



MEF



GLOBAL CONSUMER TRUST REPORT 2017

CONSUMER INSIGHTS
TO UNDERSTAND THE IMPACT,
CHALLENGES AND OPPORTUNITIES OF
BUILDING TRUST IN PERSONAL DATA



IN ASSOCIATION WITH **FORGEROCK**

CONTENTS

- FOREWORD.....3
- EXECUTIVE SUMMARY.....4
- BUILDING TRUST IN THE MOBILE ECOSYSTEM.....9
- BEHAVIOURS AND ATTITUDES IN THE PERSONAL DATA ECONOMY.....18
- CONSUMER APPETITE FOR DATA-DRIVEN PRODUCTS AND SERVICES.....26
- APPENDIX.....35
- ABOUT THE STUDY.....46



CONSUMERS WANT TO BE CONNECTED, PROTECTED AND RESPECTED.

It's no secret. We are in the midst of a digital revolution. And consumers want to be connected to everything, by everything, and from anywhere. They expect to connect to services with the same omnichannel experience whether from a computer or a mobile device. Security, privacy, identity and digital transformation professionals must ask the question: "Has anything changed since last year?" It has. From where I sit, organizations need to become more privacy aware just to survive. Regulatory stakes are increasing rapidly as consumers become more savvy about how their personal information may be used. Regulations like the EU General Data Protection Regulation and the financial world's PSD2 are bearing down on organizations even as the business stakes also rise.

New regulations and privacy awareness are a golden opportunity to build trust and respect with the consumer. Addressing privacy using a business framework approach, including a methodology that "leans in" to consent with confidence, will ensure more robust trust relationships with consumers. Customers will take action based on trust and they are more likely to purchase from consumer product companies that they believe protect and respect their personal information.

The results of MEF's 2017 Consumer Trust Study support the notion that there is a mutually beneficial value exchange when it comes to a trusted digital relationship. In exchange for a richer user experience, customers will share more data if they can trust what will be done with that data. And your business won't miss out on relationships that go dark when users walk.

Digital identity is at the very core of processing, storing and ultimately respecting personal data. In a hyper-connected market, many businesses have multiple back-end databases. The challenge is assuring consumers are protected from end to end, across products and services. We can successfully achieve the goal of connecting, protecting and respecting consumers by empowering the consumer with capabilities to provide consent and privacy preferences for their digital footprint.

It's critical to build and implement a comprehensive strategy that will satisfy compliance guidelines today and continue to build trusted relationships tomorrow. Digital identity and access management satisfies your customers wishes for privacy and consent and allows you to trust your users authenticity. In today's business, trust really does conquer all.

EVE MALER,
VP INNOVATION & EMERGING TECHNOLOGY,
FORGEROCK





**EXECUTIVE
SUMMARY**

#GCTS17



INTRODUCTION

The backdrop of MEF's 2017 Global Consumer Trust Study sees a rapidly changing global regulatory landscape when it comes to data protection. In May 2018 the European Commission's General Data Protection Regulation (GDPR) will come into force affecting any business collecting data from European citizens. All data processors – most companies – will be required to put the customer at the heart of any data exchange. Meanwhile, in the US privacy laws are under scrutiny and around the world new internet laws are being debated.

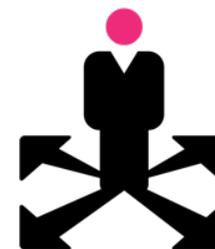
The key principles of privacy, security and identity are rapidly becoming regular boardroom topics. Consent, control and data portability are the new language of product and service design. Consumers must give permission before any data is collected. Data must be transferrable and it must be deleted or returned upon request. Critically, these and other rules will need to be implemented in ways that improve the customer experience, not detract from it.

MEF's Consumer Trust Initiative was established in 2011, a multi-stakeholder working group united by a commitment to drive best practice and innovation when it comes to consumer data. This consumer study is now in its 4th year and is part of the group's ongoing education programme to raise awareness of the importance of privacy, security and identity.

The research showcases the attitudes and behaviours of smartphone users globally when it comes to the apps and services they use to gain insights into their understandings and motivations around personal data. One of the goals of this year's study was to help businesses understand both the impact and opportunities of both new data regulation and changing consumer trends to demonstrate the importance of building trust.

This year it appears consumers are more aware than ever before of the value of their data. They know they may be affected if their data is misused or abused, and they are also increasingly aware of its commercial worth. Consumers are now more likely to engage in better control or protection of their data but also seek opportunities to benefit from this new currency.

Clearly the challenges facing all data holders and enablers of data-driven products and services are considerable. Yet the opportunities to build consumer trust are arguably greater. A new generation of services are emerging that give consumers the tools they need to take control of their data. The more mobile users engage with their data – adding to it, updating it, verifying it, providing permission for its use – the more valuable the data becomes to the company holding it.

**PRIVACY****SECURITY****IDENTITY****TRANSPARENCY****PORTABILITY****CONSENT****RIGHT TO BE FORGOTTEN**



INTRODUCTION (Cont.)

This report highlights some of the challenges and opportunities we as an industry are facing when it comes to managing and leveraging personal data. It demonstrates the importance of key data principles and identifies new behaviours and demand for services that build greater trust in the customer journey.

The study is supported by ForgeRock, Orange, and digi.me and was carried out in partnership with On Device Research. It surveys 6,500 consumers in 10 markets providing insights from smartphone users across Belgium, China, France, Germany, Poland, Romania, South Africa, Spain, UK and USA.

In this report we analyse some of the key global findings taking a deep-dive into the following areas:

- 🌀 Drivers and impact of trust in the mobile ecosystem
- 🌀 Behaviours, attitudes and motivations when it comes to personal data and key data protection principles
- 🌀 Consumer appetite for data-driven products and services

The appendix also includes additional charts and country data for your reference.





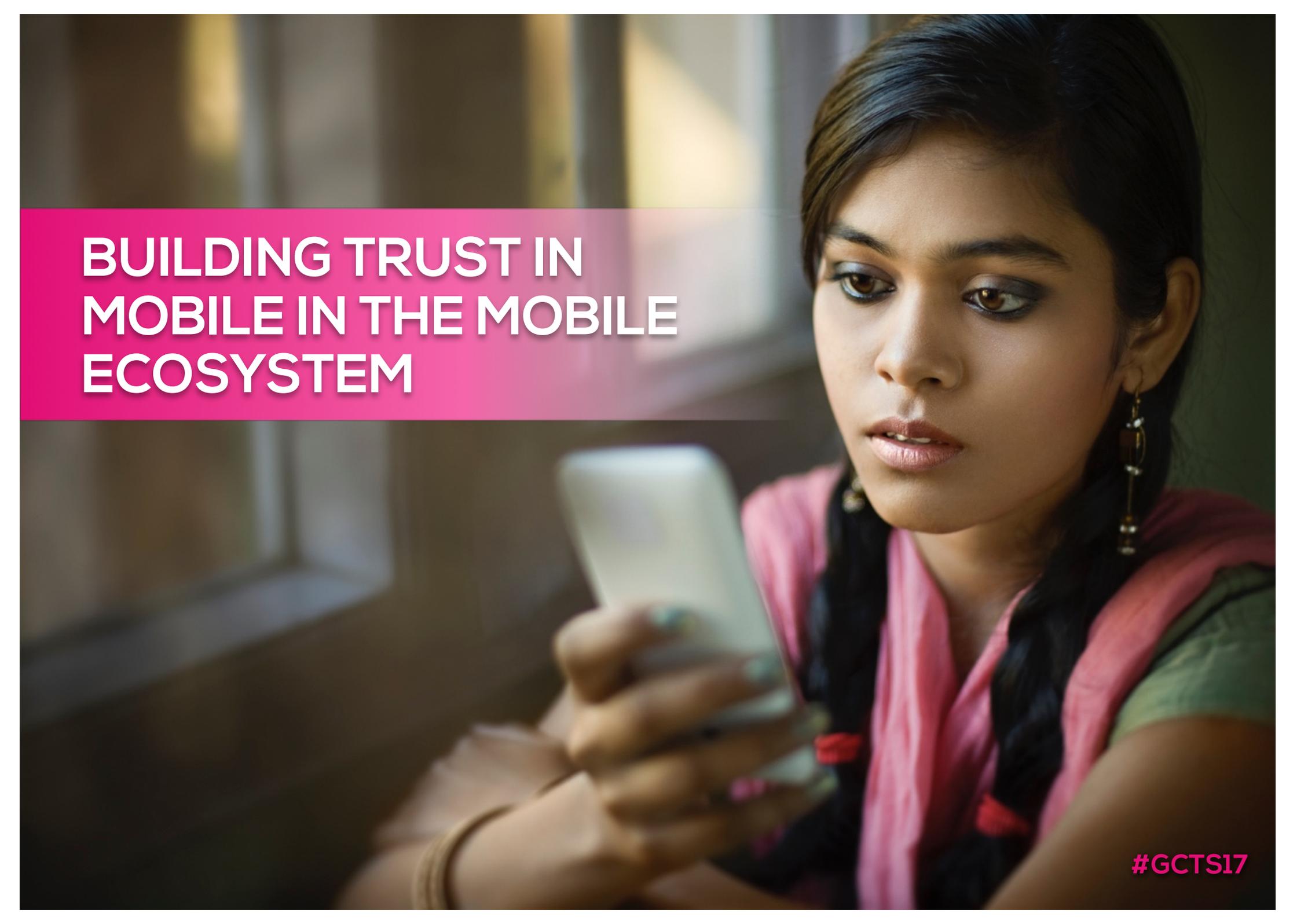
KEY FINDINGS

- When asked why they don't use more apps and services **40%** named one or more **trust issues** as the most important barrier.
- Privacy (16%)** remains the most influential trust-related concern, closely followed by **security (15%)**.
- 86% took action** as a result of trust concerns, e.g. including warning friends & family and using a competitive service.
- Almost half (**47%**) would **recommend a trustworthy app** to friends and family.
- When asked what makes an app or service trustworthy, **33%** said a '**clear, simple privacy statement**'.
- 75%** say they **read a privacy policy** or terms & conditions before signing up to a mobile app or service.
- Half of all respondents named **bad UX** as the number one reason to **lose trust** in an app or service.
- Mobile users trust **banks & credit cards (46%)** and **doctors & hospitals (45%)** most to manage their data.
- The number who said they are **always happy to share data halved** from 6-3%, while 39% said they never share it.
- Asked why they are concerned about personal data falling into the wrong hands, **47%** referred to **identity theft**.



KEY FINDINGS (CONT.)

- **53%** know they are **not in control** of the way their data is used.
- **39%** **reluctantly agree** to terms and conditions
- **14%** are **never asked for permission** before their data is collected.
- **Financial details**, e.g., bank & credit cards, are considered **most sensitive** by mobile consumers (**55%**).
- The Reluctant Sharer has been replaced by the **Savvy Consumer**. A smartphone user that jealously guards their privacy and security, but who at the same time rewards trustworthy apps and services.
- When asked what companies could provide in exchange for personal data, consumers consider **privacy-protection** and **access to their data** more important than financial and other rewards.
- **43%** said they'd be interested in a **privacy-focussed app** that shows what data is being collected across all of the user's connected devices.
- Many mobile users can already picture how **data portability** might make their life more convenient.



BUILDING TRUST IN MOBILE IN THE MOBILE ECOSYSTEM

#GCTS17



WHAT IS IT ABOUT AN APP OR SERVICE THAT MAKES IT TRUSTWORTHY?

What are the behaviours that build trust and what actions will erode it? Which elements within an app or service build user confidence, and which give cause for concern?

The 2017 study revealed key themes when it comes to building trust.

First, transparency is vital. When asked what makes an app or service trustworthy, more consumers named a 'clear, simple privacy statement' (33%) than any other attribute. Closely linked to transparency is communication. 19% want to be able to speak to someone.

