CONSUMER OPENNESS INDEX 2016

Where do you stand?

Stay Open. OX®

Foreword

Rafael Laguna, CEO, Open-Xchange

We're at a crossroads for data privacy and encryption. In a lot of ways, 2016 is a turning point for how the entire world will define these issues for years to come.

Governments and corporations are monitoring the general public more than ever and eroding civil liberties globally. Let's look at what has already been on the table this year: the replacement of Safe Harbor with a new data transfer agreement between the United States and European Union; the introduction of the Investigatory Powers Bill in the United Kingdom; the 2016 U.S. presidential election which has been filled with anti-encryption rhetoric. Add to that the debate between Apple and the U.S. government over unlocking one (or one hundred and seventy six, or all, depending on who you ask) iPhone, and the year is set to define political and personal stances on data privacy.

However, despite its prominence, the American presidential election might have the least direct impact on encryption policy. Safe Harbor, the Investigatory Powers Bill, and the Apple encryption case all have demonstrable impact on data privacy and are being pushed by legislators and law enforcement officials. Comparatively, the U.S. president has much less power to write policy regarding data privacy and encryption.

Yet, the results of the election – in a year that has emphasized encryption and digital privacy like never before – might be the clearest indicator of what the future entails for privacy advocates like myself. Neither the American public nor the country's president determines who agrees to a new Safe Harbor, what domestic British surveillance should or shouldn't look like, or even who leads Apple – but they do represent the will of the populace. This election, Americans will decide whether they will stake a firm stance on data privacy or consign themselves to the ad-hoc and silent erosion that is playing out every day.

And though 2016 opens with a focus on the United States, I do not expect that it will remain that way for long. As with the first Consumer Openness Index survey, we explored data privacy attitudes among the Internet-savvy populations in the U.S., UK, and Germany, with the goals of seeing how opinions have shifted over the past year and predicting what those shifts mean to the increasingly political debate of data privacy.

I expect 2016 will be represent a major opportunity for people to decide the future of data privacy. For those of you who have a direct vote in 2016, who have a chance to make your voice heard and tell your government that a compromise on privacy is a compromise on your rights, I ask that you don't waste it. For those of you whose efforts can – and will – come in other ways in 2016, I ask you to stay vigilant and protect your fundamental right to privacy.

Rafael
@rafbuff

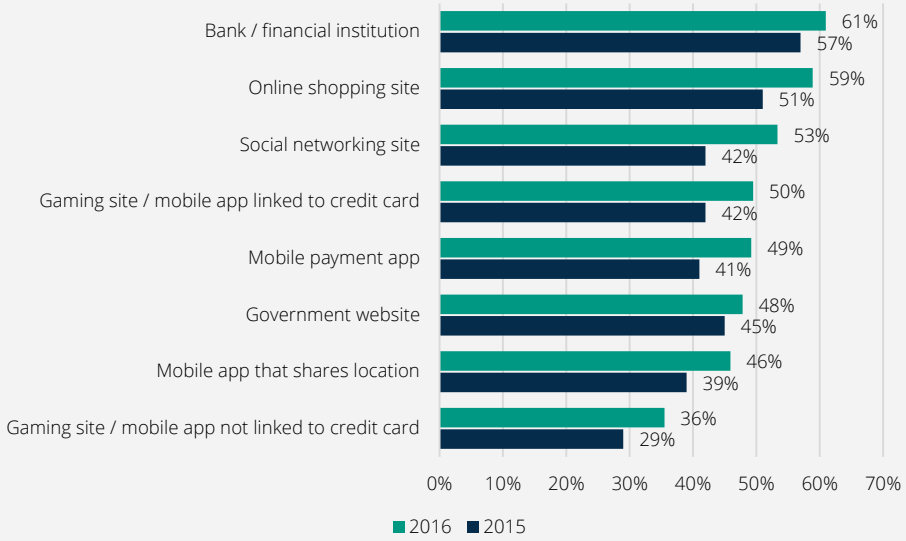
Changing Attitudes on Data Privacy

Events from the past year – the attacks in Paris and California, the striking down of Safe Harbor, the U.S. presidential election – have made data privacy issues internationally discussed and personally concerning.

Opinions about data privacy have hardened since we last published the Consumer Openness Index (COI) in 2015. The Internet-savvy populations in the U.S., UK, and Germany are more likely to report that they would stop using many types of companies if news of a privacy scandal emerged. The number of people who believe that companies such as Facebook, Twitter and Google never have the right to share their personal data is up, now representing 57% of the Internet users in the three countries.

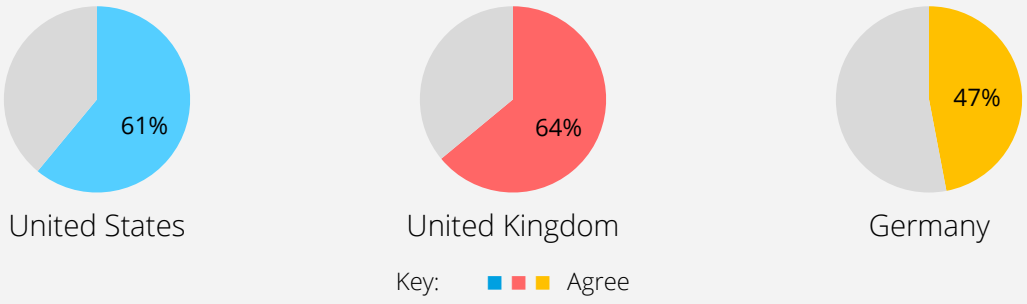
Which of the following types of companies, if any, would you immediately stop working with if there was news of a privacy scandal with that company?

In a new development since 2015, a majority of Internet users say they would stop using a social networking site if news of a privacy scandal emerged.



