CISCO CYBERSECURITY SERIES 2019 • DATA PRIVACY
NOVEMBER 2019

Consumer Privacy Survey

The growing imperative of getting data privacy right

cisco

Contents

Introduction

Most people today understand it's beneficial and often necessary to provide certain personal information to companies and applications they use in order to receive the benefits of products, services, and business relationships. At the same time, they're increasingly concerned about protecting their privacy and personal data.

Companies have a significant opportunity to capture business benefits while building trust and brand value with their customers.

We've seen a constant stream of news headlines regarding hundreds of millions of personal records exposed in data breaches and many examples of companies using customers' personal data in ways that were not anticipated – nor agreed to. With this background, the Cisco Privacy Office explored end-user (referred to in this report as "consumer") perspectives on what companies, governments, and individuals have done, and could do, to better protect and respect privacy.

The Cisco Consumer Privacy Study uses data gathered on a double-blind basis in May 2019. The survey was completed by over 2,600 adult respondents in 12 of the world's largest economies – five in Europe, four in Asia Pacific, and three in the Americas.[1] Their profiles span various age groups, gender, and income levels. Participants were asked about their attitudes and actions regarding their personal data, the products and services they use, their comfort level with potential new business models, and the impact of data privacy regulations on their behavior.

The findings from this study, along with prior Cisco research, reveal a new landscape where privacy has become a critical business imperative and an important driver of consumer behavior. Specifically, this paper explores four areas of insights:

- People care about privacy, and a surprisingly large number of them have already taken actions to protect it
- Privacy regulations and policies provide "guardrails" for innovation and help to build trust
- Consumers value government's role in regulating the use of data, and they view the EU's General Data Protection Regulation (GDPR) very favorably
- Many consumers worry they are unable to protect their data, and their biggest challenge is figuring out what companies are doing with their data

As a result, this research also suggests a new framework for measuring the benefits and return on privacy investment beyond regulatory and compliance requirements.

As more consumers place a premium on the proper protection of their data, companies have a significant opportunity to meet regulatory requirements while they capture business benefits and build trust with their customers.

"Privacy is a business imperative and ethical responsibility – not just a compliance requirement."

Harvey Jang
Chief Privacy Officer & Counsel, Cisco

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

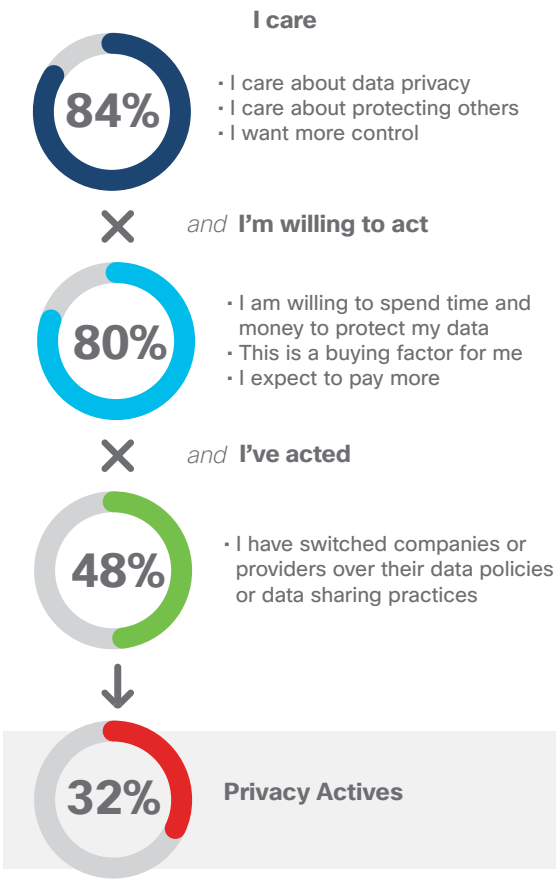
Results

Insight 1: People care about privacy, and a surprisingly large number have already taken actions to protect it

