RSA

RSA DATA PRIVACY & SECURITY REPORT

BUSINESS-DRIVEN SECURITY™

INTRODUCTION

The Convergence of Risk and Security

Cybersecurity incidents are increasing at astonishing rates with no end in sight. The impact of these incidents in business disruption, cost and invasion of individual privacy has provoked a groundswell of legislation and government regulation across the globe.

With new regulations on the horizon – and consumers increasingly aware of how their data is being handled – businesses are in uncharted territory as business risk and cybersecurity converge. Standards like the European Union General Data Protection Regulation (GDPR) are forcing risk, security, compliance, and line of business owners to juggle conflicting goals of security and privacy with business growth and innovation.

ANY ORGANIZATION THAT HANDLES THE PERSONAL DATA OF EU RESIDENTS WILL NEED TO COMPLY WITH THE GDPR, WHICH COMES INTO EFFECT ON 25TH MAY 2018. THE GDPR'S OVERALL AIM IS TO GIVE EUROPEAN RESIDENTS GREATER CONTROL AND VISIBILITY OF THEIR PERSONAL DATA, STRENGTHENING AND UNIFYING DATA PROTECTION. IT WILL ENSURE THAT INDIVIDUALS ULTIMATELY OWN AND CONTROL ANY DATA THAT RELATES TO THEM.

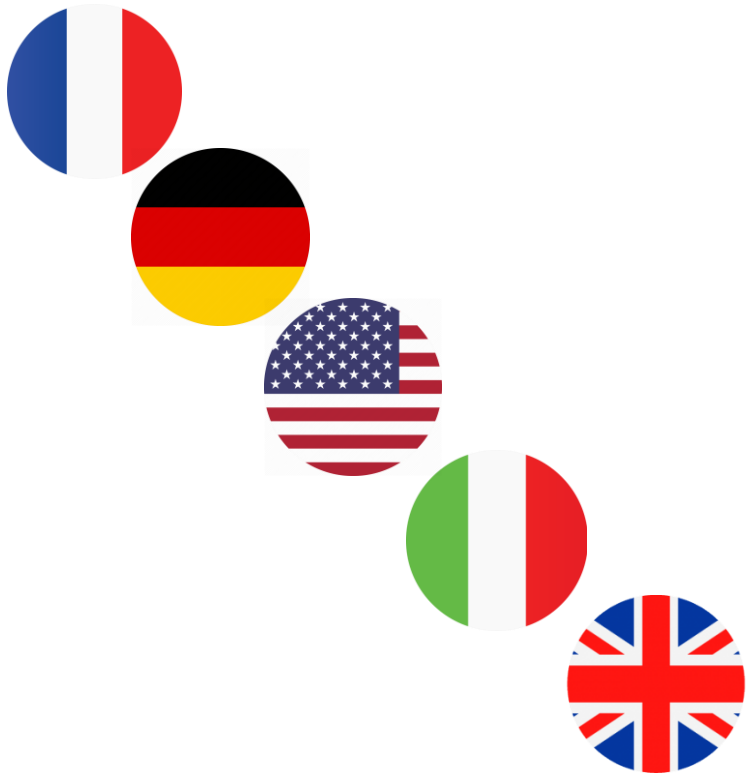
Legislation Everywhere

Any organization that handles the Personally Identifiable Information (PII) of EU residents will need to comply with the GDPR, which comes into effect on 25th May 2018. The GDPR's overall aim is to give European residents greater control and visibility of their personal data, strengthening and unifying data protection. In 2017 alone, 28 U.S. states enacted some form of cybersecurity legislation. Internationally, every major country has some form of legislation in place, with China and Australia passing privacy regulations last year, and the European Union – and the U.K. – enacting the GDPR in May 2018. Without a universally agreed upon set of standards, the onus is on companies of all sizes to continually monitor changes in the security and regulatory landscape as new requirements are mandated.

In short, consumer expectations of privacy and the accompanying regulations are translating business risk into cyber risk across the globe.