Separately, we asked what providers could do to give people more trust in the way an app or service used their data. Transparency was referenced once again: 38% want it to be clear what information is being collected and what is to be done with it.

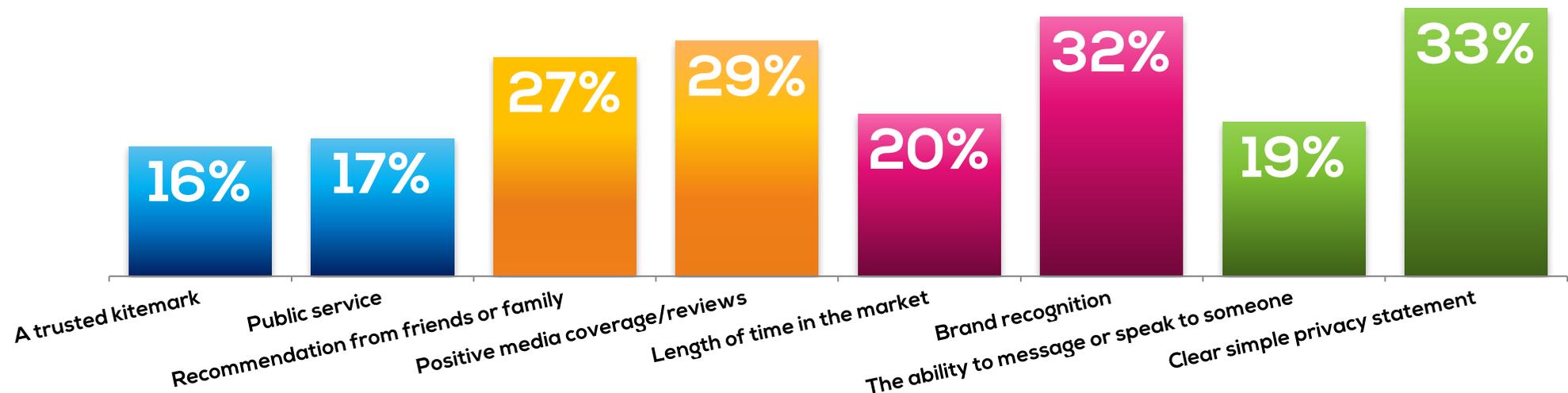
Women and older users in particular are driven by transparency. 41% of women said it made an app or service trustworthy vs 29% of men. 37% of those aged 35 and older said transparency had a positive impact vs. 32% of younger users.

Customer relationships are also key. 32% said that recognising the company behind an app or service immediately lends it credence. A further 20% said the longer an app or service has been in the market the more trustworthy it becomes.

The study also reveals the importance of influencers.

29% cited positive media coverage or reviews and 27% said recommendations from friends and families had a positive impact on an app or service's trustworthiness.

Finally, governments around the world should take note: apps and services with a civic purpose don't automatically gain trust with mobile users. Just 17% said that a public service made an app trustworthy.

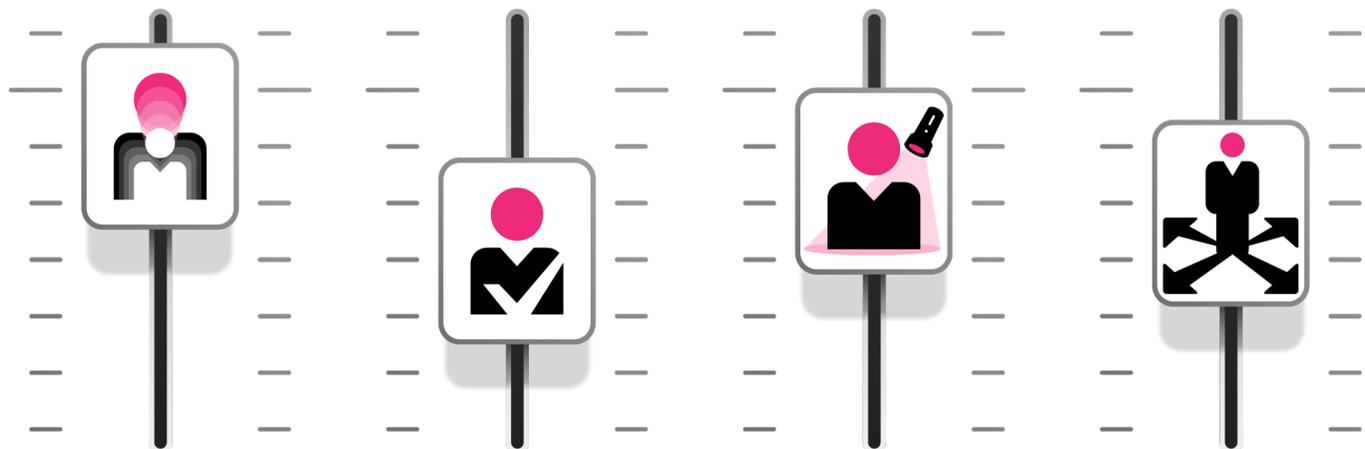


CONSUMERS TRUST SERVICES THAT PUT THEM IN CONTROL

GDPR asserts that users must be at the heart of the data collection process. Judging by the research, consumers agree.

When asked what would help build trust in app and services, almost half (42%) replied that they wanted to be able to have their data deleted. 40%

said they wanted to be able to withdraw permission for it to be used and 38% want transparency and to have control over whether their data is shared with third parties. 37% want to be able to decide what kind of information is shared and 28% want to mandate how long data is stored before being automatically deleted.



WHICH OF THE FOLLOWING WOULD HELP YOU HAVE MORE TRUST IN HOW AN APP OR SERVICE USES YOUR DATA?





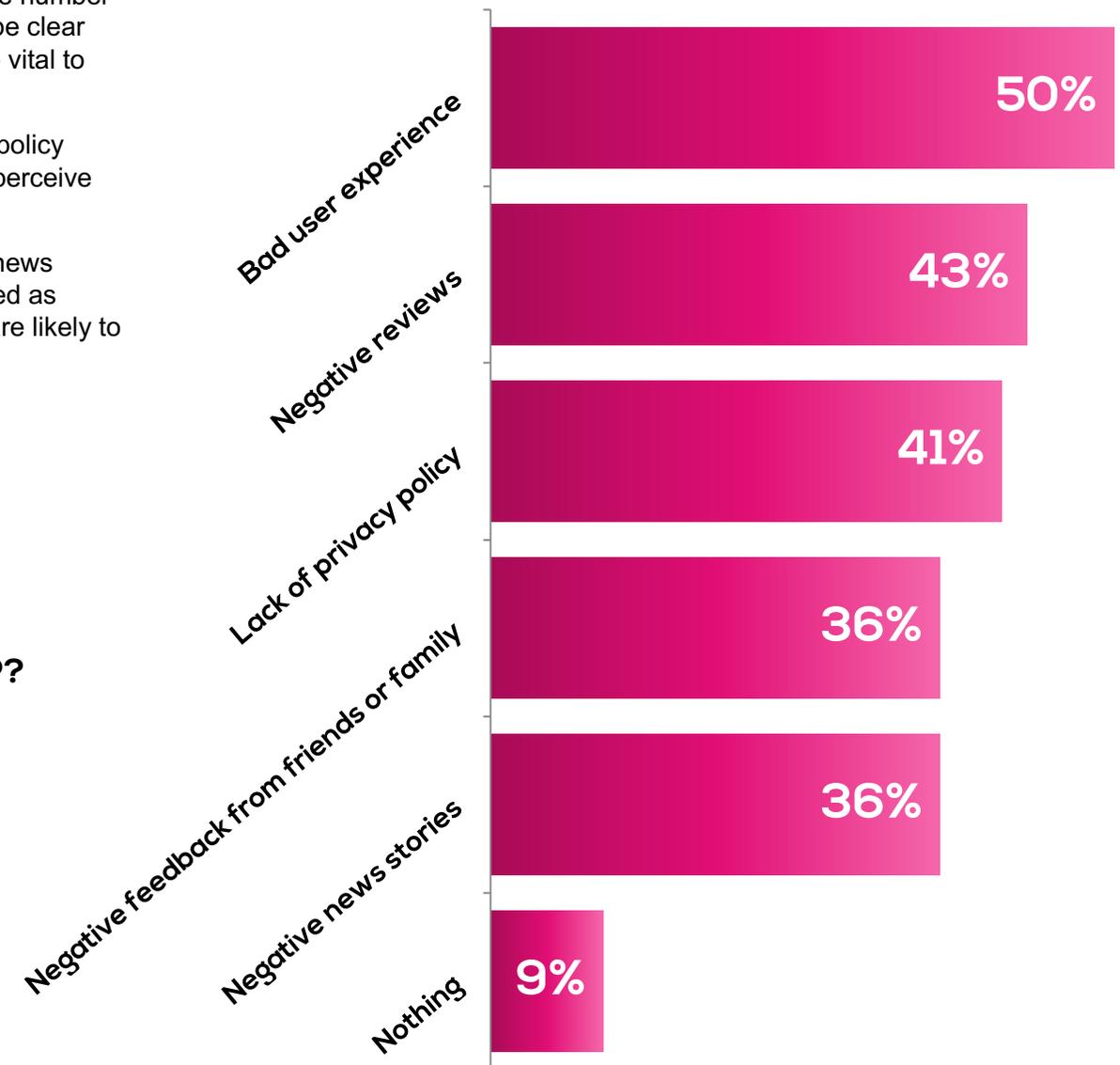
BAD USER EXPERIENCE IS THE FASTEST WAY TO LOSE TRUST

Half of all respondents (50%) named bad user experience as the number one reason to lose trust in an app or service. Providers should be clear that user interfaces, good design and on-boarding protocols are vital to reassuring the consumer that they are in safe hands.

Two other factors emerge. First, 41% said the lack of a privacy policy makes them lose trust. A design fundamental in the way users perceive apps and services.

The second is the role of influencers. Negative reviews (43%), news stories and feedback from friends and family (both 36%) are cited as grounds for mistrust. German mobile users in particular (50%) are likely to lose trust as a result of negative news stories.

WHAT MAKES YOU LOSE TRUST IN AN APP?



WHO DO CONSUMERS TRUST TO MANAGE THEIR DATA?

Who do consumers trust to manage their data? Themselves, obviously.

The majority of respondents (67%) want to take on the management of their own data. Good news for the so called Personal Data Ecosystem driven by Personal Information Management Service providers (PIMS) that allow users to control who can and can't access their personal information. However, it is interesting that a third (33%) did not respond 'myself' perhaps recognising that benefits also come with required effort.

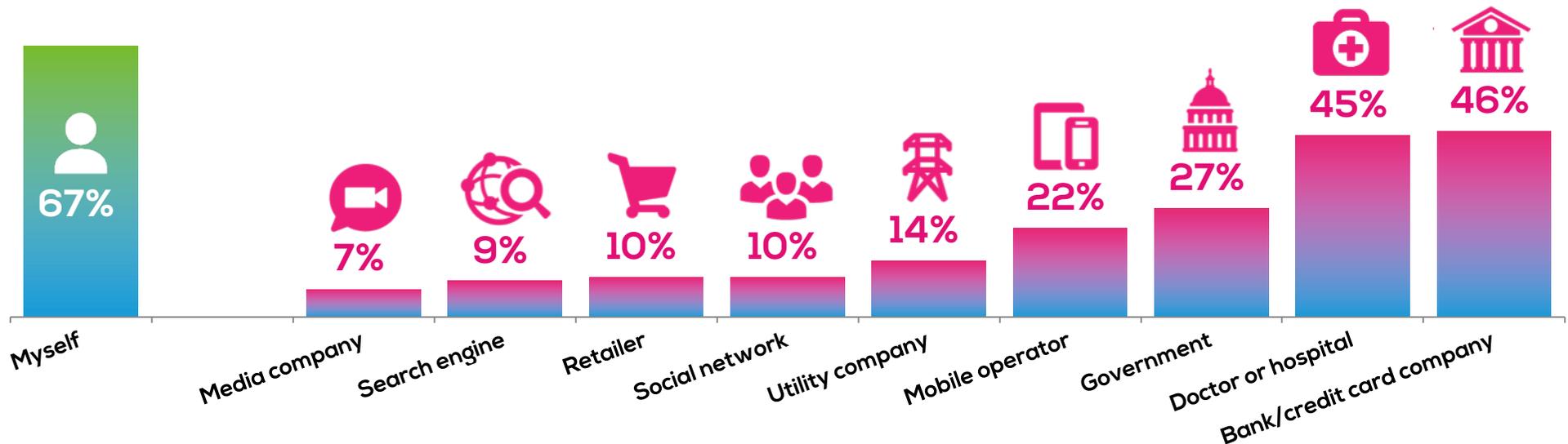
Women were more likely to want to manage their data (75% trust themselves the most vs. 63% of men). The same goes for South Africans (79%) whereas in Poland it was just 57%.