Over the past few years, the public has become more vocal in expressing that they care about data privacy. The big question has been whether they are willing to act, for instance, by giving up certain benefits or paying more to have stronger protection and control. On one hand, many experts and the media have expressed the view that there are very few users who take actions to protect their own privacy.[2] On the other hand, user awareness has recently increased in the wake of the EU's GDPR – which requires disclosures to users about their rights – and constant headlines of data breaches affecting billions of records and millions of users. With this Cisco Consumer Privacy Survey of 2019, we sought to better understand user behaviors and how far they are willing to go (and have gone) to protect their data privacy. Based on the survey responses, we have identified a surprisingly large segment of the population that indicates it cares about data privacy, is willing to act, and in fact has already acted. This segment, which we are calling "Privacy Actives", accounts for nearly one-third of all respondents.

We reached this result by first identifying the vast majority of respondents (84%) who indicated that they care about privacy. They care for their own data, they care about the data of other members of society, and they want more control over how their data is being used. Of this group, 80% also said they are willing to act to protect it. They are willing to spend time or money to keep their data safe, they see data privacy as an important factor influencing their buying decisions, and they expect to pay more for products and services with better protection. Among these respondents, nearly half (48%) indicated they had already switched companies or providers because of their data policies or data sharing practices. Putting all these attributes together, we have a segment of 32% of all respondents who care about data privacy, are willing to act, and have already taken action to protect their privacy. (See Figure 1.)

Figure 1 The Privacy Actives Segment
N=2601



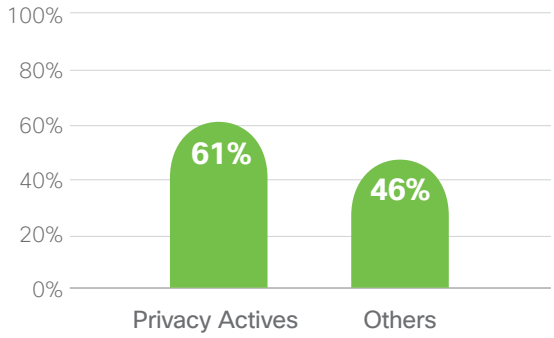
Source: Cisco Consumer Privacy Study - 2019

These Privacy Actives are not only sizable, they also represent an attractive demographic for companies selling to them. Compared to the rest of the survey respondents, the

2 Sample headlines: "You don't care enough about your data. This is why", World Economic Forum, June 26, 2018. "Why You Don't Care About Internet Privacy", Medium.com, May 24, 2018. "Privacy is Completely and Utterly Dead, and We Killed It", Forbes, August 19, 2014.

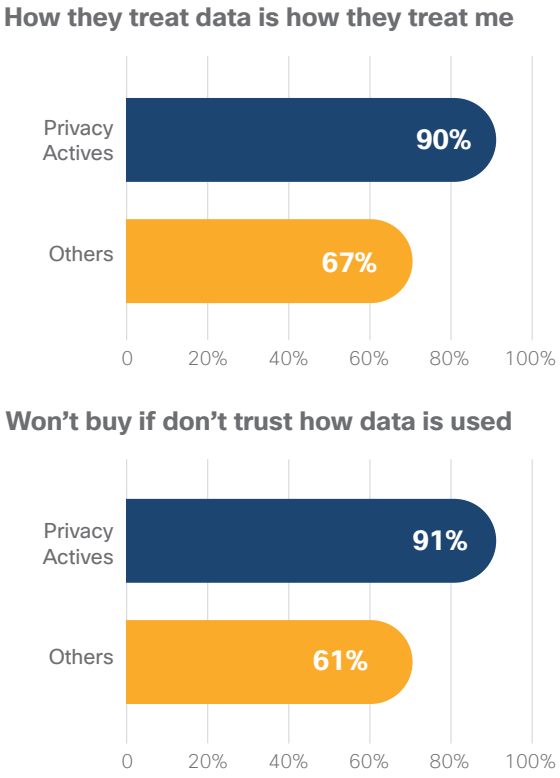
Privacy Actives are younger: 61% of them are under age 45 versus 46% of other respondents. (See Figure 2.) They also do more of their shopping online (32% vs. 23%).