But in a finding that shows the nuanced views of many, a majority of Internet users in Germany – a country whose skepticism of surveillance was demonstrated last year - believes there are cases in which companies like Facebook, Twitter, and Google have the right to share their data.

[Companies like Facebook, Twitter, and Google] never have the right to share my data.



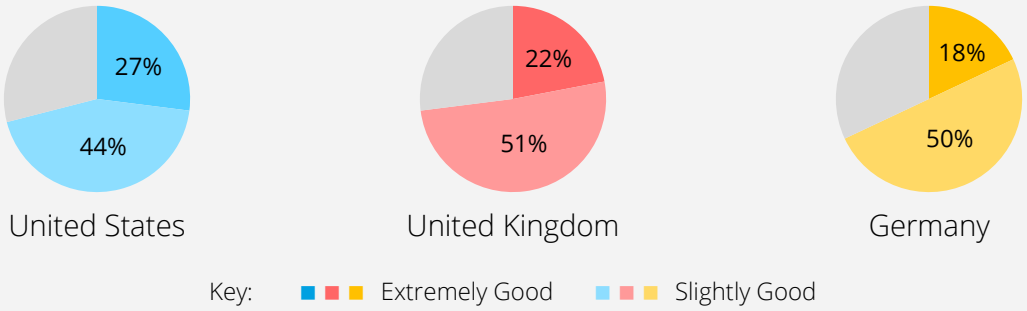
Given that Internet users are now more likely to take action in the event of a breach, the next question is: whose responsibility is it to stop one from occurring? In the case of the U.S. and UK, respondents are most likely to put that responsibility on the company that stores the data (43% and 48% of respondents, respectively), but in Germany, a plurality believes that the most responsibility lies with the user him- or herself (35%). Across the three countries, the proportion of Internet users who view themselves as the most responsible for preventing invasions of privacy increased since 2015 and now amounts to 31% of the population.

It is altogether concerning, then, that confidence in the ability to keep personal data private is down in 2016.

The percent of Internet users in the U.S., UK, and Germany who feel extremely good at keeping their personal data private is down by 5% since 2015.

Only 22% of Internet users in the three countries feel they are extremely good at keeping their personal data private, down from 27% in 2015. To sum up the situation in a few words: more people feel strongly about data privacy and their responsibility to protect it. But fewer actually think they're good at it.

How good do you think you are at keeping your personal data private when you are online?



In a new question posed in this year's COI, we asked respondents if their personal information had ever been compromised online. One in three respondents (31%) replied that they actually didn't know if their personal data had ever been compromised. This proportion remained relatively consistent across the countries, with UK Internet users expressing slightly more uncertainty (28% U.S., 36% UK, 28% Germany).

Paradoxically, this softening of confidence in the ability to keep personal data private coincides with a decrease in the use of several data protection measures – rather than adopting more measures to address their feelings of ineffectiveness, people are actually abandoning them. The proportion of respondents who report having strict privacy settings on their social media accounts and/or web browser is down by eight percentage points since last year. The proportion of Internet users who pay for a data privacy service is also down by three percentage points.

Perhaps most troubling: the use of email encryption, one of the most important and effective ways of protecting personal data, is down by eight percentage points since 2015.

In 2016, only one in five Internet users across the U.S., UK, and Germany uses email encryption. Looking at the countries themselves, email encryption is far more common in Germany; Germans are twice as likely as Americans to employ email encryption, and three times as likely as the British to do so (36% of Germans, compared to 18% of Americans and 12% of the British). Across the three countries, only 10% of Internet users report using encryption for email, messaging, voice chat, or other online communication all the time; 22% report using it some of the time.

In 2016, only one in five Internet users across the U.S., UK, and Germany uses email encryption. The reason this number is so low is the same as last year: there is no easy way to use it.

The reason why encryption is so rarely used remains the same as it was in 2015: difficulty of use. Eighty-eight percent of respondents in this year's COI reported that they would be interested in at least one encryption-related service, such as the ability to see who is monitoring or collecting their data or a one-click button that encrypts outgoing email. On average, only one in five respondents report that they use encryption as often as they would like to; in Germany, it is only one in seven.

What has prevented you from using encryption more often?

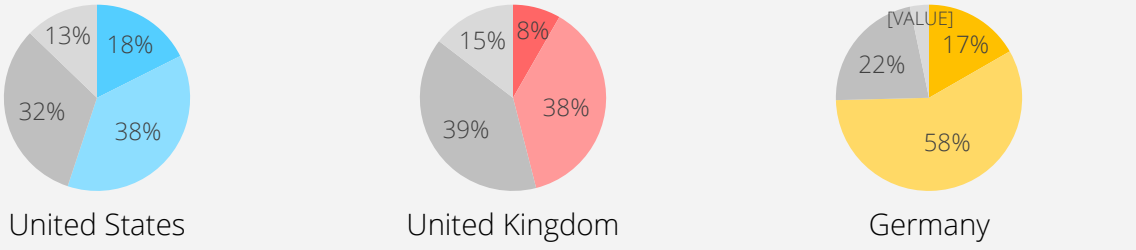
1. It seems too complicated to encrypt communications
   26% U.S.; 31% UK; 27% GER
2. There aren't enough easy ways to incorporate it
   23% U.S.; 25% UK; 23% GER
3. I don't share data over communications that I need to encrypt
   20% U.S.; 21% UK; 23% GER

Public Split on Government Access

Internet users agree that everyone has a fundamental right to privacy, but offer conflicting opinions on how, when, and whether government officials should be able to access the private data of their citizens.

The evidence is clear: 80% of Internet users agree that everyone has a fundamental right to privacy. The proportion is smaller, but a majority, 62%, is concerned about who in their government has access to their private data. But when asked how much attention they typically pay to the debate over balancing government surveillance with data privacy, responses vary widely by country.