When it comes to the organisations that are most trusted to manage data, mobile users identified two clear favourites. Banks and credit card companies came top with 46% with doctors and hospitals close behind at 45%.

There is a marked drop between these two groups and the third placed organisation, though Chinese mobile users were much more likely to say they would place their faith in government (51%). Given the investment in smart cities and other data driven services with a civic purpose, it demonstrates the work that still needs to be done to build trust.

Facing a similar challenge are mobile operators. While there is a clear opportunity to act as a safe harbour for their customers' mobile data the results show that this trusted relationship is not yet defined in the minds of the customer.

Meanwhile, just 14% trust their utility companies with their data. Consumers are likely unaware of the data collection enabling connected home apps and services. Finally, the study found only 10% of consumers trust both retailers and social networks despite the advanced engagement strategies of these verticals, for example recent efforts by social platforms to improve transparency.



A LACK OF TRUST IS STILL HOLDING THE MOBILE MARKET BACK

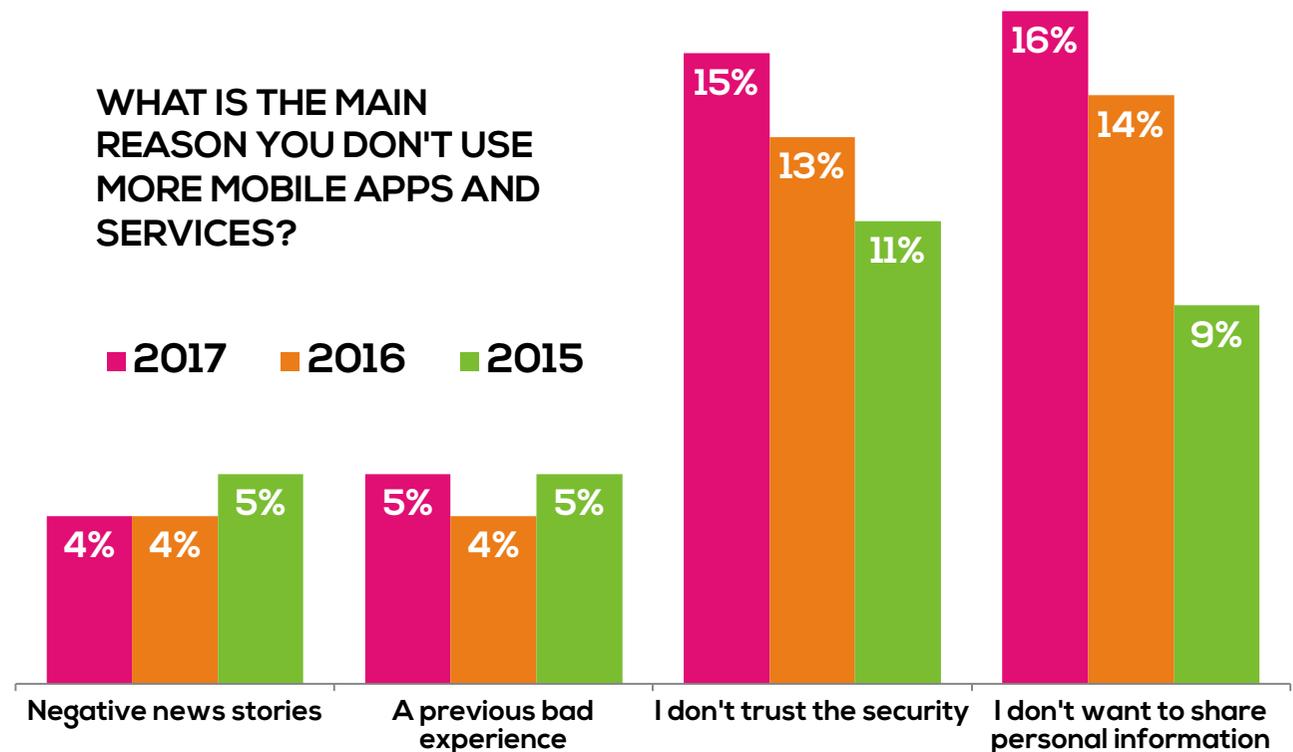
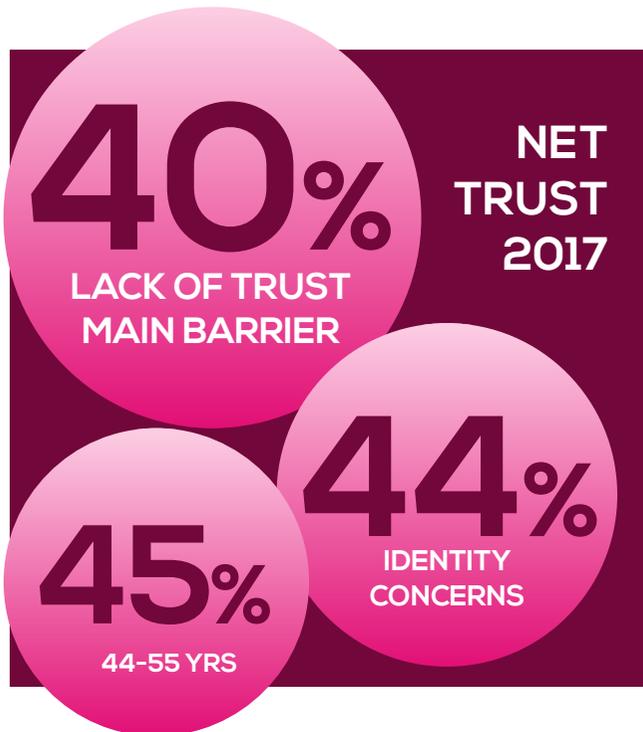
For the third year we asked smartphone users why they don't use more apps and services. For the third year in a row the answer is a lack of trust.

The number of respondents naming one or more trust issues as the most important barrier increased from 35-40%, the equivalent of a rise of 15% year-on-year.

Older consumers are more likely to cite trust as the main barrier. 45% of those aged 45-55 said trust issues were holding them back. Spanish mobile users are also above the global average in this regard (48%).

There is also an interesting link to concerns about identity. Users who said they were concerned they can't be sure of the identity of a provider were more likely to have trust issues than the average (44% vs. 40% average)

Privacy (16%) remains the most influential trust-related concern, especially in Poland (20%) and USA (19%). This is closely followed by security (15%) – no more so than in France and Spain (both 18%). There was also a slight increase in the number of users reporting a bad experience (5%).



ONE IN FOUR ARE ACUTELY IMPACTED BY TRUST

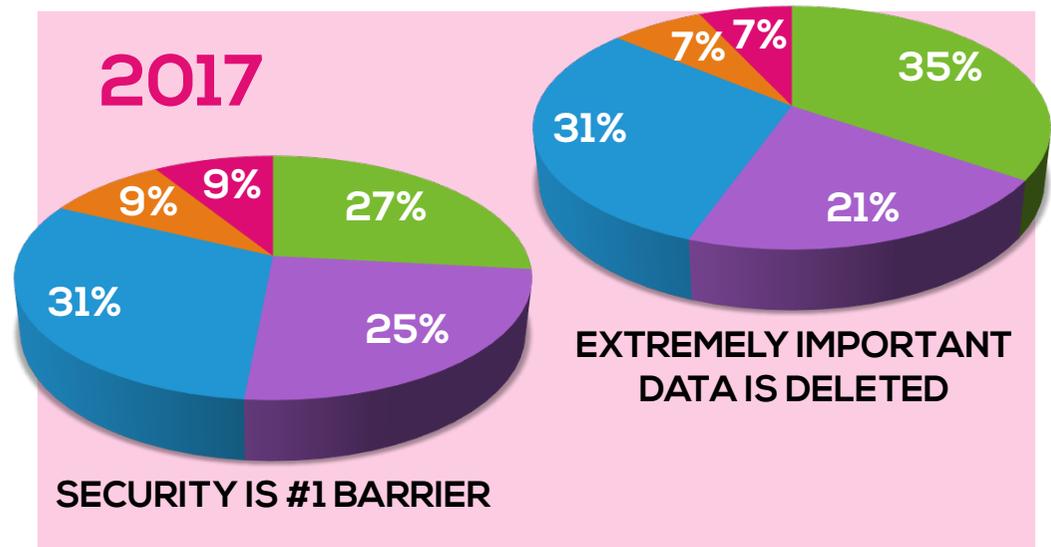
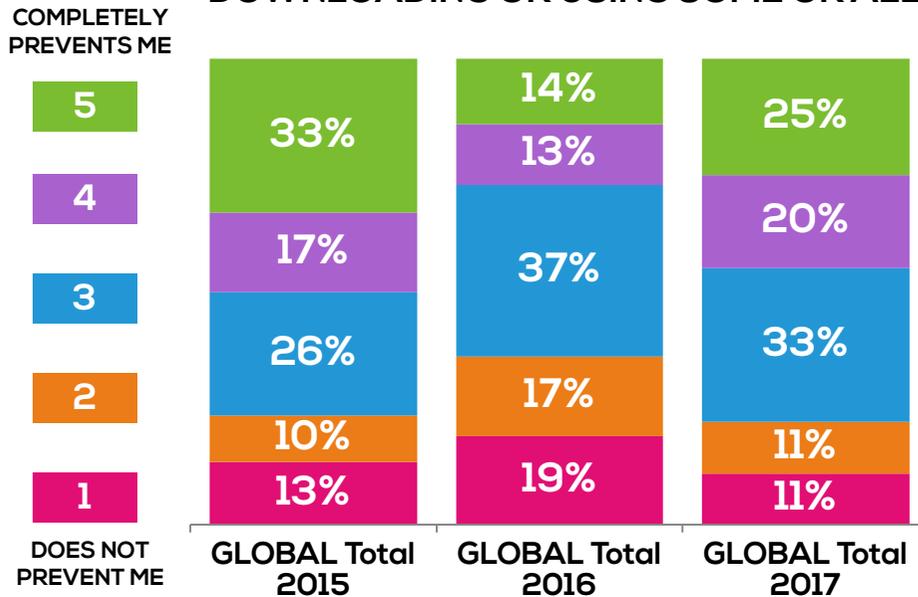
The number of mobile users who said that a lack of trust completely prevents them from buying, downloading or using apps rose this year from 14 to 25%. While this doesn't reach the high watermark of 33% in 2015, it's a worrying development after last year's improvement.

The net number of those saying it's a barrier is up two-thirds year on year from 27-45%. The consequences of this lack of trust appear most entrenched in South Africa where 38% say it completely prevents them doing more with their mobile and 54% say it's a barrier.

Security also appears to be a key driver. Of those that identified security as the single biggest reason they don't download or use more apps and services, 52% said a lack of trust prevents them doing more with their mobile (vs. an average of 45%).