RSA

ABOUT THE SURVEY



Our objective in conducting the first RSA® Data Privacy and Security Survey was to understand the value that the average consumer puts on privacy and to identify the ways that data collection, storage, compliance and security trends can impact businesses.

As we enter another year rife with both cyber and business risks, businesses are adapting to their customers' privacy demands, as well as legislation, which is extending globally and into industry-specific markets.

To that end, we asked consumers in France, Germany, Italy, the United Kingdom and the United States about the impact privacy, data and regulations have on their relationship with businesses.

Some of what we heard was expected – that consumers feel most protective of their banking and security information (which were the top answers across every region) – but we also came away with some surprising findings. For example, we discovered that consumers' behavior is less impacted by a fear of hackers than it is a desire to avoid marketers. More than 40% of respondents admitted to falsifying personal information and data when signing up for products and services online.

To understand how consumer behavior affects businesses, we also asked about the extent to which consumers would avoid a business after a data breach or other incident.

It is our pleasure to present the findings from RSA's Data Privacy and Security Survey.

We hope you find them interesting and insightful.

METHODOLOGY

We surveyed more than

7,500

CONSUMERS ACROSS

FRANCE GERMANY ITALY U.K. U.S.A.

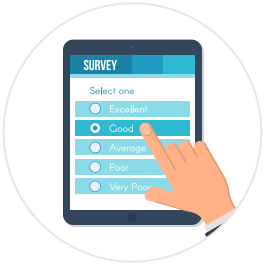
All figures, unless otherwise stated, are from YouGov Plc.

TOTAL SAMPLE SIZE:

7,579

FRANCE	GERMANY	ITALY	U.K.	U.S.A.
1,025	2,232	1,134	2,112	1,076

FIELDWORK OCCURRED 15 DECEMBER 2017 – 3 JANUARY, 2018



SURVEY WAS CARRIED OUT ONLINE

THE FIGURES HAVE BEEN WEIGHTED AND ARE REPRESENTATIVE OF ALL ADULTS (AGED 18+) IN EACH REGION

KEY INSIGHT #1

Consumers are most concerned with their financial wellbeing…but that might be changing.

While the definition of PII is broadening – for instance, the GDPR encompasses anything from names, photos, posts on social media, email addresses, bank details, and IP addresses, right through to genetic data – the top concerns among consumers when it comes to having personal information lost tends to skew more towards traditional financial, security and identity data.

Every demographic group in our survey listed financial and banking information as their top concern with respect to lost data; however, younger millennials (ages 18-24) were much more concerned about having stolen personal information (messages or photos) used against them as blackmail.

80%

OF RESPONDENTS LISTED FINANCIAL & BANKING INFORMATION, MAKING IT THE TOP CONCERN WITH RESPECT TO LOST DATA

76%

OF RESPONDENTS LISTED SECURITY INFORMATION (PASSWORDS), AND 72% IDENTITY (PASSPORTS, DRIVING LICENSE) AS AREAS OF CONCERN

51%

OF YOUNGER MILLENNIALS (AGES 18 –24) IN THE SURVEY ARE CONCERNED WITH PERSONAL INFORMATION BEING USED FOR BLACKMAIL

84%

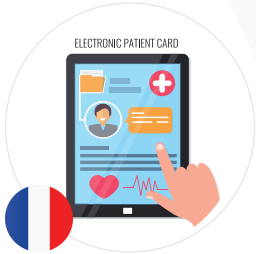
OF UK RESPONDENTS AND 81% OF ITALIAN RESPONDENTS LISTED SECURITY INFORMATION AS A CONCERN, BOTH HIGHER THAN THE GLOBAL AVERAGE

51%

OF GERMAN RESPONDENTS ARE PROTECTIVE OF THEIR GENETIC DATA, COMPARED TO ONLY 39% IN ITALY AND FRANCE

46%

OF AMERICAN RESPONDENTS ARE CONCERNED ABOUT LOCATION INFORMATION, THE HIGHEST OF ANY COUNTRY



45%

OF FRENCH RESPONDENTS LISTED MEDICAL DATA AS A CONCERN, COMPARED TO 59% OF ALL RESPONDENTS

RSA

KEY INSIGHT #2

Consumers' awareness of data capture and breaches is growing, with 73% of respondents claiming to be more aware of data breaches compared to five years ago.

