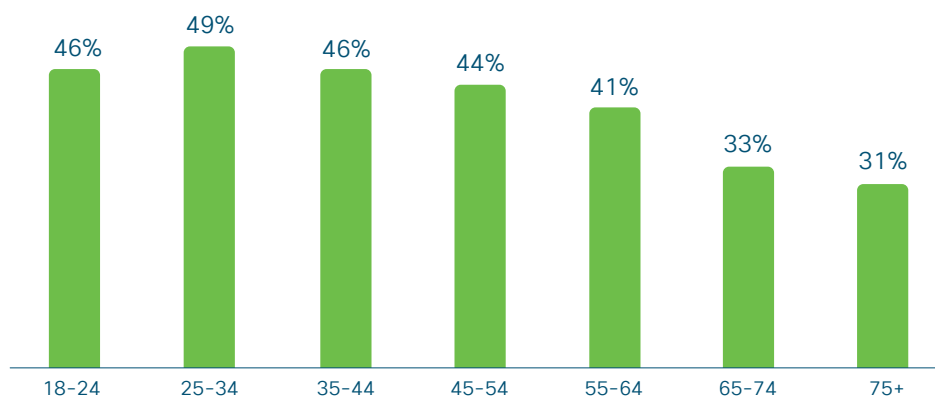


Source: Cisco Consumer Privacy Study - 2020

From a demographic perspective, younger people are more aware of privacy legislation than older consumers.

Nearly 50% of consumers, aged 25-34, are aware of one or more privacy regulations, versus 41% of those aged 55-64 and only 31% of those over age 75. (see Figure 13). Just as younger people are more active in protecting the privacy of their data (see Section 2 above), they also are more knowledgeable about the privacy regulations in place. This may bode well for the future.

Figure 13. Privacy Awareness, by Age. N=2602.



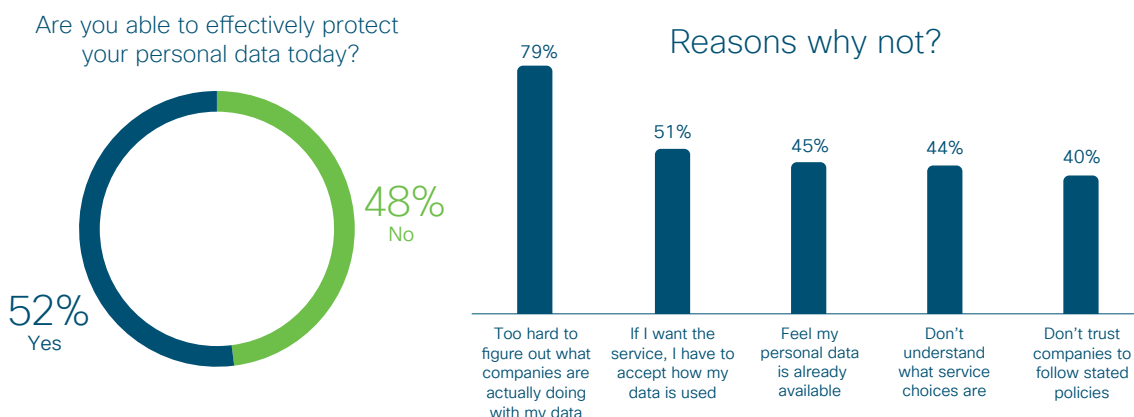
Source: Cisco Consumer Privacy Study - 2020

4. Consumers want more transparency on how their data is being used


Many consumers still don't feel their data is safe. Among survey respondents, nearly half (48%) said they don't feel they can effectively protect their data today. And the reason is quite clear. The primary reason, cited by 79% of them, is that it's **too hard for them to figure out what companies are actually doing with their data**. Other responses, included feeling they had no choice if they wanted to use an application or service (51%), feeling their data is already available from past breaches (45%), and not understanding what other choices they may have (44%). (See Figure 14.) Consumers want transparency on how their data is being used, not lengthy consent documents or hard-to-find information. And they want privacy regulators to ensure that companies are doing what they say they are doing.

Privacy laws help improve consumer trust, as individuals who have some knowledge of privacy regulations are more confident that their data is safe. Among respondents who were aware of one or more privacy regulations, only 64% felt they could effectively protect their data. This is compared to only 44% among those who were not aware of any privacy regulations. It seems that privacy regulation helps provide a measure of confidence to consumers worried about the safety of their information, and it would help for more consumers to know about these laws.

Figure 14. Ability of Users to Protect Their Data and Reasons They Think They Can't. N=2602.



Source: Cisco Consumer Privacy Study - 2020



“The pandemic has only elevated privacy as a central condition for trust in an environment where governments, businesses and schools have gone virtual.”