The data also showcases the importance of deleting data when asked by the user. Of those that said it was extremely important that data was deleted upon request, 56% said they were prevented by trust concerns from doing more with their mobile.

TO WHAT EXTENT DOES A LACK OF TRUST PREVENT YOU FROM BUYING, DOWNLOADING OR USING SOME OR ALL APPS IN YOUR PHONE?



CONSUMERS WILL TELL YOU IF THEY DON'T TRUST YOU

The impact of trust is clear. 86% of customers will take some kind of remedial action as a result of trust concerns - a slight increase on last year. Just 6% took no action at all. Such findings make it clear that good data stewardship is not optional if companies want to build long term customer relationships with sustainable business models built on data.

In 2017 there was a significant increase in those who simply stop using an app (38-44%) with a more modest rise in the number deleting the offending app/service from their phone (52-54%).

Connected home users are more likely to switch providers as a result of trust concerns. 23% of those that recently bought a smart device for the

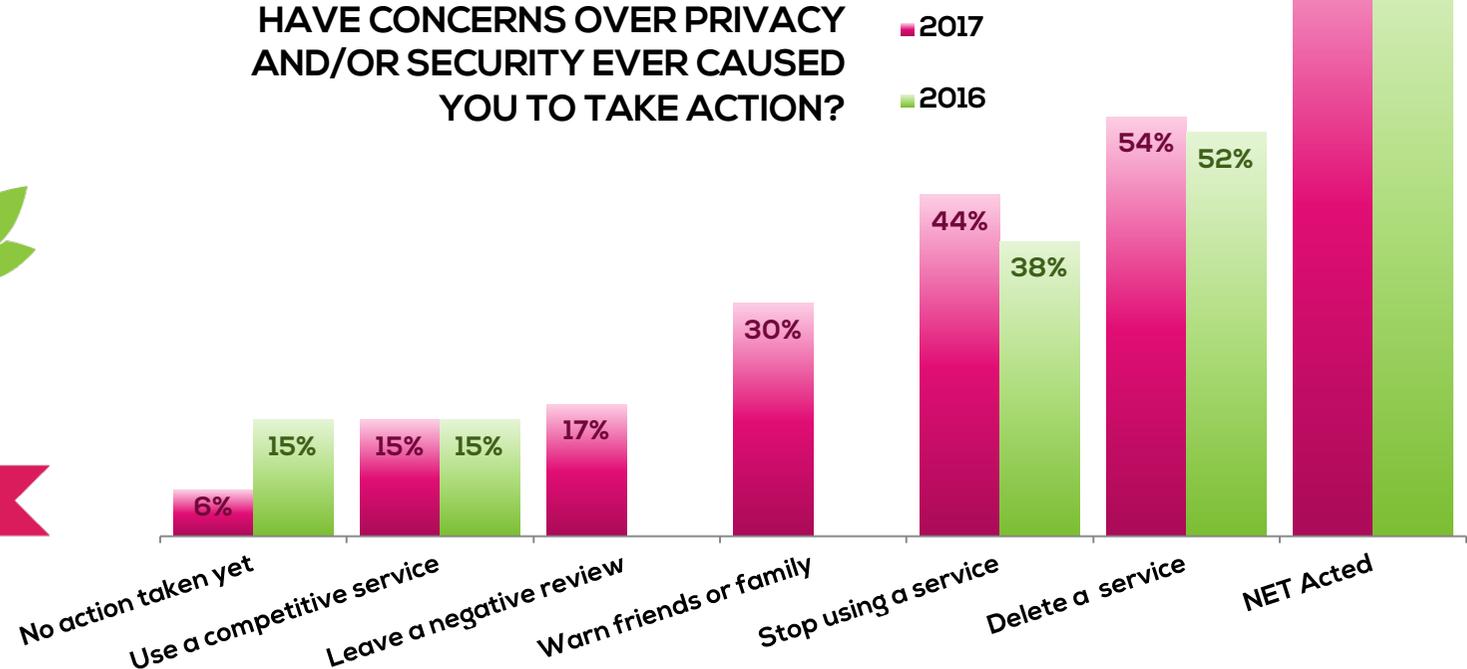
home said they would use a competitive app or service vs the 15% global average. The same applies to those that are put off by concerns that they can't be sure of a provider's identity. 21% of this group said they would switch providers.

French mobile users (20%) are most likely to download a competitive app or service; the Chinese least likely (9%).

People who had a bad experience are the most likely to write about it. 23% of this group said they would leave a negative review (vs the 17% average).



HAVE CONCERNS OVER PRIVACY AND/OR SECURITY EVER CAUSED YOU TO TAKE ACTION?



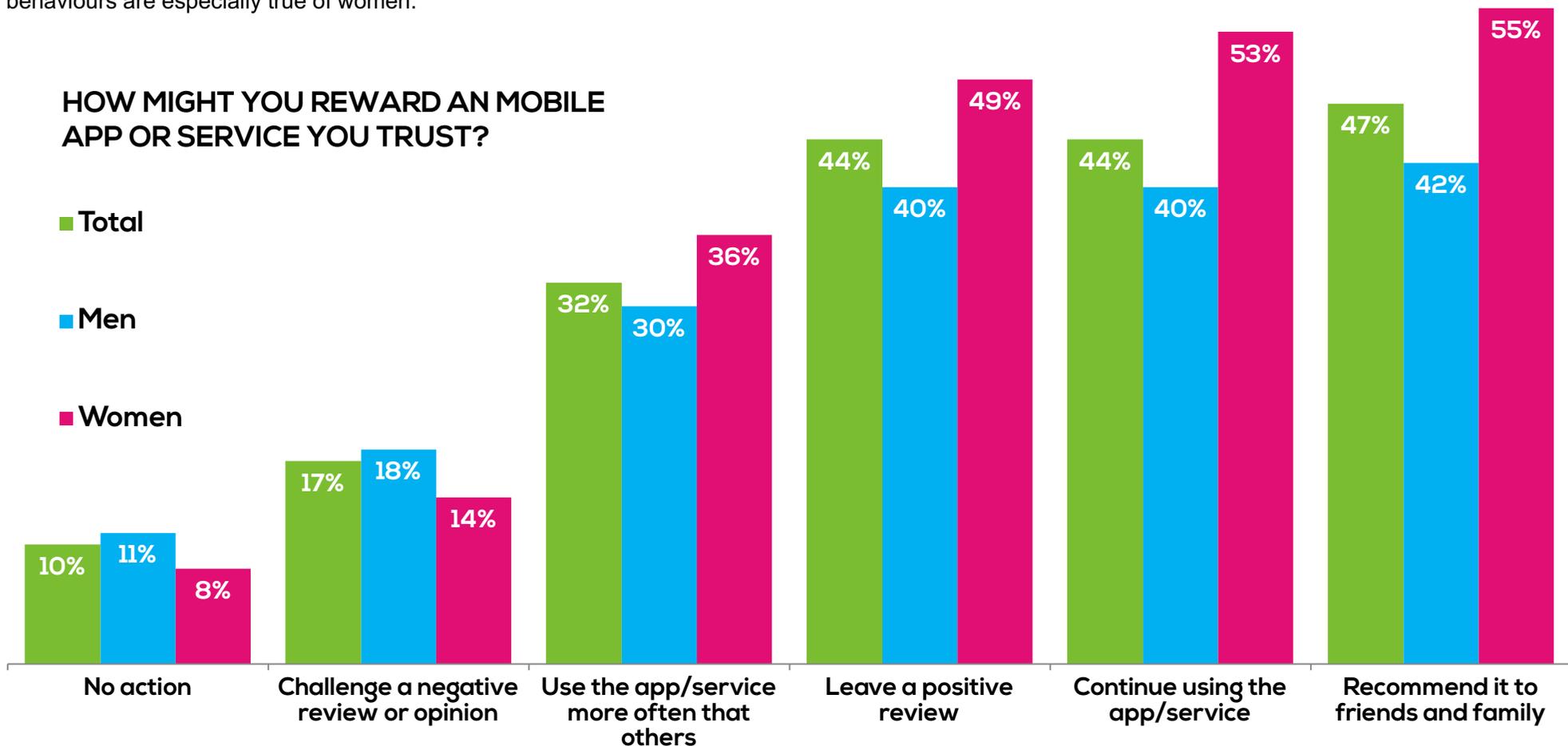
CONSUMERS HAPPY TO REWARD TRUSTWORTHY SERVICES

The good news is that consumers are equally motivated to reward an app or service that has earned their trust.

Almost half would recommend a trustworthy app to friends and family (47%) or leave a positive review (44%). A third (32%) say they would use the app/service more often than they would other apps/services. All three behaviours are especially true of women.

17% - a not inconsiderable number – are prepared to challenge negative perceptions of an app or service on the provider’s behalf. This is the sole activity where men are more likely to engage than women.

HOW MIGHT YOU REWARD AN MOBILE APP OR SERVICE YOU TRUST?





CONSUMER BEHAVIOURS AND ATTITUDES IN THE PERSONAL DATA ECONOMY

#GCTS17

75% SAY THEY ALWAYS OR SOMETIMES READ A PRIVACY POLICY

WHEN SIGNING UP TO A SERVICE DO YOU...



In 2017 consumers are not just more concerned about their personal data, they are changing their behaviours accordingly. The research charts a trend toward a greater investment in time to understand how an app or service might impact their privacy.

More than half (53%) said it was extremely important to know that an app or service is using their personal data. This represents a slight increase on last year (51%). 69% consider it important overall – five percentage points higher than the 2016 findings. Women and over 55s are most likely to consider transparency 'extremely important' (62% and 65% respectively). In South Africa it's 72%.

Even so, it may still come as a surprise that 75% say they sometimes or always read a privacy policy or terms and conditions before signing up to a mobile app or service. This is especially the case in China and UK (both 82%) and USA (79%). Whereas, in France (65%) and Belgium (62%) mobile users are less likely to take the time to assess an app or service's impact on their privacy.

Early adopters of connected homes (80%) are more likely than the average to read a privacy policy. With IOT services it can pose a greater design challenge to present privacy information but it clearly is important for mass market adoption.

Finally, those who had a bad experience also said they are more likely than the average to read a privacy policy (84%). This is understandable given they have learned the hard way that some apps and services can have an adverse impact on their privacy and/or security.

DON'T FORGET THE RIGHT TO BE FORGOTTEN

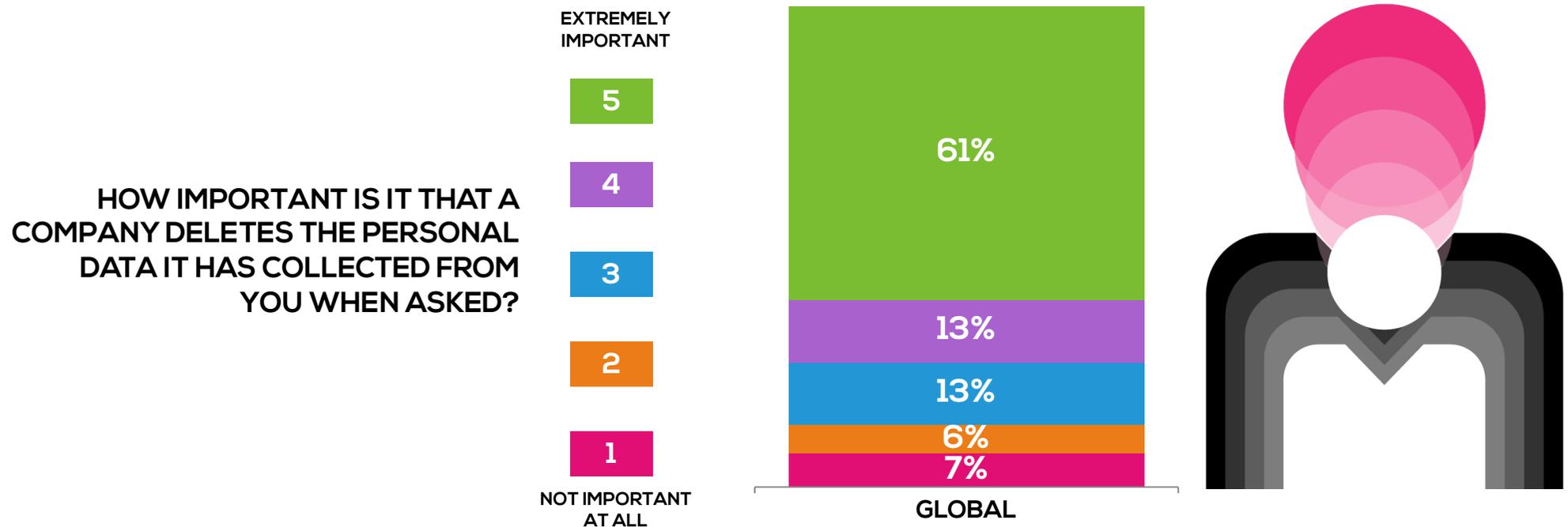
One of the principles enshrined within the new European data protection regulations is the Right To Be Forgotten; in other words the ability for consumers to request that all their personal data be deleted.