Figure 2 Percentage aged 18-44 Privacy Actives vs. others
N=2601



Source: Cisco Consumer Privacy Study - 2019

Figure 3 Attitudes of Privacy Actives versus others
N=2601

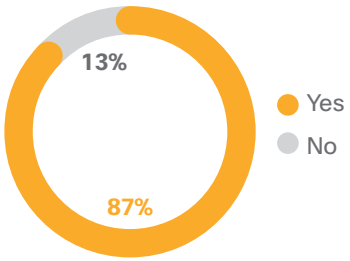


Source: Cisco Consumer Privacy Study - 2019

Perhaps even more importantly, Privacy Actives see respect for privacy as core to the brand of the companies with which they do business. Ninety percent say they believe how their data is treated is indicative of the way they will be treated as a customer; and 91% won't buy from a company if they don't trust how their data will be used. (See Figure 3.)

The emergence of the Privacy Actives segment also helps explain some of the more interesting findings from the Cisco 2019 Data Privacy Benchmark Study. That study highlighted that 87% of companies are experiencing sales delays caused by their customers' privacy concerns. (See Figure 4.) People today are more concerned about privacy; they are asking more questions about what data is collected, how it is used, who has access to it, and how long it is retained. The fact that more consumers are willing to choose (or change) providers shows evidence consistent with this trend.

Figure 4 Organizational respondents experiencing delays in their sales cycles due to customers' data privacy concerns
Percent of respondents, N=2064



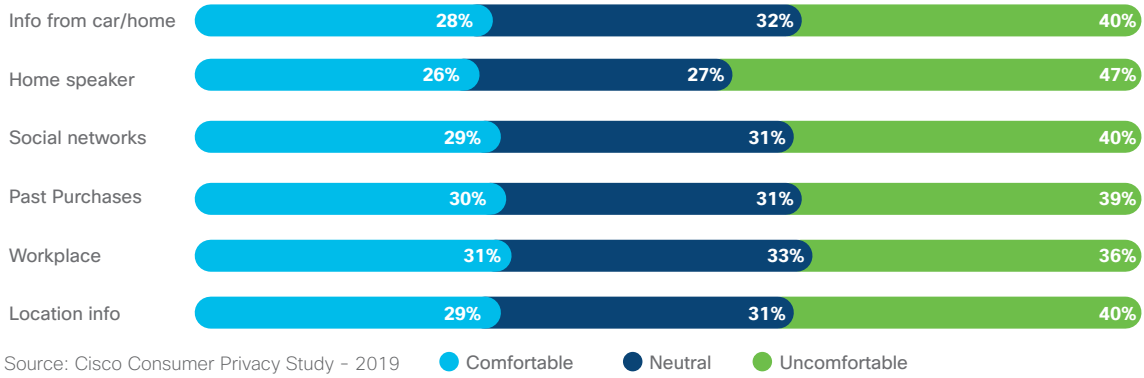
Source: Cisco 2019 Data Privacy Benchmark Study

In addition, we noted that 97% of companies recognized they were realizing benefits such as competitive advantage or investor appeal from their privacy investments. With a large number of consumers closely associating a company's privacy practices with its brand, it makes sense that companies are realizing these business benefits well beyond any compliance requirements.

"This research from Cisco confirms that people have become aware of their privacy rights, and they will proactively choose to interact with organizations who they trust will be responsible with their data. It is therefore a business imperative and a competitive advantage for companies to embrace transparency and accountability in how they manage personal data and focus on building digital trust with their customers."