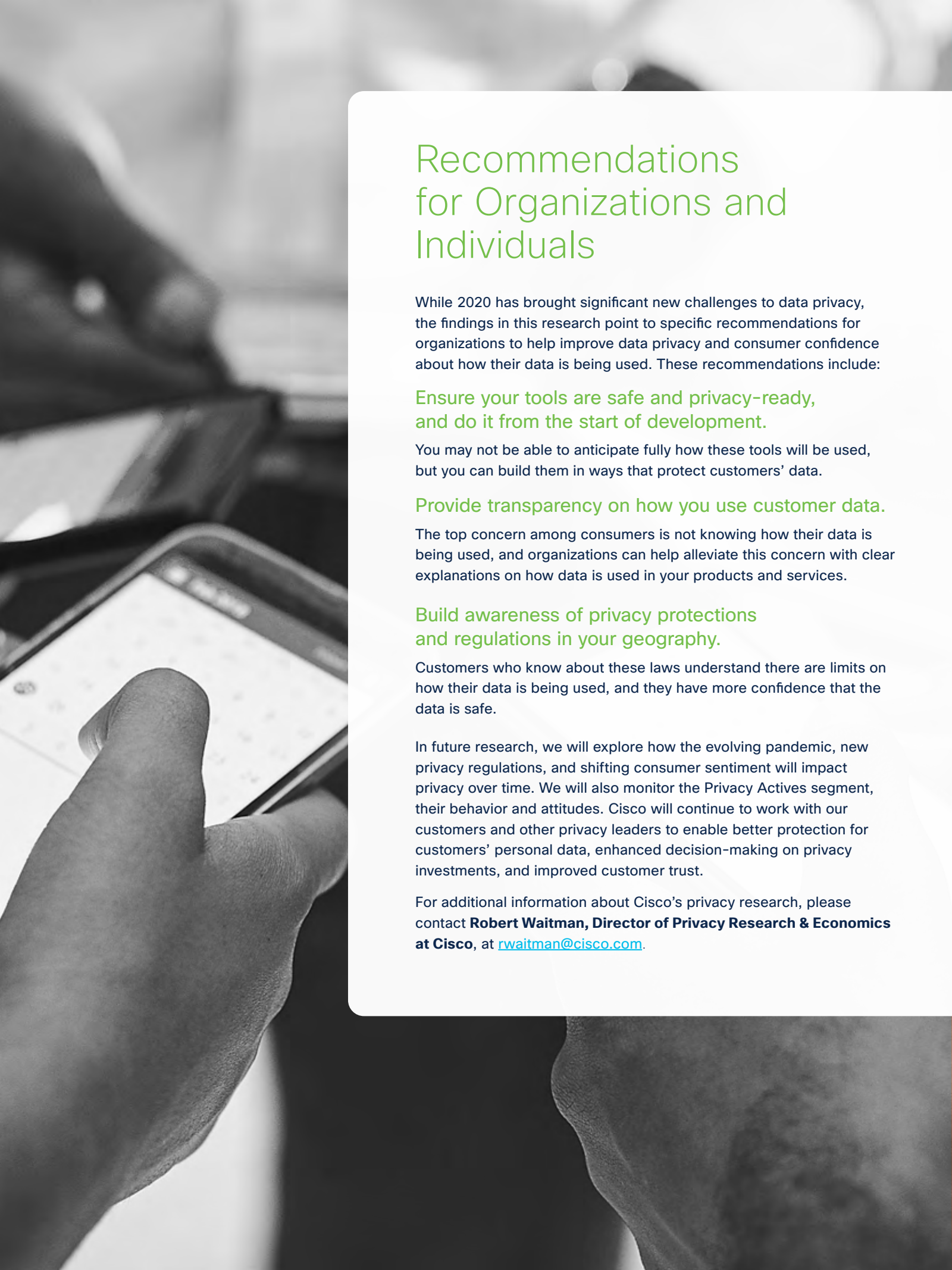
– Omer Tene, VP and Chief Knowledge Officer,
International Association of Privacy Professionals (IAPP)

“Cisco’s latest privacy research highlights that people care deeply about protecting their data, and many have stopped doing business with companies due to data privacy concerns.”

– Brad Arkin, SVP and Chief Security and Trust Officer, Cisco

“It is remarkable that so many people can’t figure out what companies are doing with their data. Trust requires a transparency revolution!”

– Martin Abrams, Executive Director,
Information Accountability Foundation (IAF)



Recommendations for Organizations and Individuals

While 2020 has brought significant new challenges to data privacy, 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:

Ensure your tools are safe and privacy-ready, and do it from the start of development.

You may not be able to anticipate fully how these tools will be used, but you can build them in ways that protect customers' data.

Provide transparency 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 clear explanations on how data is used in your products and services.

Build awareness of privacy protections and regulations in your geography.

Customers who know about these laws understand there are limits on how their data is being used, and they have more confidence that the data is safe.

In future research, we will explore how the evolving pandemic, new privacy regulations, and shifting consumer sentiment will impact privacy over time. We will also monitor the Privacy Actives segment, their behavior and attitudes. 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 & 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 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 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 2019 series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark 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 June 2020

RPT_06_2020

© 2020 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. (2062922)





SECURE