MEF's research suggests that this protection will be welcomed. 61% said it was extremely important a company deletes personal data when you ask it to. This is especially important for women (69%) and those older than 35 (70%).

Users of certain types of services are more likely to want the right to be forgotten. 69% of those that use their mobile to carry out banking activities, for example, say it's extremely important that a company delete their data upon request.

The research also suggests that privacy is driving this desire for a right to be forgotten. 70% of those that say it's extremely important to delete data also say they're concerned that personal information might be shared without permission.

84% of those that said it is extremely important also say they are completely prevented from doing more with their mobile. This perhaps suggests that if mobile users are able to have their data deleted on request they will be more likely to engage with mobile apps and services in the long term.



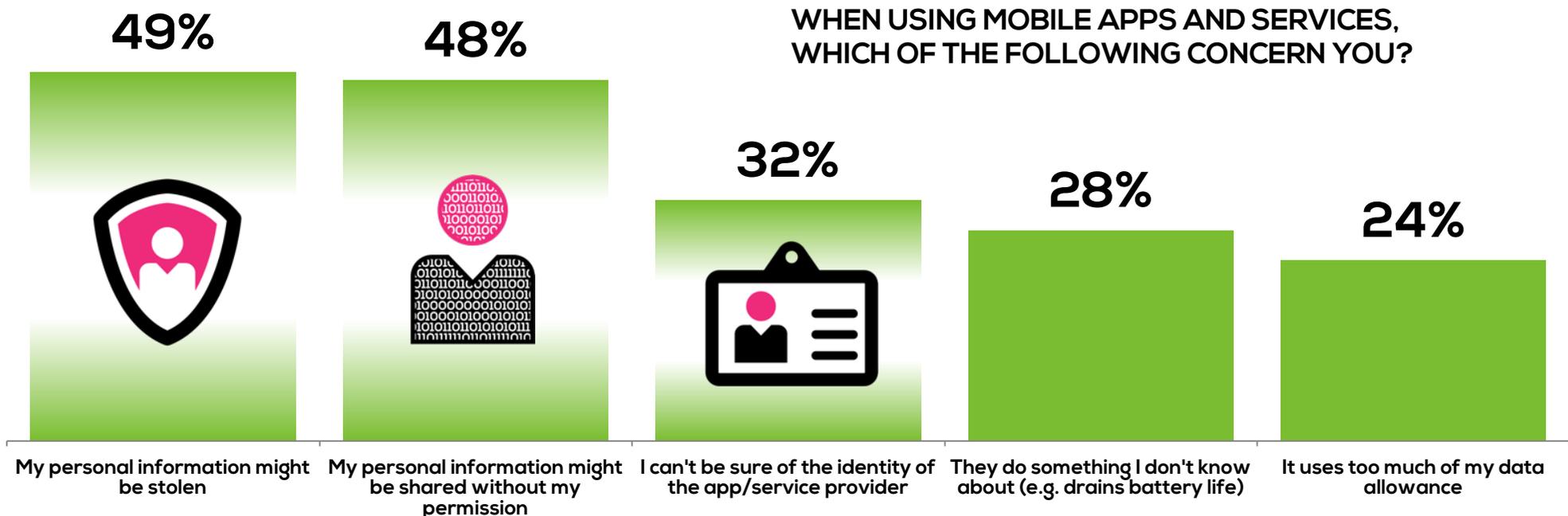
WHAT ARE PEOPLE WORRIED ABOUT, SPECIFICALLY?

When users were asked the exact nature of their concerns, two responses stood out: security (49%) and privacy (48%). Given the financial implications of information being stolen it's not surprising that half of respondents cite security but it's interesting that privacy of personal data ranks just as highly. Consumers also have concerns over identity with a third of respondents (32%) saying they can't be sure whether or not the provider is who they say they are.

There is some diversity of response by country. In Romania (38%) mobile users are less concerned about apps and services sharing their information. In the USA, by contrast, it's 59%.

Not for the first time, women are more likely to have trust-related concerns than men. 56% are concerned about security and 57% that personal information might be shared without permission. For men it's 45% and 44% respectively.

That personal data concerns rank so highly demonstrates its perceived value. Other concerns such as battery life (28%) or 'bill-shock' caused by extra data use (24%) were found to be less important to consumers. South Africans are the most concerned about their data allowance being used up (38% vs the 24% average).



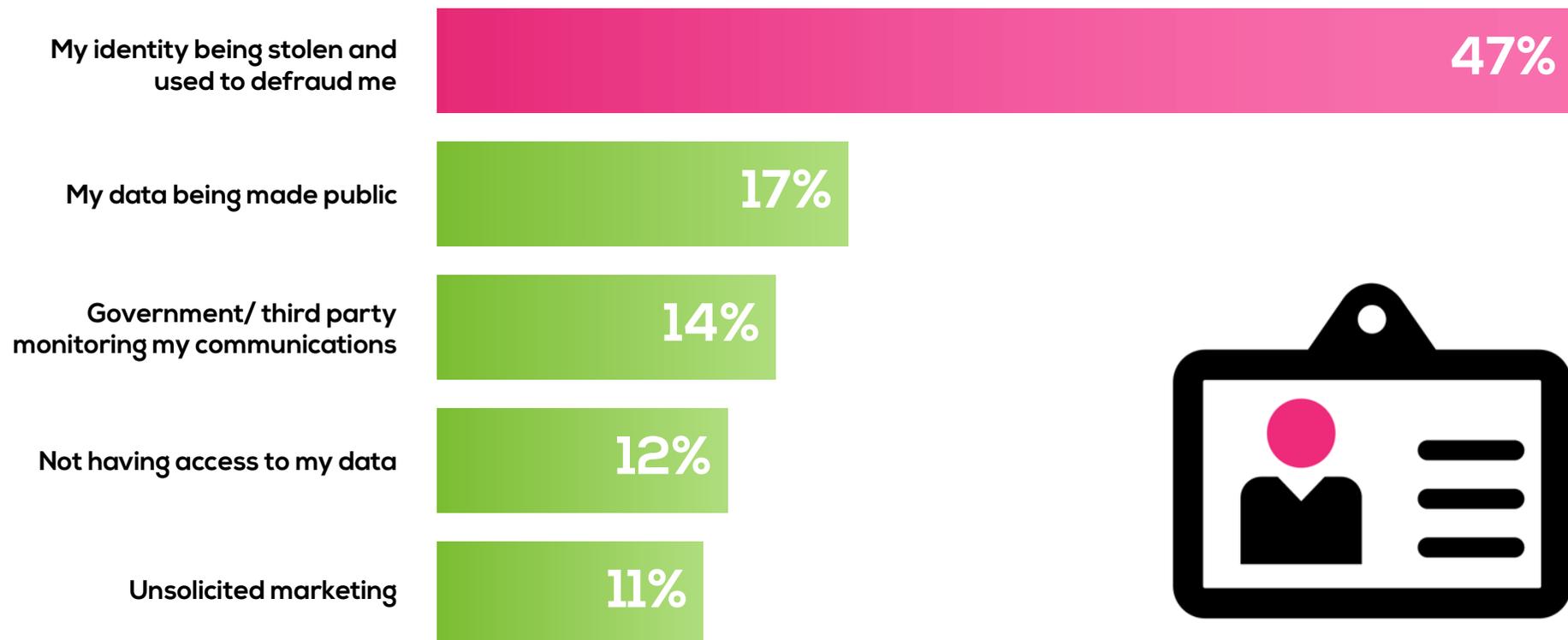
IDENTITY THEFT IS PREYING ON CONSUMERS' MINDS

Expanding on personal data-related concerns, consumers were asked to consider the resulting scenario they fear the most. Identity theft is absolutely front of mind: almost half (47%) named that their main concern.

This is especially true of women: 53% named identity fraud as their top concern as opposed to 43% of men.

Despite the ongoing headlines and commentary around the behaviour of security services in some countries, few are concerned about the government monitoring their communications (14%).

WHICH PERSONAL DATA SCENARIO WOULD CONCERN YOU THE MOST:





MORE THAN HALF FEEL THEY HAVE LOST CONTROL OF THEIR DATA

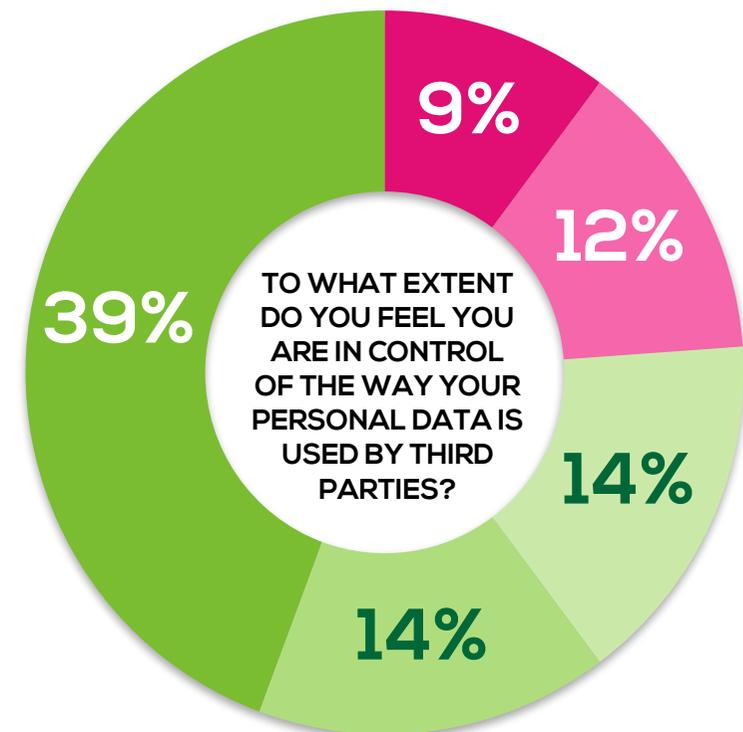
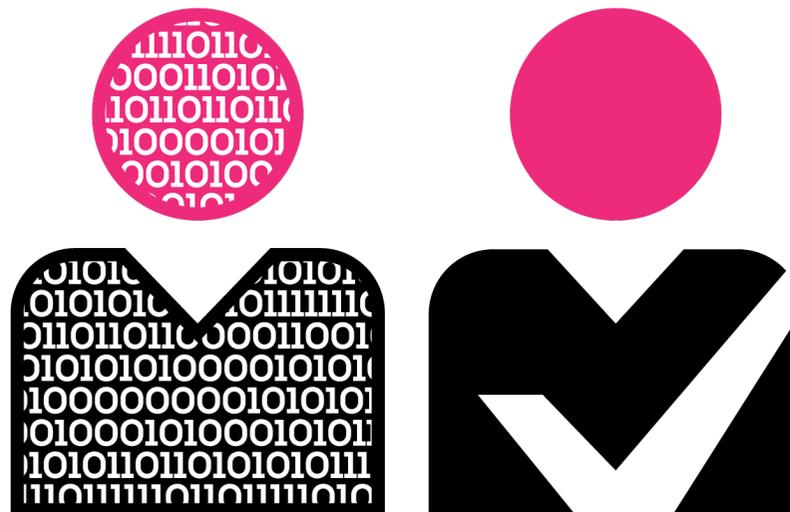
One of the outcomes that data protection regulators want to see is the situation where consumers are fully informed and in total control of the way their data is used.