49%

OF AMERICAN RESPONDENTS CLAIMED TO BE MUCH MORE AWARE OF DATA BREACHES THAN IN THE PAST

62%

OF ALL RESPONDENTS SAID THEY WOULD BLAME THE COMPANY THAT LOST THEIR DATA, EVEN BEFORE BLAMING HACKERS. AS CONSUMERS BECOME BETTER INFORMED, THEY EXPECT MORE TRANSPARENCY AND RESPONSIVENESS FROM THE STEWARDS OF THEIR DATA

72 HOURS

ONE FACTOR HELPING CONSUMERS ACHIEVE BETTER DATA TRANSPARENCY IN THE COMING YEAR WILL BE NEW REQUIREMENTS ABOUT BREACH NOTIFICATION AND REPORTING

UNDER THE GDPR, DATA CONTROLLERS AND PROCESSORS MUST SUPPLY A DETAILED REPORT REGARDING ANY BREACH OF PERSONAL DATA TO THEIR LOCAL DATA AUTHORITY 'WITHOUT UNDUE DELAY', AND WHERE POSSIBLE WITHIN 72 HOURS OF THE BREACHED PARTY BECOMING AWARE OF IT.

KEY INSIGHT #3

Consumers' data collection behaviors are changing. 41% of respondents admitted to intentionally falsifying personal information and data when signing up for products and services online.

59%

OF RESPONDENTS WHO FALSIFIED DATA DID SO TO AVOID UNSOLICITED COMMUNICATIONS AND 55% SAID THEY WANTED TO AVOID MARKETING

35%

FALSIFIED INFORMATION DUE TO SECURITY CONCERNS

55%

AVOID HANDING DATA OVER TO A COMPANY THAT HAS BEEN SELLING OR MISUSING DATA WITHOUT CONSENT

54%

ARE LESS LIKELY TO BUY PRODUCTS OR SERVICES FROM A COMPANY THEY KNOW TO HAVE BEEN MISHANDLING DATA

78%

OF RESPONDENTS LIMIT THE AMOUNT OF PERSONAL INFORMATION THEY PUT ONLINE OR SHARE WITH COMPANIES

RSA

KEY INSIGHT #3

(continued)

82%

OF UK RESPONDENTS CLAIM THEY WOULD BOYCOTT A COMPANY THAT REPEATEDLY DEMONSTRATED THEY HAVE NO REGARD FOR PROTECTING CUSTOMER DATA (72% IN THE U.S., 69% IN FRANCE, 64% IN ITALY, AND 57% IN GERMANY)

31%

BELIEVE COMPANIES HAVING MORE OF THEIR CUSTOMER DATA MEANS THEY CAN OFFER BETTER AND MORE PERSONALIZED PRODUCTS/SERVICES AND ONLY 26% WOULD GLADLY TRADE THEIR DATA FOR IMPROVED CUSTOMER EXPERIENCE AND SERVICES

50%

WOULD BE MORE LIKELY TO SHOP WITH A COMPANY THAT COULD PROVE IT TAKES DATA PROTECTION SERIOUSLY
(FOR INSTANCE, IF THEY COULD PROVIDE CLEAR GUIDANCE ON THEIR DATA PROTECTION AND PRIVACY POLICIES AND HOW DATA WOULD BE USED)

UNDER THE GDPR, INDIVIDUALS HAVE EXTENDED RIGHTS OVER THEIR PERSONAL DATA, INCLUDING THE RIGHT TO DATA 'PORTABILITY' (TO REQUEST A COPY OF ANY PERSONAL DATA HELD ON THEM), OR TO REQUEST THAT THEIR PERSONAL DATA IS RECTIFIED OR DELETED.