How much attention do you typically pay to the debate over balancing government surveillance with data privacy?



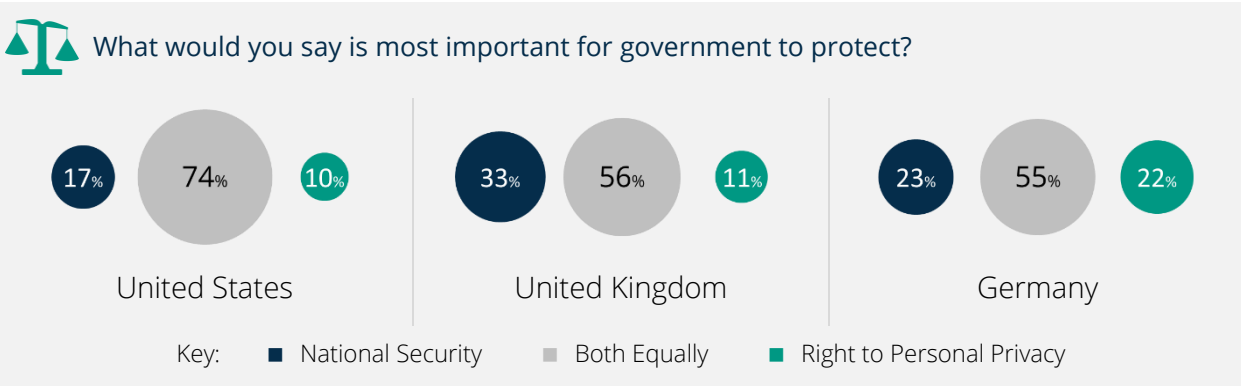
In the U.S. and Germany, a majority of Internet users pay at least somewhat close attention to the debate over balancing government surveillance with private data. Germany shows the highest proportion by far, with three quarters of its Internet-savvy population paying at least somewhat close attention to the debate. But in the United Kingdom, less than half of the Internet-savvy populace is paying attention to the debate. .

"Three quarters of German Internet users pay at least somewhat close attention to the debate over government surveillance and data privacy. Eighty one percent of American Internet users care about the data privacy positions of the presidential candidates. Where is this level of discourse in the United Kingdom?" – Rafael Laguna, CEO, Open-Xchange

In the United States, where the long presidential primary campaign is nearing its conclusion, 81% of Internet users report that they care about the candidates' positions on data privacy, and a slight majority (51%) believe that the candidates should pay more attention to the subject. The issues at stake affect more than just America, according to majorities in all three countries. Sixty-three percent of Internet users across all three countries believe that the

presidential elections will impact government policy on data privacy around the world; in Germany, that proportion is 77%.

However, it is also clear that many people either haven't staked a firm position for or against government intrusion in their data, or they hold a highly nuanced view. Majorities in all three countries answered that it is most important for governments to equally protect the personal freedom of speech and right to personal privacy. Majorities also responded that it is most important for governments to equally protect national security and the right to personal privacy. In theory, this is an understandable view; in practice, it is tenuous at best.

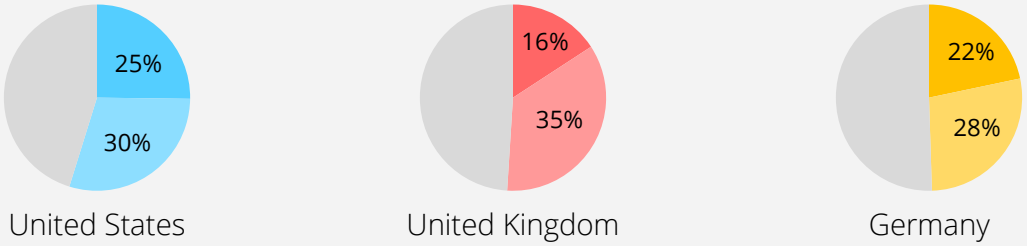


The topic of "back doors" that unlock encrypted devices and communication has increasingly been discussed in the international media conversation over the past year, coming to a new head with Apple's refusal to unlock the phone of one of the attackers involved in the recent attack in San Bernardino, California. We can't predict which way public opinion will eventually sway in the case of Apple – a recent study by Pew found that a majority support the government – but at the very least, majorities in all three countries understand and appreciate the reasoning behind its argument.

Sixty-eight percent of Internet users in the U.S., UK, and Germany believe that building back doors into encrypted systems will make it easier for criminals to steal personal data – and nearly the exact same percent (69%) believe that it will make it easier for government officials to access encrypted data. Reflecting the jaded sense that many have about government surveillance, half of Internet users in all three countries believe that there is no need for back doors anyways – governments will be able to access their data no matter what they do.

"Half of our respondents think that there isn't a need to build "back doors" to encryption, because governments will be able to access their data no matter what they do. First, that isn't true – and second, I don't think that's a healthy way to approach this debate." – Neil Cook, Chief Security Architect, Open-Xchange

There is no need for [encryption] "back doors" - governments will be able to access my data no matter what I do.

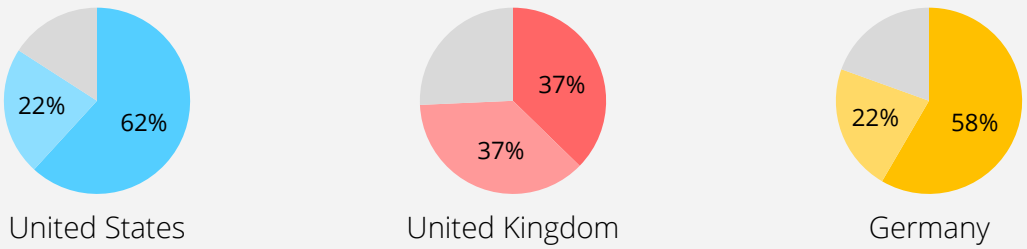


Data privacy is even more political in 2016

Right from the start, Apple and the US Government brought data privacy to the front of the international political conversation, but it is only the continuation of a politicization that grew throughout 2015. The presidential election in the U.S., the introduction of the "Snooper's Charter" in the UK, and the invalidation of the Safe Harbor agreement in the European Union have strengthened political lines and encouraged politicians to take firmer stances for or against data privacy.