Bojana Bellamy
President, Centre of Information Policy Leadership (CIPL)

Figure 5 Users' comfort levels with new business models.
N=2601



In future research, we'll continue to monitor the Privacy Actives segment, including its size, demographic makeup, and behaviors.

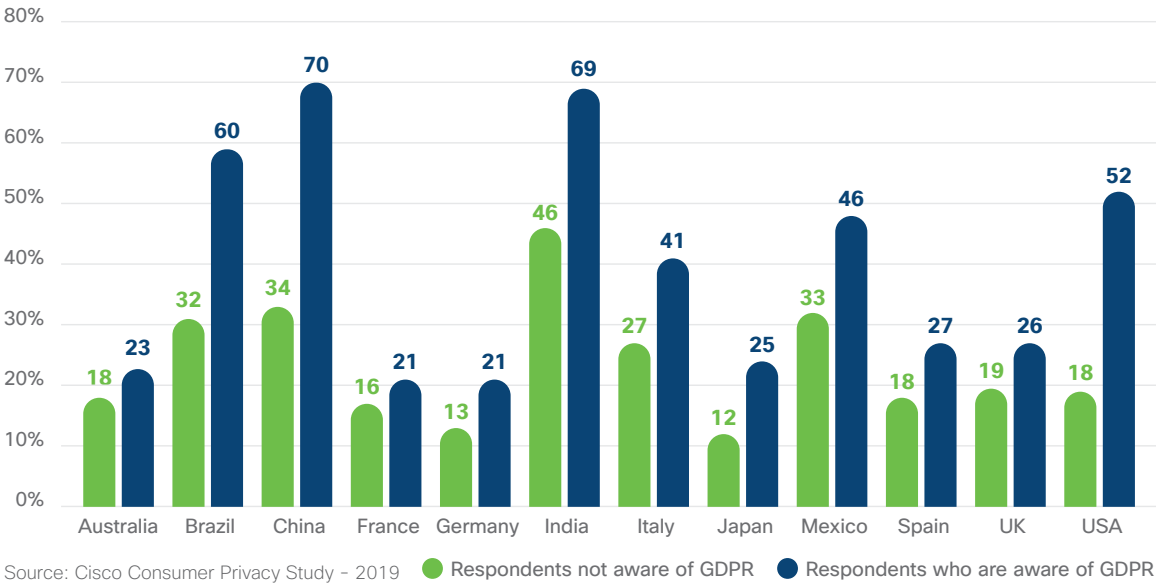
Insight 2: Privacy regulation provides "guardrails" for innovation and helps build trust

A second area of focus in the survey was to understand consumers' interest and acceptance of emerging business models that might involve using their personal data in new ways that could benefit the individual or society at large. Some users find these models invasive, while others find them acceptable. We wanted to better understand this dynamic, and also wanted to understand whether privacy regulations play a role in user acceptability. While each of the models we tested included using personal data in a potentially unanticipated way, each also included a personal or societal benefit. The models we tested included:

- Sharing personal information from your home or your car in exchange for receiving health or safety warnings that could benefit you and your family.
- Allowing a smart home speaker (e.g., Alexa, Echo) to "listen" for personal information in exchange for receiving health or safety warnings that could benefit you and your family.
- Sharing personal information from your social networks (e.g., Facebook, Twitter) that could be aggregated and anonymized to improve the health of the overall population.
- Sharing personal information about your past purchases combined with relevant health information to enable a retainer to suggest products (e.g., shoe style) that would be best for you.

> **"Data privacy and protection differentiates business today. Do it right, you stand out. Do it wrong, and you will be called out."**
>
> John N. Stewart
> SVP, Chief Security and Trust Officer, Cisco

Figure 6 Average comfort level with six new business models, by country.
N=2601



Source: Cisco Consumer Privacy Study - 2019

- Sharing personal information from your workplace (e.g., your location and movements) that could be aggregated to improve the efficiency and safety of the work environment for everyone.
- Sharing personal information about your current geographic location in exchange for promotional offers and pricing advantages from local stores.