CONCLUSION

What This Means for Businesses

Privacy and data security is truly a global issue, which is apparent in both the survey responses and data protection regulations. For example, the GDPR will impact all companies that handle EU resident data – that includes businesses in post-Brexit Britain, U.S. cloud providers and any other organization doing business with residents of the EU.

The far-ranging nature of this legislation, rising consumer awareness, and the potential financial impact of customer backlash and regulatory action make it critical that businesses review their data collection and processing frameworks now, to understand their risk exposure in the future.

If a company fails to comply with the GDPR – for example, by not having the proper controls in place, losing customer data, or failing to make personal data available to data subjects within 'a reasonable time' – they may face fines of up to 4% of their global turnover, or €20 million, whichever is greater.

As businesses continue their digital transformations, making greater use of digital assets, services, and big data, they must also be accountable for monitoring and protecting that data on a daily basis.

When new regulations like the GDPR come into play, fines for violating data protection laws will grow, adding punitive damages to the other costs of a data breach. Before this happens, organizations need to know where data resides, who has access to it, and how it's being secured to understand the risk it brings to their business.

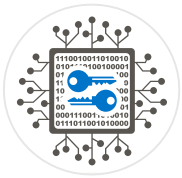
IF A COMPANY FAILS TO COMPLY WITH THE GDPR – FOR EXAMPLE, BY NOT HAVING THE PROPER CONTROLS IN PLACE, LOSING CUSTOMER DATA, OR FAILING TO MAKE PERSONAL DATA AVAILABLE TO DATA SUBJECTS WITHIN 'A REASONABLE TIME' – THEY MAY FACE FINES OF UP TO 4% OF THEIR GLOBAL TURNOVER, OR €20 MILLION, WHICHEVER IS GREATER.

RSA

STEPS BUSINESSES CAN TAKE TODAY

UNDERSTAND WHAT PERSONAL DATA YOU PROCESS:

It is not just understanding how PII is defined, but where it is stored, how it is used and who in your organization has access to it. Operationalize your thinking on all aspects of privacy.



ADDRESS PRIVACY AT EVERY LEVEL:

Establish ‘privacy by design’ by addressing privacy at every level – at the technology level and at the business level – it really must be a holistic approach to successfully converge business and security risk.

TAKE A RISK-BASED APPROACH:

Risk, data, security, and compliance teams must work together with line of business leaders to protect your organization and – more importantly – your customer data.

ENSURE YOUR APPROACH IS BLENDED:

Think about these four areas – Breach Response, Data Governance, Risk Assessment, and Compliance Management – as you build out your strategy. Are you ready for any kind of breach? How are you governing access to your data? How are you documenting your processing activities around your data so that you can put governance processes in place? An important part of that is assessing the risks around that data and then demonstrating compliance at the end.

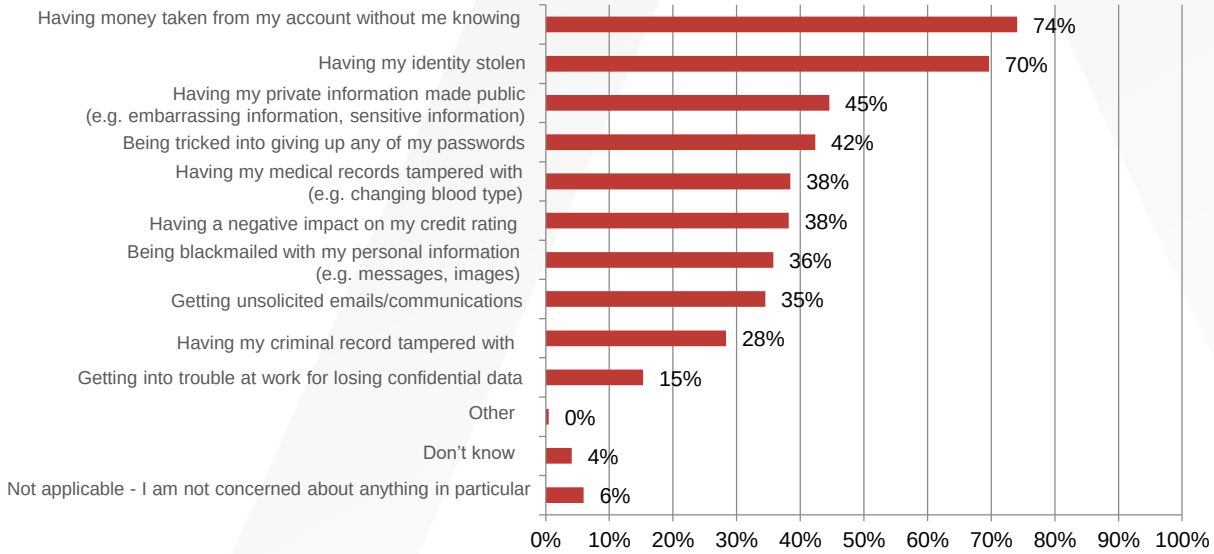
For more information about the GDPR and data privacy, please visit:
https://www.rsa.com/en-us/solutions/gdpr-compliance-with-rsa