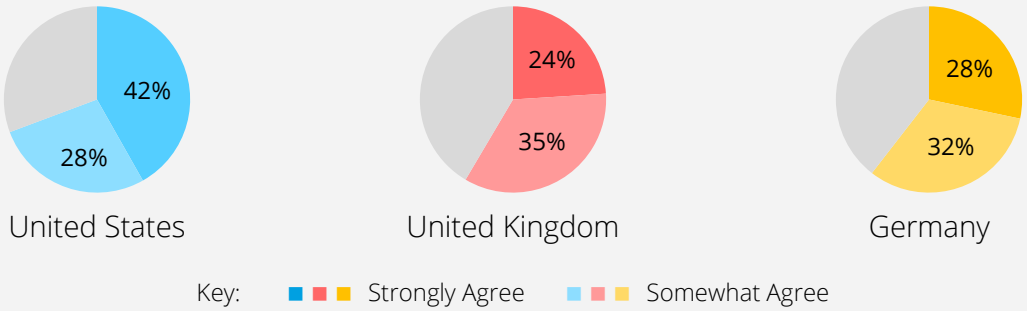
Looking to the United States, responses suggest that Internet-savvy voters want data privacy to be a bigger topic during the presidential election. Eighty-one percent of Internet users say that they care a lot about the data privacy positions of the candidates, and 51% believe that the candidates should pay more attention to data privacy. However, few actually understand the candidates' positions on the subject. When asked to identify the general positions each candidate has taken on the issue, at least 40% of respondents answered "don't know" for each one. In the end, a majority of American respondents indicated that a candidate's position on data privacy would impact their decision to vote for him or her, and only one in five say that the impact would be significant.

Everyone has a fundamental right to privacy.



Travelling across the Atlantic, the introduction of the Investigatory Powers Bill, known (derisively) to some as the Snooper's Charter, has divided the electorate and brought the issue of data privacy to further prominence. According to our findings in this year's COI, equal proportions of the Internet-savvy electorate believe that the introduction of the bill was justified (23% agree, 22% disagree, 54% unsure). One in four respondents indicated that they would be less likely to support a political party if a majority voted in favor of the bill (25%), more than the one in seven (15%) who indicated that a party's support would not affect their voting decision, but the majority (60%) is unsure. Regardless of opinion on the bill, one finding is clear: a majority (53%) believe that Home Secretary Theresa May has not adequately explained the impact of the bill and presented a balanced argument for its introduction.

I am concerned about who in the government has access to my data.



Transitioning to Germany, public skepticism of government surveillance – which was reflected in the 2015 COI – has remained constant in response to political events. Nearly half of German Internet users (46%) are favorable towards the European Court of Justice's decision to invalidate Safe Harbor, far more than those who were unfavorable towards the decision (25%). Germans remain skeptical of government collection of their data; half believe that German companies should not pass along personal data to the German government, if requested (49%), and a strong majority believe that German companies should not pass along personal data to the American government (76%). However, reflecting the nuanced view that many across these three countries hold, Germans are more likely to believe that companies like Facebook, Twitter, and Google have the right to share personal data when it helps law enforcement or government agencies keep them safer (34% of Germans vs. 21% of Americans and 21% of the British).

Conclusion: Preparing for an influential 2016

The past year has shown conflicting reactions to the battle over data privacy that is playing out on an increasingly public stage. Internet users in each of the three countries care more about keeping their data private, but are less confident in their ability to do so and are taking fewer actions to protect their privacy.

As we wrap up this year's Consumer Openness Index, new developments are emerging – at times hourly – about the competing narratives offered by Apple and the U.S. Government. The case, which will likely impact data privacy efforts across the globe, may be the tipping point in many people's minds. Are we comfortable with government officials having access to our data? If yes, who else are we comfortable with having it? If no: the same question still applies.

Respondents in 2016 offered stronger opinions than last year. They said that they are more likely to sever ties with many types of services if news of a privacy scandal breaks, even omnipresent social media platforms. The percent of Internet users who believe that companies like Facebook, Twitter, and Google *never* have the right to share their data went up. At least one in three Internet-savvy citizens in the U.S., UK, and Germany indicate that a candidate's stance on data privacy will at least moderately impact the decision of who to vote for in their country's next national elections.

We believe in the right to privacy, but have a hard time balancing it with our belief in the right to security. This year – 2016 – is when many will have to make up their minds.

Eighty percent of respondents believe in a fundamental right to privacy, but more than half believe that the government should be able to access encrypted files to keep them safe from foreign attack. We expect that as this year unfolds, these questions will be asked in increasingly specific contexts.

It has worked out that the United States is home to the year's first major tests of how data privacy and government surveillance will be balanced in practice – the Apple encryption case and the upcoming presidential election – but it won't stay that way for long. Bills, treaties, civil cases, executive actions, summits, business decisions, petitions, protests; we anticipate that 2016 will be a year when people across the world are faced with specific, hard questions about how much they are willing to sacrifice their privacy to accomplish other goals.

To American voters, we challenge you to do your homework, ask hard questions, and consider data privacy when casting your ballot in November. To the media, we challenge you to not shirk from publicizing this critical debate and keeping it in the public consciousness. To business owners, we challenge you to take note of these findings and recognize how important it is to keep your customers' data safe as growing numbers of breaches diminish customer trust and

threaten your livelihood. And to Internet users across the globe, we challenge you to pay attention in 2016. This is a year when decisions are going to be made across businesses and governments, when true leadership in data privacy has the potential to emerge, and it is up to you to voice your opinions.