Survey respondents were generally not supportive of these new business models. Despite the potential personal or societal health and safety benefits associated with the models, 36% to 47% (depending on the model) indicated they were not comfortable having their data used in this way, while only 26%-31% indicated they were comfortable. (See Figure 5.) As a result, companies seeking to introduce products and services using personal data in new ways should make sure they have considered and addressed customers' potential data privacy concerns.

Privacy regulations, to the extent people are aware of them, seem to play an important role in making users more comfortable with how their data might be used. Specifically, respondents who were aware of privacy regulations (like GDPR) indicated they were much more comfortable with these potential new business models than those who were not aware. Averaged across all six of these models, 38% of respondents who were aware of GDPR were comfortable with them versus only 24% of respondents who were unaware of GDPR.

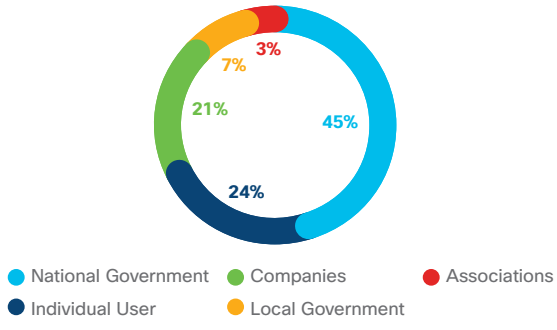
Interestingly, this increase in comfort level was consistent across every country in the study. While there are differences as to the absolute comfort level, each geography showed higher comfort levels among the respondents who were aware of GDPR. When privacy controls are clearly identified (e.g., in a specific law or standard), they seem to be beneficial for both consumer and corporate activities. (See Figure 6.)

In the Cisco 2019 Data Privacy Benchmark Study, 42% of companies indicated that their privacy investments enabled agility and innovation at their companies. By knowing what they couldn't do from a privacy perspective, they were much freer (and in some cases, compelled) to pursue new ideas on what they could do. These results do not imply that every regulation would be beneficial to corporate innovation or to consumers. Too much, too prescriptive, or inconsistent regulation could be costly, burdensome, and confusing for both companies and users. Nonetheless, it appears that at least some regulation provides benefits to all in an otherwise confusing landscape.

Insight 3: Consumers value government's role in regulating the use of personal data, and they view GDPR very favorably

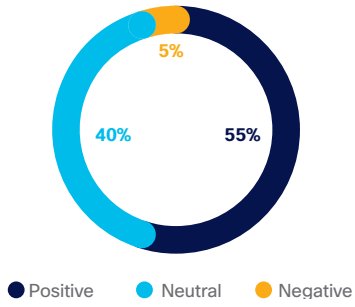
Survey respondents were asked which entity – federal or local government, companies, industry associations, or individuals – should have primary responsibility for protecting personal data. Governments can provide regulation and oversight, but confusing or overly broad regulation can also become burdensome on companies and individuals. Companies have a responsibility to protect the data of their customers, but sometimes their short-term profit motives interfere. Many consumers might accept they are also partially responsible for their decisions on when and how they share their data, but they might struggle to understand exactly what is being done with their data. While respondents were somewhat split on the question of who is responsible for protecting data privacy, most selected federal government (45%), followed by the individual user (24%) and companies (21%). (See Figure 7.)