MEF's research suggests there's a long way to go before that is achieved. Fewer than 1 in 10 (9%) say they are always asked for permission and make a conscious choice about how their data is used. Another 12% state that they have some control over their data some of the time.

This means the majority (53%) consider they are not in control of the way their data is used. Of these, many do agree to the terms and conditions presented to them, but only reluctantly. 39% say 'I know that by agreeing to the terms and conditions I am giving permission, but I don't feel I have a choice'. This is especially true in the US (48%), among women (47%) and those whose data-related concerns revolve around the fact their data might be shared without permission (49%).

The rest of the 53% is made up of the 14% of mobile users who say that they know information is being collected but are never asked for permission. This is understandably higher for those who also say they have had a bad experience which damaged their trust in mobile apps and services (21%).

A further 14% say they didn't even know apps and services use their personal data. This lack of understanding demonstrates a different – but no less damaging – lack of control over personal data.



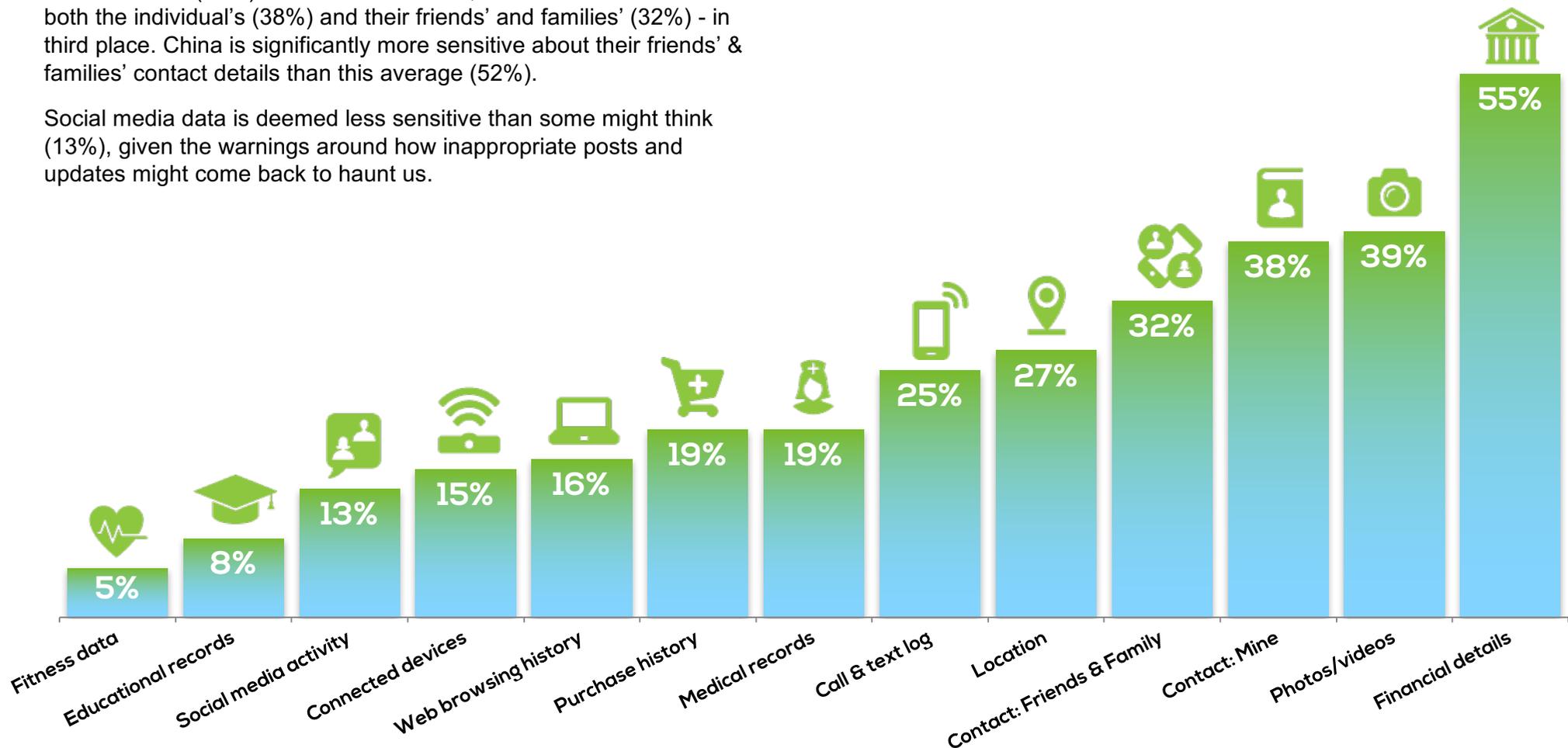
WHAT TYPES OF DATA DO CONSUMERS CONSIDER MOST SENSITIVE?

Financial details – for example, bank and credit cards – are considered most sensitive by mobile consumers. More than half (55%) named this type of data. South African mobile users are most concerned about the integrity of their financial information (67%), as are women (66%).

Photos/videos (39%) are a distant second, with contact information - both the individual's (38%) and their friends' and families' (32%) - in third place. China is significantly more sensitive about their friends' & families' contact details than this average (52%).

Social media data is deemed less sensitive than some might think (13%), given the warnings around how inappropriate posts and updates might come back to haunt us.

Mobile health, education and IOT are all nascent markets. This might explain why those data types are considered less sensitive than their use cases might suggest. As services roll out it will be interesting to track whether these categories advance up mobile users' worry-list.



PEOPLE ARE INCREASINGLY UNCOMFORTABLE SHARING INFORMATION

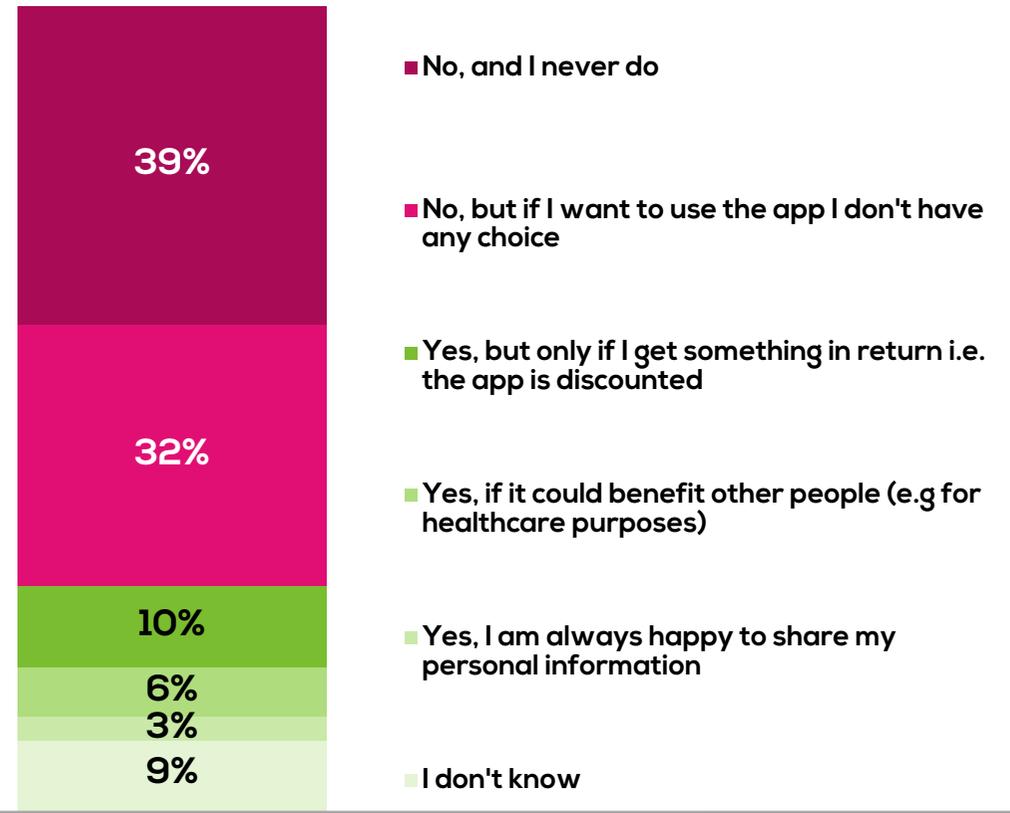
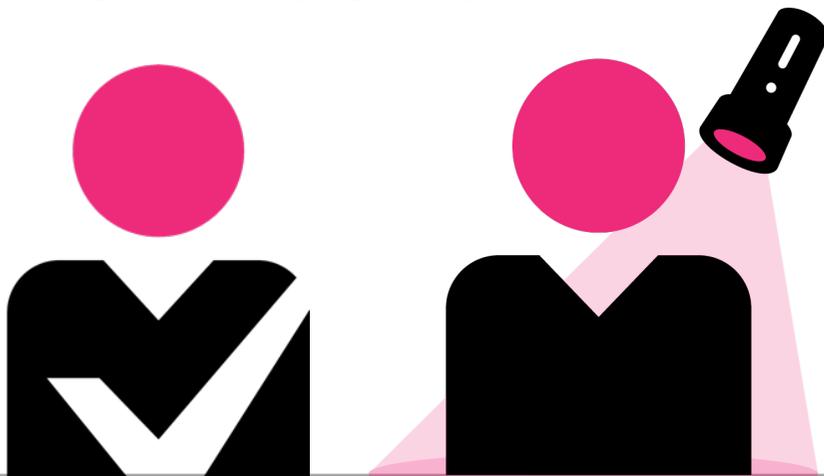
In 2017 the number of people who said they are always happy to share personal information halved from 6-3%.

Conversely, 39% said they never share data – demonstrating a lack of understanding of the data collection practices of mainstream apps and services. Intriguingly this applies especially to both the oldest (44% of over 55s) and the very youngest (42% of 16-24 year olds).