RSA

FULL REPORT FINDINGS

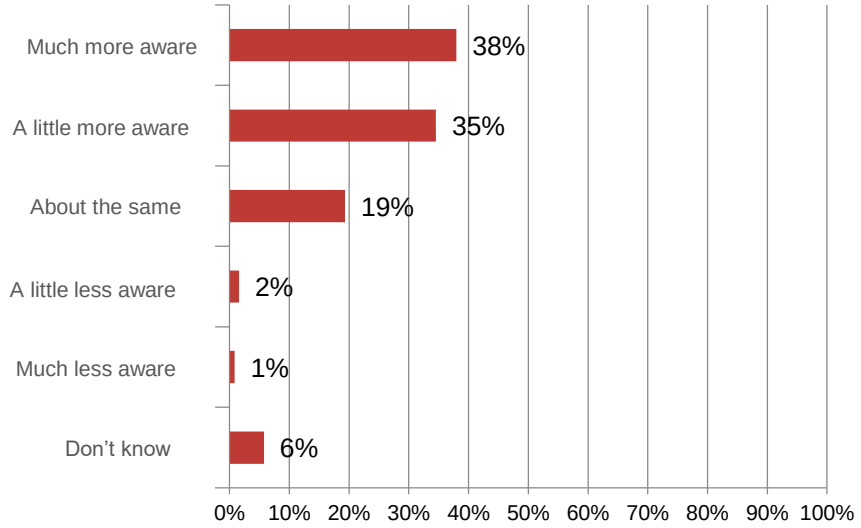
Which of the following types of personal information/data do you feel protective of?

Which, if any, of the following would you say you are concerned about?