Figure 7 Who is primarily responsible for protecting data privacy
N=2601



Source: Cisco Consumer Privacy Study - 2019

Figure 8 Overall sentiment regarding the impact of GDPR
N=941

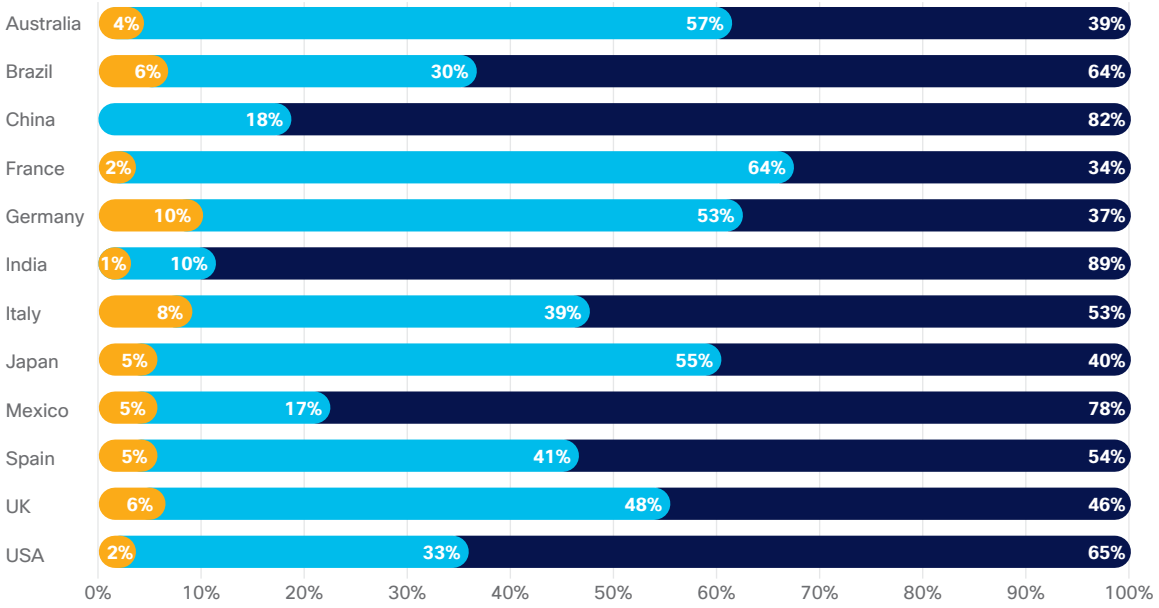


Source: Cisco Consumer Privacy Study - 2019

Indeed, all three would seem to have an important role to play in protecting personal information. Governments can oversee what companies are doing, companies can set and follow appropriate data policies anchored in the principles of transparency, fairness, and accountability, and individuals can take steps to protect their own privacy and accept responsibility for the choices they make. With more respondents indicating they wanted the government to be responsible, perhaps it's not surprising that those familiar with GDPR felt it had a very positive impact. An overwhelming majority of respondents expressed a positive view of the GDPR, with 55% of respondents in favor and only 5% of respondents expressing a negative view. (See Figure 8.)

Although there is some variation across countries, there is generally a very positive view of GDPR among consumers worldwide with very little negative sentiment. (See Figure 9.) Respondents were also asked about whether GDPR was effective in meeting various privacy goals for the individual. Fifty-two percent said they felt they had more control of their personal data as a result of GDPR, 59% said they have a greater ability to exercise their rights regarding data, and 47% said they have greater trust in companies that use their data. On the negative side, 47% expressed notification fatigue and said they receive far too many meaningless privacy-related notifications as a result of GDPR. (See Figure 10.)

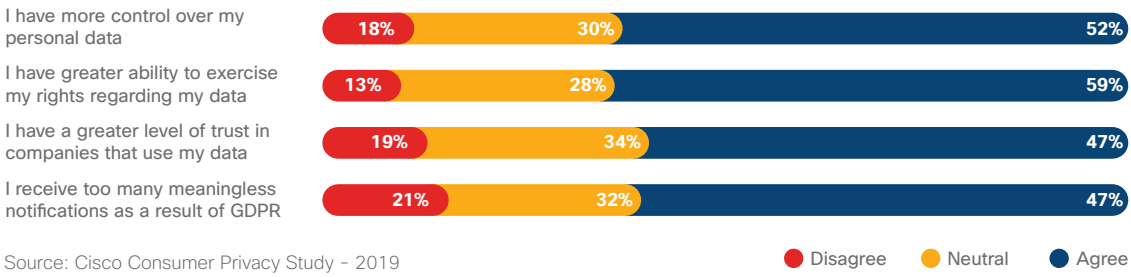
Figure 9 Overall sentiment regarding the impact of GDPR, by country.
N=941