It's your year. Use it.

Methodology

To complete the Consumer Openness Index 2016, Open-Xchange worked with March Communications to design a survey that would explore attitudes and behaviors towards data privacy among Internet users. The survey of 3,000 Internet users was fielded by independent research company OnePoll and spanned audiences of 1,000 each in the United States, United Kingdom, and Germany. The margin of error is ± 1.8% across all three countries, and ± 3% within each country. All stated differences from last year's Consumer Openness Index are statistically significant at the 95% confidence level.

Full Results

The sample size for each country is n=1,000 people, aged 18+, who use the Internet at least three times per week.

6. How good do you think you are in general at keeping your personal data private when you are online?	USA	UK	Germany
Extremely good	27%	22%	18%
Slightly good	44%	51%	50%
Neither good nor bad	23%	23%	25%
Slightly bad	5%	3%	6%
Extremely bad	1%	0%	1%

7. What actions do you take to keep your personal data private online?	USA	UK	Germany
Email encryption	18%	12%	36%
I don't put personal information about myself online	38%	50%	47%
I don't make any financial transactions online	15%	8%	17%
I have strict privacy settings on my social media accounts and/or web browser, etc.	38%	40%	37%
I have requested for my information to be removed from sites	20%	17%	10%
I pay for a service to keep my personal data private online	10%	5%	10%
I double-check to make sure the URL is correct (and the website is not spoofed) before transmitting personal data	41%	44%	45%
I enable two-step authentication on websites	18%	23%	17%
I use security-related browser extensions	38%	27%	40%
I check the status of the SSL certifications on websites	29%	28%	34%
None of the above	14%	11%	7%

8. You indicated earlier that your job entails a significant amount of time spent working on a computer. How much do you know about the personal data your employer collects from your computer activity?	USA	UK	Germany
I am completely aware of the personal data my employer collects from my computer activity	54%	34%	52%
I am somewhat aware of the personal data my employer collects from my computer activity	25%	40%	31%
I am not aware of the personal data my employer collects from my computer activity	21%	26%	17%

9. Have you ever had personal information compromised online?	USA	UK	Germany
My personal information has been compromised at least once in the past year.	10%	5%	6%
My personal information has been compromised, but it was more than one year ago.	15%	10%	14%
I don't know if my private information has been compromised.	28%	36%	28%
My personal information has never been compromised.	48%	49%	52%

10. [IF INFORMATION HAS BEEN COMPROMISED] What information of yours was compromised?	USA	UK	Germany
Demographic information (e.g. name, age, address, phone number)	33%	24%	45%
Government information (e.g. passport number, social security number, national insurance number)	18%	17%	16%
Financial information (e.g. bank account number, credit card information, purchase history)	63%	51%	36%
Other information	16%	16%	24%
None of the above / I don't know what information of mine was compromised.	3%	4%	2%
None of the above / I prefer not to answer.	2%	6%	1%

11. [IF PARENT OF CHILD UNDER 18 LIVING IN HOME] How good do you think <u>your child or children</u> (thinking of those aged under 18 who live at your house/place of residence) are at keeping their personal data private when they are online?	USA	UK	Germany
Extremely good	26%	14%	29%
Slightly good	24%	27%	33%
Neither good nor bad	14%	23%	17%
Slightly bad	5%	8%	6%
Extremely bad	6%	2%	1%
Don't know	8%	5%	3%
N/A - none of my children access the Internet	17%	21%	10%

12. [IF PARENT OF CHILD UNDER 18 LIVING IN HOME] Has your child or children (thinking of those aged under 18 who live at your house/place of residence) had their personal information compromised online?	USA	UK	Germany
At least one of my children has had their personal information has been compromised in the past year.	5%	5%	4%
At least one of my children has had their personal information has been compromised, but it was more than one year ago.	5%	8%	9%
I don't know if their private information has been compromised.	20%	27%	21%
Their personal information has never been compromised.	70%	60%	66%

13. In which cases do you believe companies like Facebook, Twitter and Google have the right to share your data, i.e. your "likes," your location, your marital status, etc.?	USA	UK	Germany
When my data helps make ads shown to me more interesting or relevant	12%	8%	14%
When my data helps those sites better understand overall human behavior	10%	9%	13%
When my data helps me automatically log into other sites or applications	16%	10%	13%
When my data helps another business serve me better	12%	8%	13%
When my data helps law enforcement or government agencies keep me safer	21%	21%	34%
None - They never have the right use my public data	61%	64%	47%
Other	1%	2%	1%

14. In your opinion, who is most responsible for ensuring online companies do not invade their users' privacy?	USA	UK	Germany
The user	34%	25%	35%
The company itself	43%	48%	26%
The government	9%	13%	20%
A third-party online privacy institution	4%	4%	13%
Other person	0%	0%	2%
None / I don't know	9%	11%	6%

15. Which of the following types of companies, if any, would you immediately stop working with if there was news of a privacy scandal with that company?	USA	UK	Germany
A social networking site	53%	48%	59%
A gaming site or mobile application that is linked with my credit card	47%	49%	53%
A gaming site or mobile application that is not linked with my credit card	36%	34%	37%
An online shopping site	62%	57%	58%
A bank or other financial institution	63%	59%	62%
A mobile application that helps me pay for things with my phone or tablet	48%	49%	51%
A mobile application that tells people my location	45%	47%	46%
A government website with access to my personal information	51%	44%	48%
None of the above / N/A	14%	16%	6%

16. How familiar are you with the concept of encryption, defined as: "Encryption is a way to make a message or file more secure by scrambling the contents so that it can be read only by someone who has the password to unscramble it."	USA	UK	Germany
Extremely familiar	15%	10%	7%
Very familiar	20%	20%	24%
Somewhat familiar	38%	39%	43%
Not very familiar	16%	20%	20%
Not at all familiar	11%	13%	6%