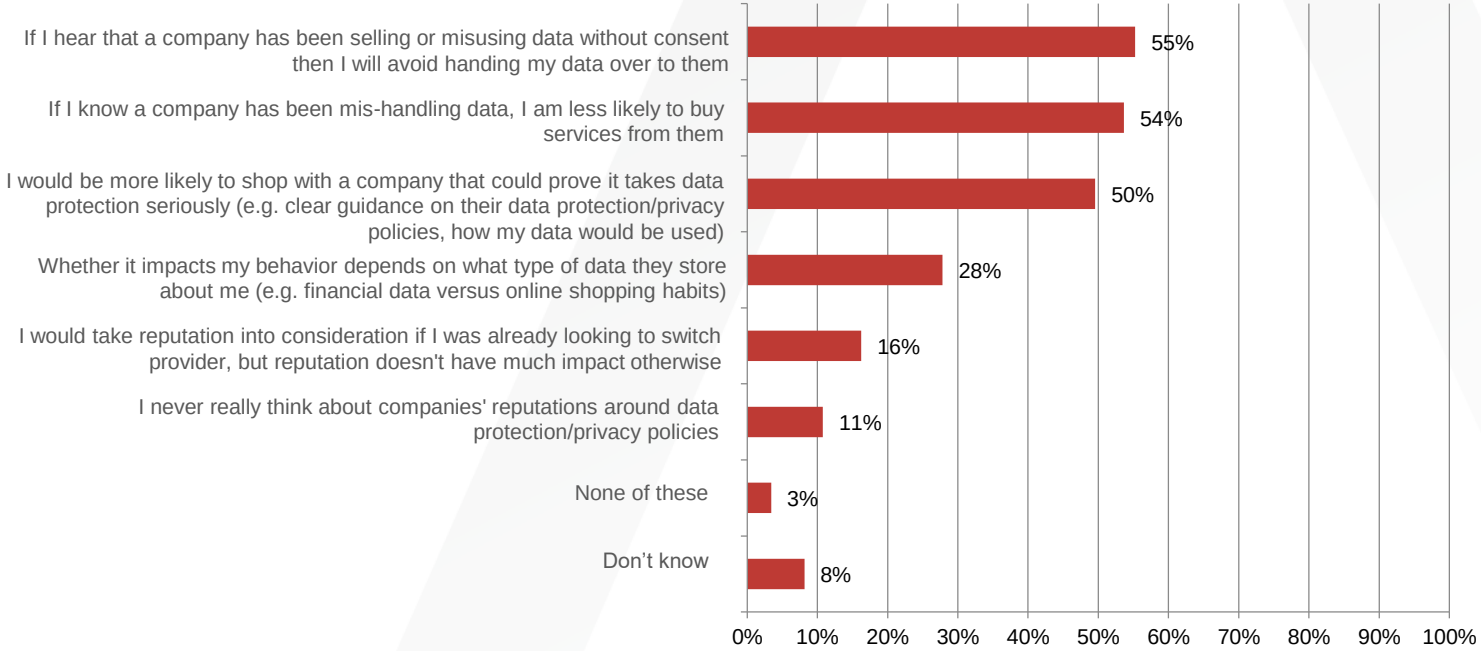


FULL REPORT FINDINGS

Would you say you are more or less aware of data breaches now compared to 5 years ago (i.e. in 2012)?