Source: Cisco Consumer Privacy Study - 2019

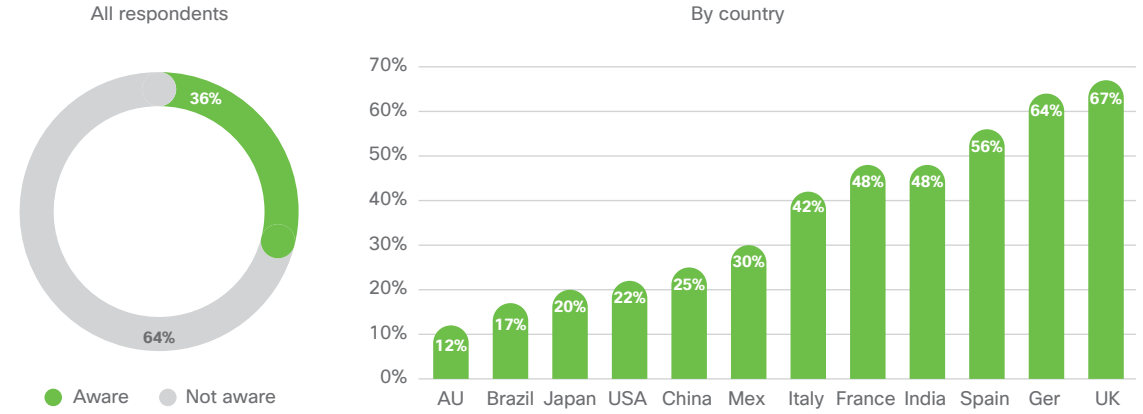
Note: For Australia, Brazil, and Japan, the number of respondents familiar with GDPR is relatively small, so the margin of error is significant. The results are included because the margin of error is still much smaller than the percentage differences between respondents with positive and negative sentiment.

Figure 10 Impact of GDPR on the individual.
N=941



Source: Cisco Consumer Privacy Study - 2019

Figure 11 Awareness of GDPR
N=2601



Source: Cisco Consumer Privacy Study - 2019

Our survey also revealed limitations to the public perception of privacy regulations. Public awareness is still only partial and has much room for improvement. Overall, only about one-third of respondents across the 12 countries in our survey are familiar with these new regulations. Even in Western Europe, where the GDPR went into effect with considerable press and corporate communications in mid-2018, about a third of respondents are still not aware of GDPR, and a minority of respondents is still neutral regarding its benefits. (See Figure 11.)

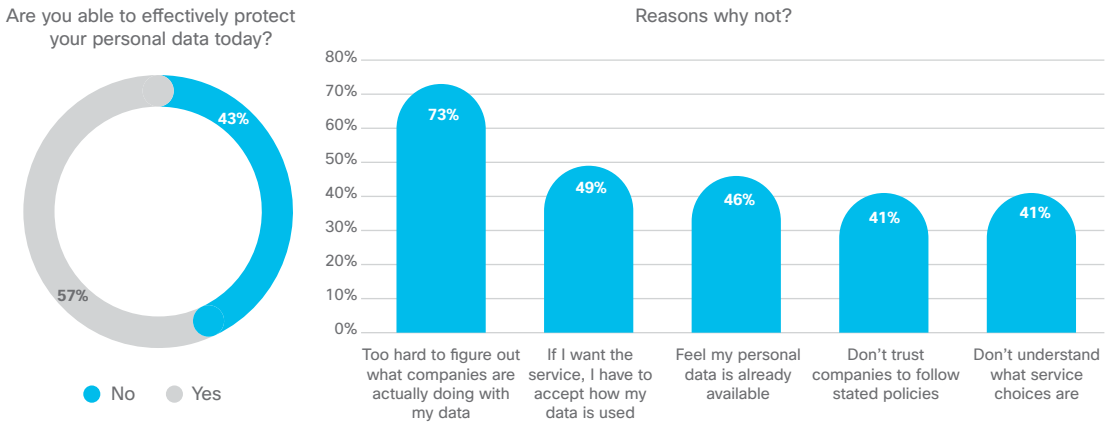
Insight 4: Many consumers feel they are unable to protect their personal data, and their biggest challenge is figuring out what companies are doing with their data