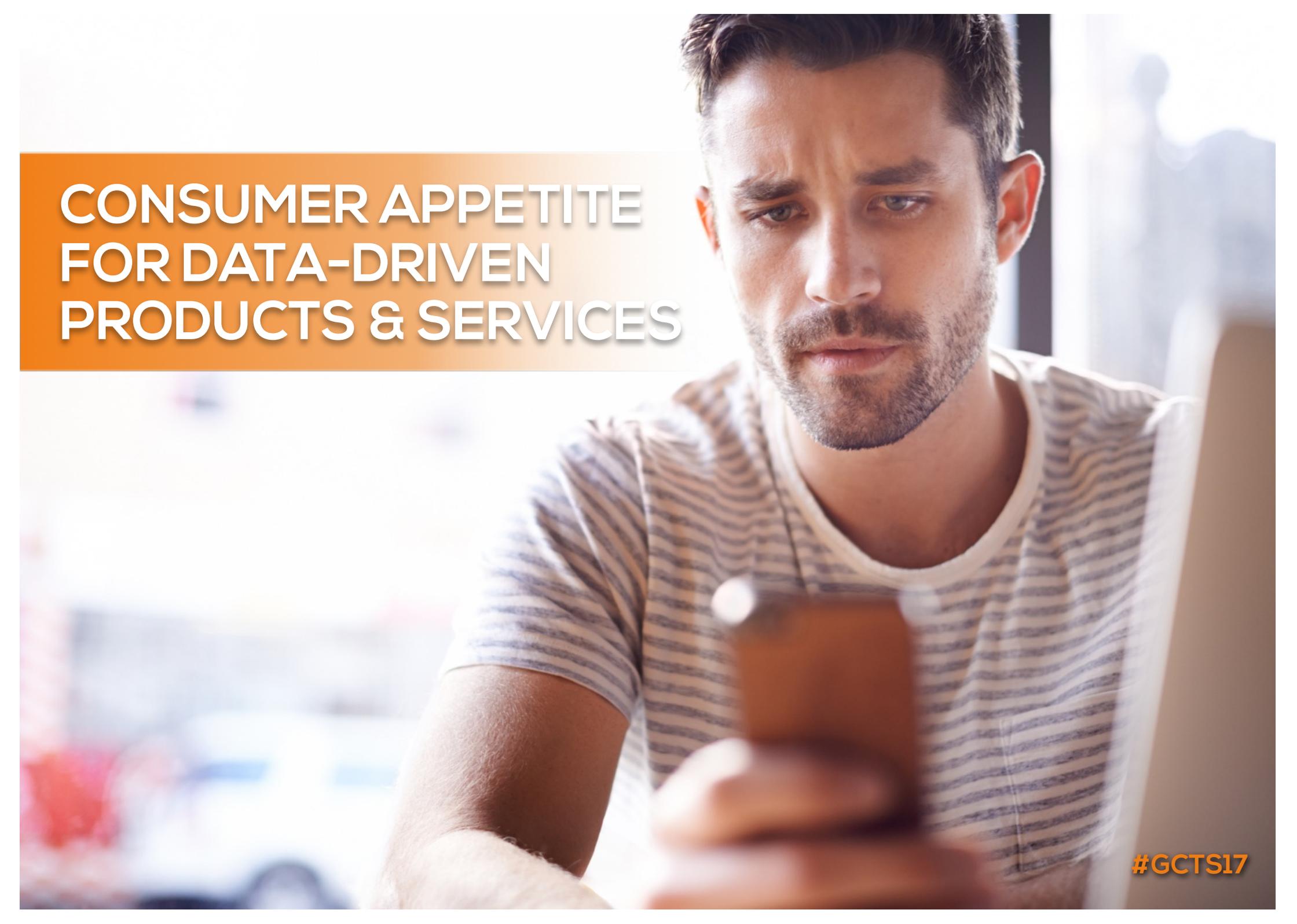
Also on a downward curve are those that say they are prepared to share their personal information in exchange for something. This number dropped by a third, from 15-10%. The exception to this are both users of smart home services (17%) and mobile users in China (16%).

This year MEF asked if people would share data for altruistic reasons. 6% said that they would indeed be happy to do so if it benefited others, for example for healthcare purposes. Unsurprisingly, users of medical and fitness apps are most likely to share data for the good of others (10%). It will be interesting to see if the number of altruistic sharers increases alongside positive media reports of data being used for societal good.

ARE YOU COMFORTABLE SHARING YOUR PERSONAL DATA WHEN YOU USE A MOBILE APP OR SERVICE?



GLOBAL Total

A man with short dark hair and a light beard, wearing a white and blue striped t-shirt, is looking down at a smartphone he is holding in his hands. The background is a bright, out-of-focus outdoor scene, possibly a parking lot or a public area, with some blurred figures and structures. The overall lighting is bright and natural.

CONSUMER APPETITE FOR DATA-DRIVEN PRODUCTS & SERVICES

#GCTS17

THE EMERGENCE OF THE SAVVY CONSUMER

Last year's research identified the rise of the Reluctant Sharer: consumers who did not want to share personal information but knew must if they want to use the app or service. In 2017 this number dropped a fifth, from 41-32%. Women, however, are still likely to identify themselves within this category (40% compared with just 28% of men).

In 2017 this drop in reluctant sharers sees a new category emerge: the 'Savvy Consumer'.

A smartphone user that guards their privacy and security, they are prepared to penalise any provider that abuses their trust but will also reward trustworthy apps and services.

The research also shows that the Savvy Consumer instinctively recognises the benefits of an emerging class of new data-driven mobile service which lets them take more control of their privacy. They also understand why it might be useful to be able to transfer data between providers – a service not commonly available at present but soon to be mandated by regulation.

Moreover, when asked what companies could offer in exchange for his or her data, the Savvy Consumer names not only financial rewards, discounts and free mobile services, but also the right to have data returned or deleted on request.

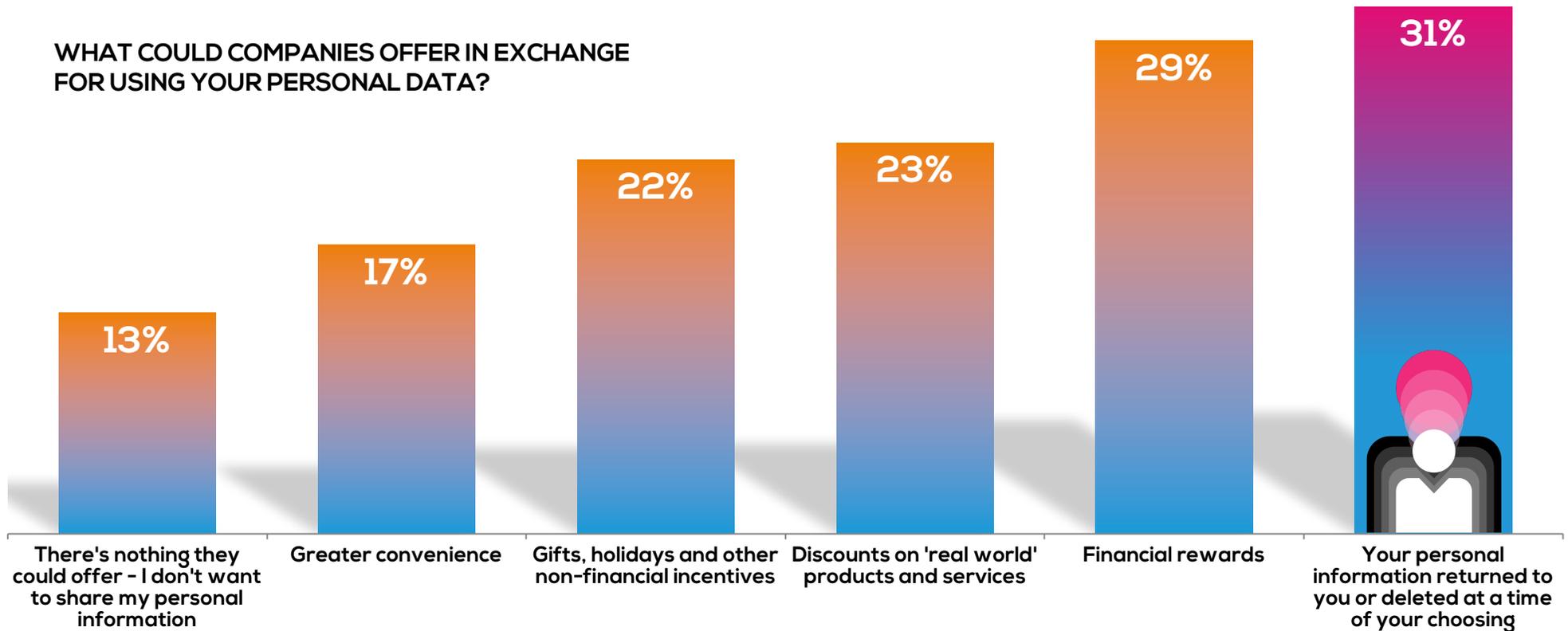


OFFERING A FAIR AND EQUITABLE VALUE EXCHANGE

If there was ever a time when companies could collect personal data without offering anything in return, the research makes clear those days are gone. Going beyond compliance, the research demonstrates a clear demand for app and service providers to develop consumer-centric data-driven products.

We asked mobile users what they wanted in exchange for their personal data. The top answer was revealingly not money, though 29% did name financial rewards and 23% requested discounts on real world products and services. Instead, the response that most people gave was that personal information could be returned or deleted at a time of their choosing (31%).

WHAT COULD COMPANIES OFFER IN EXCHANGE FOR USING YOUR PERSONAL DATA?



THOSE THAT VALUE CONTROL MOST HIGHLY ARE INFLUENTIAL PARTICIPANTS IN THE TRUST DEBATE

As we have seen, almost a third (31%) would exchange their personal data in return for greater control over it. They value this more highly than financial and other kinds of rewards.

MEF's research reveals some fascinating insights into this group of savvy consumers, demonstrating their influence on the trust debate.

Firstly, they are more likely to be women (39% vs. 27% men) and heavy mobile users of real-world services like taxi or food delivery (43%).

Their desire to exercise greater control over personal data is driven, at least in part, by concerns over identity theft. 55% of this group said this was their main concern as opposed to 49% of the global total.

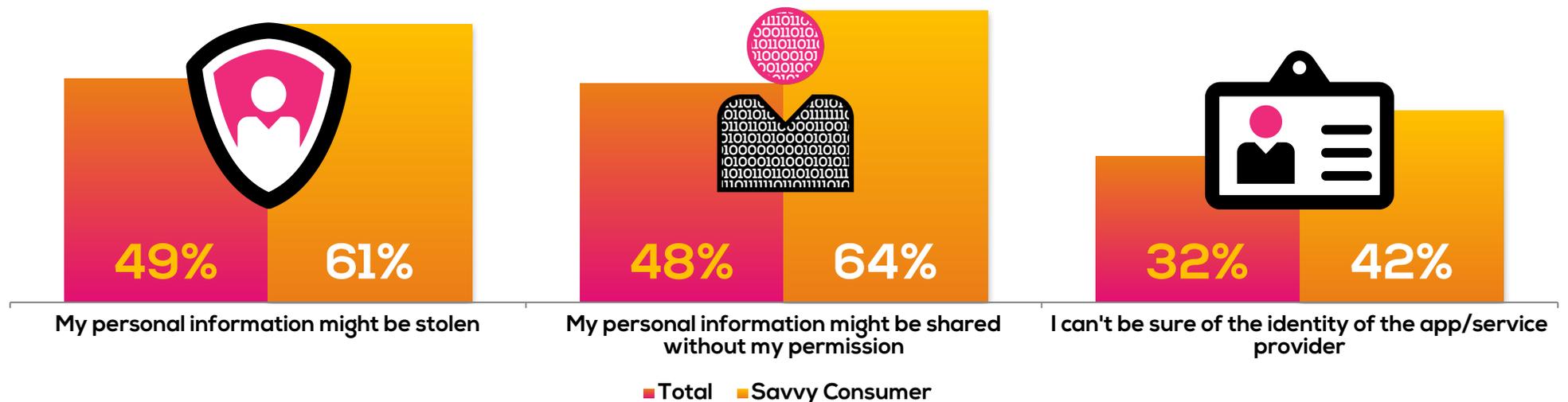
This group are more likely to feel they have lost control over their data. 53% said 'I know that by agreeing to the terms and conditions I am giving permission, but I don't feel I have a choice' versus the 39% average.

They are also more likely to value an app which shows exactly what personal data is being collected by all their connected devices (60% vs. the 43% average).

Transparency is seen as the essential trust building attribute. Half (50%) said a clear simple privacy policy makes an app or service trustworthy, against the global average (33%).

Their influence is key. Two-thirds (67%) say they would promote trustworthy apps and services to friends and family – 20% more than the global average.

WHEN USING MOBILE APPS AND SERVICES, WHICH OF THE FOLLOWING CONCERN YOU?