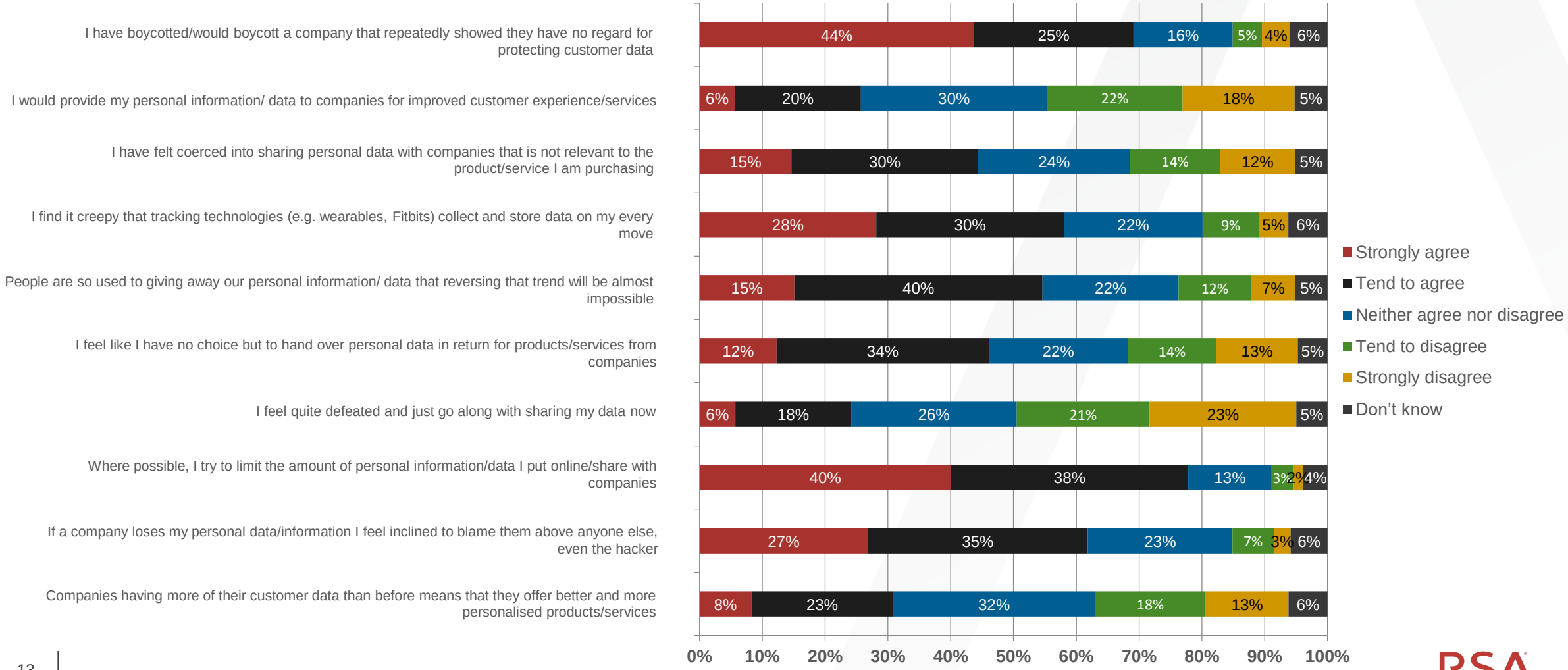


Which of the following statements apply to you?



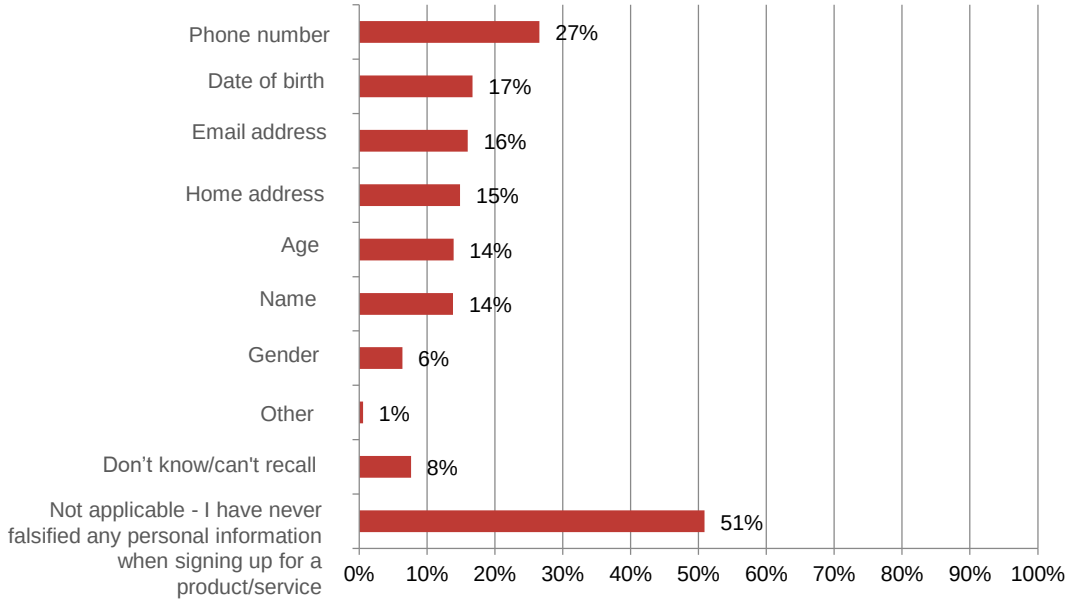
FULL REPORT FINDINGS

To what extent, if at all, do you agree or disagree with each of the following statements?



FULL REPORT FINDINGS

Which of the following pieces of personal information have you ever intentionally falsified when signing up for a product/service



You said you have intentionally falsified information when signing up for a product/service... Which of the following are reasons for this?