17. Do you currently use encryption for your email, messaging, voice chat, or any other form of online communication? (Please note, certain messaging apps have encryption built in, e.g. WhatsApp. If you are unsure, please select "I don't know")	USA	UK	Germany
Yes, all of the time	11%	5%	14%
Yes, some of the time	17%	19%	30%
Yes, rarely	8%	10%	21%
No, never	29%	31%	14%
I don't know	35%	36%	22%

18. How likely are you to use encryption for your email, messaging, voice chat or any other form of online communication in the future?	USA	UK	Germany
Extremely likely - I do not use it but I will	8%	3%	1%
Very likely	8%	6%	15%
Somewhat likely	33%	38%	37%
Not very likely	36%	42%	40%
Not at all likely	15%	12%	7%

19. What would make you more likely to use encryption on more of your online communications?	USA	UK	Germany
Instruction on how to use encryption	43%	42%	40%
An easy to way to make something encrypted at the click of a button	57%	52%	55%
Encryption coming standard with my programs and applications	51%	52%	40%
A better understanding of what it means to use encryption	38%	35%	34%
None / Nothing would make me more likely to use encryption	13%	13%	7%
Other	1%	1%	1%

20. What has prevented you from using encryption more often?	USA	UK	Germany
It doesn't seem to be that helpful for keeping my data private	5%	4%	9%
I don't share data over communications that I need to encrypt	20%	21%	23%
It seems too complicated to encrypt communications	26%	31%	27%
It seems too complicated to give others a password to see my communications	18%	21%	20%
Nothing will ever keep my data completely private	16%	16%	19%
There aren't enough easy ways to incorporate it	23%	25%	23%
I understand it, but the people I'm communicating with don't	11%	12%	21%
None / Nothing has prevented me from using encryption more often / I use it as often as I want to	27%	21%	15%
Other	4%	4%	1%

21. Assuming that adoption was easy and cheap, which encryption-related services would you be interested in using?	USA	UK	Germany
The ability to see who is monitoring or collecting my data	53%	47%	52%
The ability to track where my personal data goes after submitting it - similar to how postal services allow you to track packages along a delivery route	46%	39%	43%
A one-click button that encrypts outgoing e-mail	51%	51%	44%
A program that easily encrypts files	50%	45%	49%
A program that runs in the background of your computer or mobile device that encrypts all transmitted data	47%	44%	47%
None of the above	14%	15%	8%
Other	0%	1%	0%

23. How much attention do you typically pay to the debate over balancing government surveillance with data privacy?	USA	UK	Germany
Very close attention	18%	8%	17%
Somewhat close attention	38%	38%	58%
Not much attention	32%	39%	22%
No attention at all: I never pay attention to the debate over balancing government surveillance with data privacy	13%	15%	3%

24. Which would you say is most important for government to protect?	USA	UK	Germany
Personal freedom of speech	5%	11%	15%
Right to personal privacy	14%	21%	30%
Both equally	81%	69%	56%

25. Which would you say is most important for government to protect?	USA	UK	Germany
National security	17%	33%	23%
Right to personal privacy	10%	11%	22%
Both equally	74%	56%	55%

27. How much do you agree or disagree with the following statements relating to encryption and government access?	USA	UK	Germany
The government should be able to access encrypted files to keep us safe from foreign attack.			
Strongly agree	30%	27%	20%
Somewhat agree	28%	36%	27%
Neither agree nor disagree	26%	27%	30%
Somewhat disagree	8%	6%	12%
Strongly disagree	8%	5%	11%
Law enforcement officials should be able to access encrypted files to catch criminals.			
Strongly agree	25%	26%	25%
Somewhat agree	34%	37%	32%
Neither agree nor disagree	26%	28%	27%
Somewhat disagree	7%	5%	9%
Strongly disagree	9%	4%	7%
Everyone has a fundamental right to privacy.			
Strongly agree	62%	37%	58%
Somewhat agree	22%	37%	22%
Neither agree nor disagree	13%	21%	14%
Somewhat disagree	2%	4%	4%
Strongly disagree	1%	1%	2%
I am concerned about who in the government has access to my data.			
Strongly agree	42%	24%	28%
Somewhat agree	28%	35%	32%
Neither agree nor disagree	21%	30%	28%
Somewhat disagree	6%	9%	8%
Strongly disagree	4%	3%	3%
I think that national security officials should be able to access personal data.			
Somewhat agree	16%	19%	9%
Somewhat agree	29%	36%	17%
Neither agree nor disagree	30%	29%	30%
Somewhat disagree	12%	10%	21%
Strongly disagree	14%	6%	23%
I think that law enforcement officials should be able to access personal data.			
Somewhat agree	13%	14%	17%
Somewhat agree	25%	33%	29%
Neither agree nor disagree	31%	34%	29%
Somewhat disagree	14%	12%	14%
Strongly disagree	17%	7%	11%

I think the government should be able to monitor personal data, but not store it on their servers for any length of time.			
Somewhat agree	17%	14%	14%
Somewhat agree	29%	39%	28%
Neither agree nor disagree	30%	32%	31%
Somewhat disagree	10%	9%	13%
Strongly disagree	13%	6%	13%
I think that companies should attempt to block government requests for personal data.			
Somewhat agree	25%	12%	24%
Somewhat agree	23%	20%	30%
Neither agree nor disagree	38%	43%	34%
Somewhat disagree	10%	17%	9%
Strongly disagree	5%	8%	4%
I would be comfortable with my government sharing my personal data with foreign allies.			
Somewhat agree	7%	7%	5%
Somewhat agree	7%	12%	12%
Neither agree nor disagree	17%	26%	23%
Somewhat disagree	15%	24%	21%
Strongly disagree	54%	32%	40%
Other countries are more effective at enforcing data privacy than my own.			
Somewhat agree	13%	8%	13%
Somewhat agree	16%	17%	20%
Neither agree nor disagree	53%	65%	47%
Somewhat disagree	11%	8%	13%
Strongly disagree	8%	3%	7%