The increased focus on privacy has brought a number of challenges, and one of the biggest issues raised by our survey respondents is the need for greater transparency and simplicity in understanding how their data is being used. Forty-three percent of all respondents don't believe they can adequately protect

"This Cisco research shows that privacy has become a critical issue for individuals worldwide, and companies (like ours) need to continue to treat our customers' data properly to build and maintain their trust."

Tom Moore
Chief Privacy Officer and SVP, AT&T

Figure 12 Ability of users to protect their data and reasons why they think they can't
Left: N=2601 **Right:** N=1129



Source: Cisco Consumer Privacy Study - 2019

their personal data today. This concern is also higher with respondents 55 years of age and above, with 52% indicating they cannot protect their personal data today. Respondents who worried they could not protect their data were also asked the primary cause of this problem. The top answer, cited by nearly three-fourths of respondents, was that "it's too hard to figure out what companies are doing with my data." Other significant responses included: "If I want the service, I have to accept how my data is used" (49%); "I feel my data is already available" (49%); and "I don't trust companies to follow their stated policies" (41%). (See Figure 12.)

These responses reveal a gap between consumers' expectations and companies' stated and actual practices. It appears that companies haven't done an ample job of explaining clearly to customers how their data is being used, and demonstrating that they are, in fact, following stated policies to respect and protect data privacy.

Conclusion

The results of this survey, combined with past Cisco data privacy research, suggest a new framework for measuring the benefits and return on privacy investments. Interviews with privacy decision-makers show that companies and their governance entities (board of directors) have generally focused on legal compliance and avoiding the potential of regulatory fines and penalties. Our recent findings suggest an even broader value model for capturing the business benefits of privacy, including the following areas.

1. Attracting and retaining customers who care about privacy and are willing to act.

This research shows the vast majority of people care about protecting their privacy, and a third are already acting by switching providers when one falls short. This segment represents an attractive portion of the customer base, as they are younger, more affluent, and more online than the rest of the population. Customers are increasingly seeing data privacy as a critical part of the brand of a company, and companies need to invest in privacy to make sure their customers understand and are comfortable with their data practices and policies. If not, customers will migrate to other companies with which they are more comfortable.

2. Improving business agility and innovation.

In this research, customers have shown an increased willingness to accept new uses of their data when they feel adequate protections are in place. They're looking to governments, as well as companies, to adopt rules and policies that provide these protections. When these "guardrails" are in place, there is greater flexibility for companies to innovate and greater acceptance by customers of new business models. This further validates our previous research showing companies are seeing these benefits from their privacy investments.

3. Reducing sales friction.

Having more customers care about privacy and being willing to act can also create friction in a company's sales cycle. Potential customers are increasingly asking questions about how their data will be used when choosing a vendor. If companies don't have transparent and easily understood information, they will see significant delays and lost opportunities in their sales cycles.

4. Enhancing the overall attractiveness of the company.

Shareholders and investors are also beginning to understand the increasing importance of privacy to a company's brand and value, and they will reward those companies who get it right.

In conclusion, organizations should think of the value of privacy broadly, beyond compliance and risk avoidance. For many organizations, privacy has now become a critical business imperative.

About the Cisco Cybersecurity 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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published November 2019 PRIV_07_1119_FINAL