28. Some officials have called for the creation of "back doors" in encrypted networks that enable governments to easily access encrypted files. How much do you agree or disagree with the following statements related to these "back doors"?	USA	UK	Germany
"Back doors" built into encryption networks will enable government officials to access encrypted data.			
Somewhat agree	31%	19%	21%
Somewhat agree	30%	41%	32%
Neither agree nor disagree	33%	37%	35%
Somewhat disagree	3%	2%	7%
Strongly disagree	3%	1%	5%
Building "back doors" into encryption networks will make it easier for criminals to steal personal data.			
Somewhat agree	33%	22%	24%
Somewhat agree	28%	36%	31%
Neither agree nor disagree	34%	39%	35%
Somewhat disagree	4%	3%	7%
Strongly disagree	2%	1%	2%
"Back door" policies in certain countries will encourage business to relocate to where their data is more secure.			
Somewhat agree	20%	14%	19%
Somewhat agree	30%	31%	30%
Neither agree nor disagree	42%	49%	39%
Somewhat disagree	5%	5%	9%
Strongly disagree	2%	1%	3%
There is no need for "back doors" - governments will be able to access my data no matter what I do.			
Somewhat agree	25%	16%	22%
Somewhat agree	30%	35%	28%
Neither agree nor disagree	34%	40%	35%
Somewhat disagree	7%	8%	11%
Strongly disagree	4%	2%	4%

29. In your country's next national election, how much do you think a candidate's position on data privacy would/will impact your decision about whether or not to vote for him/her?	USA	UK	Germany
It would/will have a significant impact on my decision	19%	9%	21%
It would/will have a moderate impact on my decision	23%	25%	35%
It would/will have a small impact on my decision	23%	24%	21%
It would/will not impact my decision at all	15%	22%	14%
I'm not sure	20%	21%	8%

31. Do you think that the US presidential candidates should pay more, less, or the same amount of attention to data privacy?	USA	UK	Germany
The candidates should pay more attention to data privacy	51%		
The candidates should pay less attention to data privacy	3%		
The candidates should pay the same amount of attention to data privacy as they currently do	27%		
None of the above / I don't know	19%		

32. How much do you personally care about the data privacy positions of the presidential candidates overall?	USA	UK	Germany
I care a lot about the data privacy positions of the candidates	37%		
I care a little about the data privacy positions of the candidates	44%		
I don't care at all about the data privacy positions of the candidates	19%		

33. How much do you agree or disagree with the following statements relating to the presidential election?	USA	UK	Germany
I want the next U.S. president to do more to protect data privacy.			
Somewhat agree	34%		
Somewhat agree	34%		
Neither agree nor disagree	30%		
Somewhat disagree	2%		
Strongly disagree	1%		
I think the next U.S. president should defer more to defense and intelligent experts when crafting data privacy policy.			
Somewhat agree	26%		
Somewhat agree	33%		
Neither agree nor disagree	33%		
Somewhat disagree	4%		
Strongly disagree	3%		
I want the next U.S. president to prioritize data privacy over defense concerns.			
Somewhat agree	17%		
Somewhat agree	19%		
Neither agree nor disagree	39%		
Somewhat disagree	16%		
Strongly disagree	9%		

I want the next U.S. president to prioritize defense concerns over data privacy.			
Somewhat agree	28%		
Somewhat agree	30%		
Neither agree nor disagree	34%		
Somewhat disagree	5%		
Strongly disagree	3%		

34. Focusing on the U.S. presidential election, how do you think the election of a candidate who is <u>against data privacy protections</u> would affect your personal view of the United States as a whole?	USA	UK	Germany
It would positively affect my opinion of the country.	18%	7%	8%
It would negatively affect my opinion of the country.	36%	28%	50%
It would have no impact on my opinion of the country.	21%	35%	29%
I don't know	26%	30%	13%

35. To what extent do you think the U.S. presidential elections will impact the government policy on data privacy <u>around the world</u>?	USA	UK	Germany
I think they will have a large impact on government policy around the world	18%	12%	21%
I think they will have a moderate impact on government policy around the world	22%	24%	36%
I think they will have a small impact on government policy around the world	18%	20%	20%
I think they will not impact government policy at all around the world	13%	12%	11%
I don't know	29%	32%	12%

37. Based on what you know, what do you think are the positions of the below candidates concerning data privacy? Do you feel they are generally in favor of data privacy, against it, neutral, or do you not know for sure?	USA	UK	Germany
Donald Trump			
Generally for	21%		
Generally neutral	13%		
Generally against	24%		
Don't know	43%		
Ted Cruz			
Generally for	14%		
Generally neutral	18%		
Generally against	19%		
Don't know	50%		
Marco Rubio			
Generally for	12%		
Generally neutral	20%		
Generally against	16%		
Don't know	52%		
Ben Carson			
Generally for	14%		
Generally neutral	17%		
Generally against	16%		
Don't know	53%		
Jeb Bush			
Generally for	11%		
Generally neutral	18%		
Generally against	22%		
Don't know	49%		
Chris Christie			
Generally for	9%		
Generally neutral	18%		
Generally against	20%		
Don't know	53%		
John Kasich			
Generally for	7%		
Generally neutral	19%		
Generally against	15%		
Don't know	60%		
Carly Fiorina			
Generally for	10%		
Generally neutral	18%		
Generally against	17%		

Don't know	55%		
Rand Paul			
Generally for	15%		
Generally neutral	18%		
Generally against	15%		
Don't know	53%		
Mike Huckabee			
Generally for	10%		
Generally neutral	18%		
Generally against	18%		
Don't know	55%		
Hillary Clinton			
Generally for	25%		
Generally neutral	14%		
Generally against	22%		
Don't know	40%		
Bernie Sanders			
Generally for	21%		
Generally neutral	17%		
Generally against	15%		
Don't know	48%		
Martin O'Malley			
Generally for	6%		
Generally neutral	21%		
Generally against	12%		
Don't know	61%		

38. Which candidate do you think is the most clear about his or her position on data privacy and protecting consumer data?	USA	UK	Germany
Marco Rubio	12%		
Mike Huckabee	10%		
Hillary Clinton	25%		
Rand Paul	15%		
Martin O'Malley	6%		
Donald Trump	21%		
Bernie Sanders	21%		
Jeb Bush	11%		
John Kasich	7%		
Ted Cruz	14%		
Ben Carson	14%		
Chris Christie	9%		
Carly Fiorina	10%		
N/A - there are two or more candidates whose position I feel is equally clear	0%		
None of the above / Don't know	0%		

40. To what extent do you agree that UK companies (high-street banks such as RBS or retailers such as M&S) should have the right to pass personal data to the UK Government and third parties, if requested?	USA	UK	Germany
Strongly agree		7%	
Somewhat agree		25%	
Neither agree nor disagree / Unsure		32%	
Somewhat disagree		19%	
Strongly disagree		16%	

41. To what extent do you agree that American companies (US owned retailers such as Asda or online service providers such as Facebook or Amazon) should have the right to pass on personal data to the American Government and third parties, if requested?	USA	UK	Germany
Strongly agree		5%	
Somewhat agree		16%	
Neither agree nor disagree / Unsure		29%	
Somewhat disagree		22%	
Strongly disagree		27%	

42. Do you believe the introduction of the Investigatory Powers Bill is justified?	USA	UK	Germany
Yes		23%	
No		22%	
Unsure		54%	

43. Would you be more likely or less likely to support a political party if the majority of their members voted in favour of the Investigatory Powers Bill?	USA	UK	Germany
More likely		15%	
Less likely		25%	
Unsure		60%	

44. Would you consider joining legal action against an organisation if you believed its processes for handling your data infringed your privacy?	USA	UK	Germany
Yes		33%	
No		18%	
Unsure		48%	

45. Do you believe the Home Secretary, Theresa May, who is spearheading the introduction of the Investigatory Powers Bill, has the right to pass legislation that will enable the Government to access your mobile and Internet data?	USA	UK	Germany
Yes		26%	
No		39%	
Unsure		35%	

46. Do you believe Home Secretary, Theresa May, has adequately explained the impact of the Investigatory Powers Bill to the UK public and presented a balanced argument for its introduction?	USA	UK	Germany
Yes		12%	
No		53%	
Unsure		35%	

47. How much do you agree or disagree with the following statements concerning David Cameron's moves to weaken (or ban) encryption on devices used in the UK?	USA	UK	Germany
The moves to weaken or ban encryption infringe on the right to privacy of UK citizens.			
Strongly agree		19%	
Somewhat agree		31%	
Neither agree nor disagree		42%	
Somewhat disagree		7%	
Strongly disagree		1%	
The reputational damage caused by the Investigatory Powers Bill will be bad for UK businesses.			
Strongly agree		14%	
Somewhat agree		26%	
Neither agree nor disagree		48%	
Somewhat disagree		11%	
Strongly disagree		2%	
Weakened encryption will make investment in the UK less attractive to foreign companies.			
Strongly agree		14%	
Somewhat agree		28%	
Neither agree nor disagree		50%	
Somewhat disagree		8%	
Strongly disagree		2%	
Some UK businesses will move operations abroad to avoid sharing their information with the government.			
Strongly agree		16%	
Somewhat agree		30%	
Neither agree nor disagree		46%	
Somewhat disagree		7%	
Strongly disagree		2%	
Making personal data easier for government officials to access will also make it easier for criminals to access that data as well.			
Strongly agree		24%	
Somewhat agree		36%	
Neither agree nor disagree		34%	
Somewhat disagree		5%	
Strongly disagree		1%	
Weakening encryption protections will help law enforcement catch cybercriminals and protect the country.			
Strongly agree		13%	
Somewhat agree		30%	
Neither agree nor disagree		42%	

Somewhat disagree		10%	
Strongly disagree		5%	

49. Do you think that German companies should pass along personal data to the German government, if requested?	USA	UK	Germany
Strongly agree			7%
Somewhat agree			16%
Neither agree nor disagree / Unsure			28%
Somewhat disagree			22%
Strongly disagree			27%

50. Do you think that German companies should pass along personal data to the American government, if requested?	USA	UK	Germany
Strongly agree			3%
Somewhat agree			7%
Neither agree nor disagree / Unsure			15%
Somewhat disagree			18%
Strongly disagree			58%

51. How well-informed do you think you are about the European Court of Justice's decision last year to invalidate the Safe Harbor data transfer agreement between the European Union and the United States of America?	USA	UK	Germany
Very well-informed			9%
Somewhat informed			41%
Not informed at all			50%

52. For your information, the Safe Harbor agreement allowed American companies operating within Europe to collect and process E.U. customer data on servers located in the U.S. The European Court of Justice declared that, given the legal ability of U.S. intelligence agencies to request access to data housed on servers located in the U.S., the conditions of Safe Harbor did not provide adequate protections for the personal data of E.U. citizens.			
To what extent are you favorable or unfavorable towards the Court's decision to declare Safe Harbor invalid?	USA	UK	Germany
Very favorable			24%
Somewhat favorable			22%
Neither favorable nor unfavorable			29%
Somewhat unfavorable			13%
Very unfavorable			12%