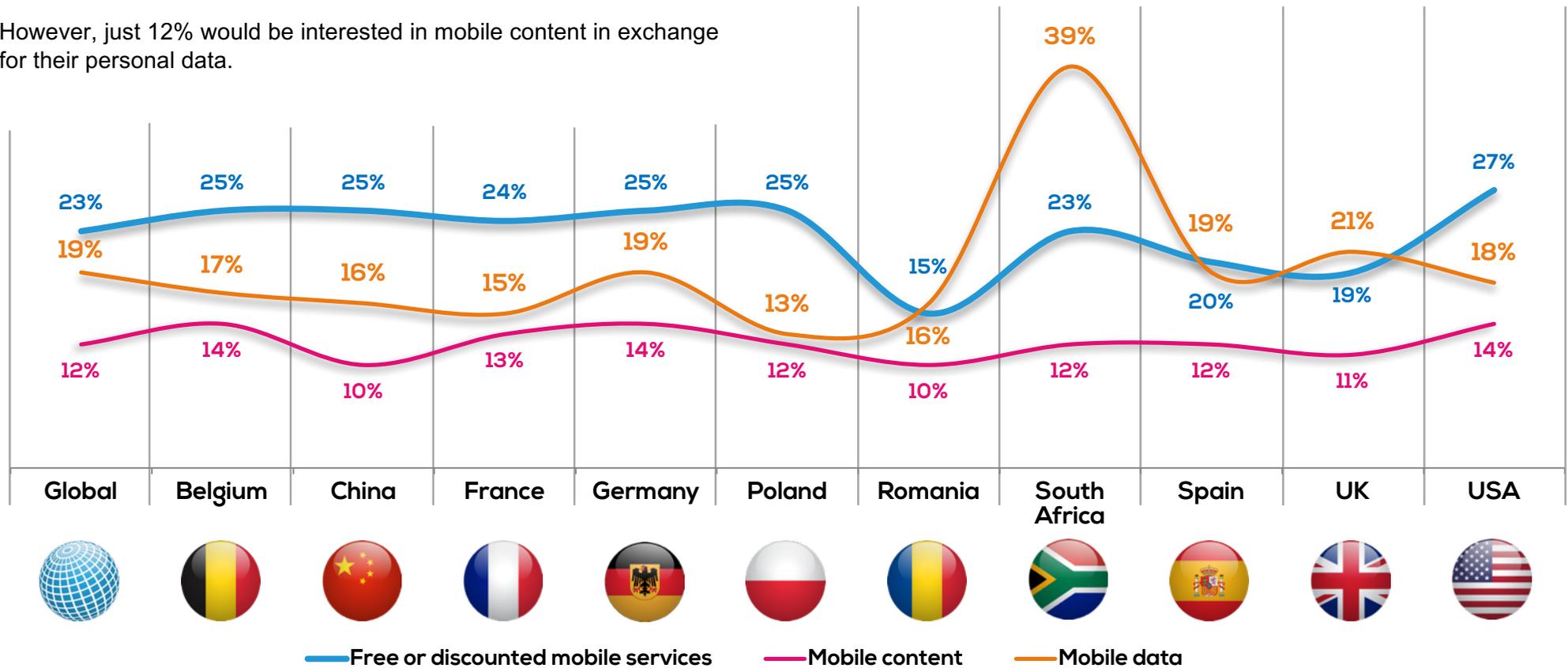
MOBILE INCENTIVES

One obvious value exchange opportunity is to offer consumers mobile-related incentives. However, the response here was mixed.

On the plus side one in four (23%) would be interested in free or discounted mobile services in exchange for their personal data. One in five (19%) would appreciate additional data allowance – especially in South Africa where this leaps to 39%.

However, just 12% would be interested in mobile content in exchange for their personal data.

WHAT COULD COMPANIES OFFER IN EXCHANGE FOR USING YOUR PERSONAL DATA?



STRONG DEMAND FOR DATA-DRIVEN PRODUCTS AND SERVICES

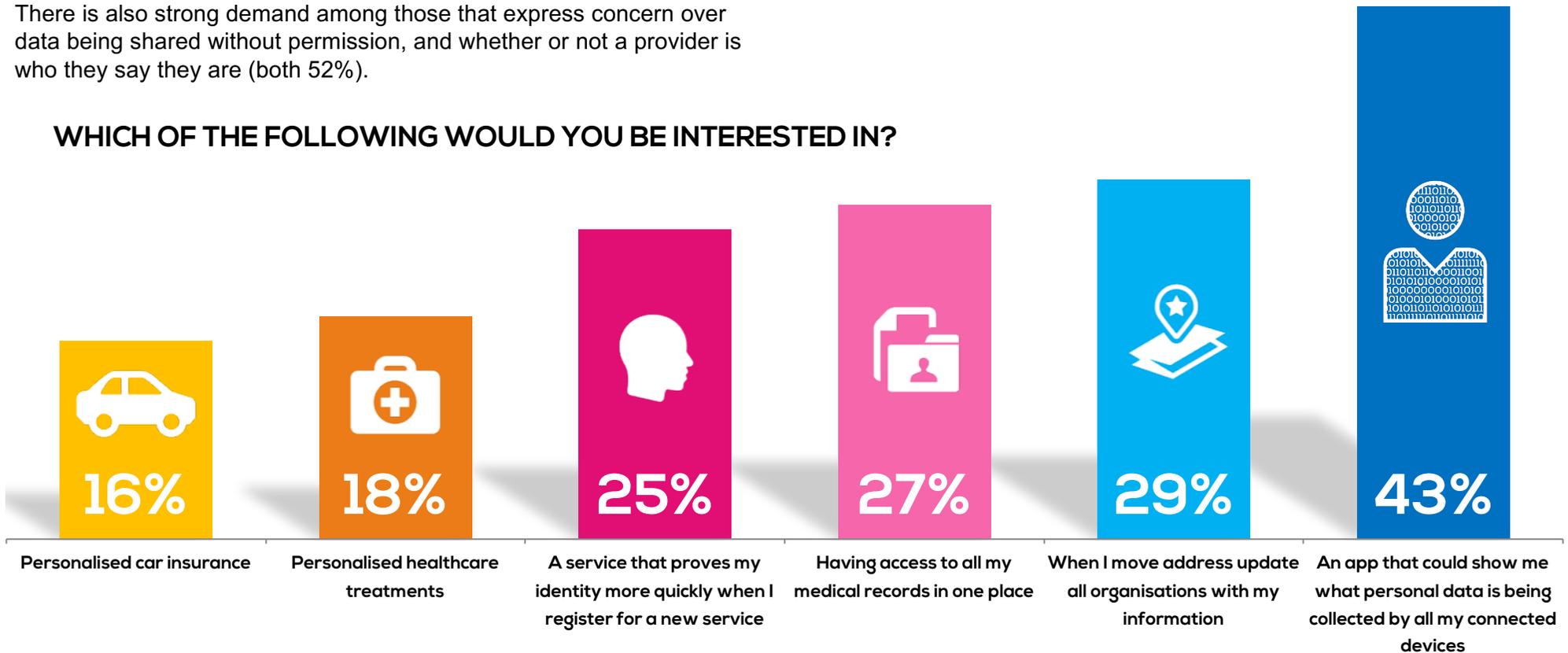
The research reveals a powerful latent demand for the new services that are emerging in a data-driven economy. While nascent in terms of adoption, trials taking place in innovation labs can be encouraged by fact that mobile users recognise the hypothetical benefits, showing the market’s strong potential.

43% said they’d be interested in a privacy-focussed app that shows what data is being collected across all of the user’s connected devices. There is also strong demand among those that express concern over data being shared without permission, and whether or not a provider is who they say they are (both 52%).

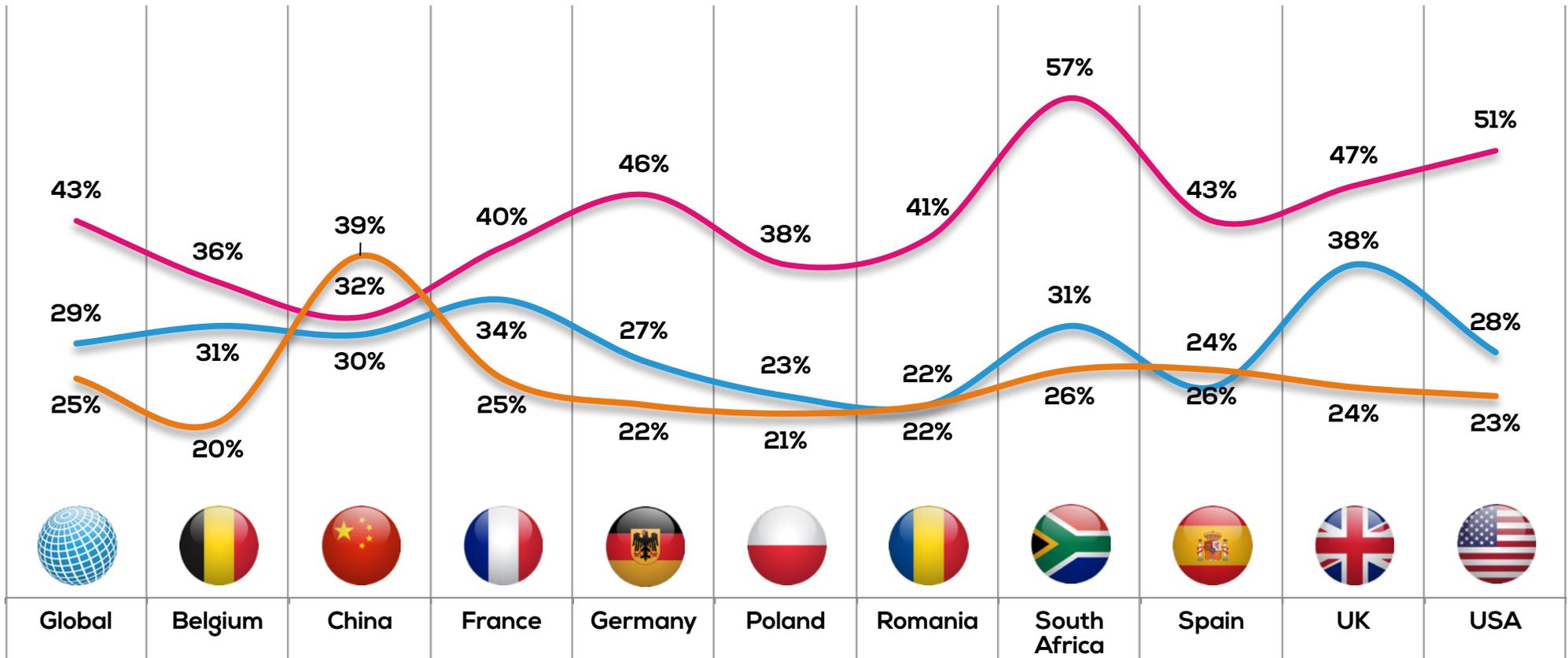
More than a quarter (29%) would appreciate a service that facilitated a change of address. One in four (25%) would appreciate faster identity verification, particularly in China (39%).

Consumers also responded well to services that facilitated healthcare. 27% said it would be useful to have access to all medical records in one place and 18% welcomed personalised treatment plans.

WHICH OF THE FOLLOWING WOULD YOU BE INTERESTED IN?



WHICH OF THE FOLLOWING DATA-DRIVEN SERVICES WOULD YOU BE INTERESTED IN?



- When I move address I could update all the organisations that need to know my information once only
- An app that could show me exactly what personal data is being collected by all my connected devices
- A service that proves my identity more quickly when I register for a new service

CONSUMERS FORESEE BENEFITS OF DATA PORTABILITY

One trust-building principle championed by regulators is the requirement for app or service providers to be able to transfer personal data to other companies upon request.

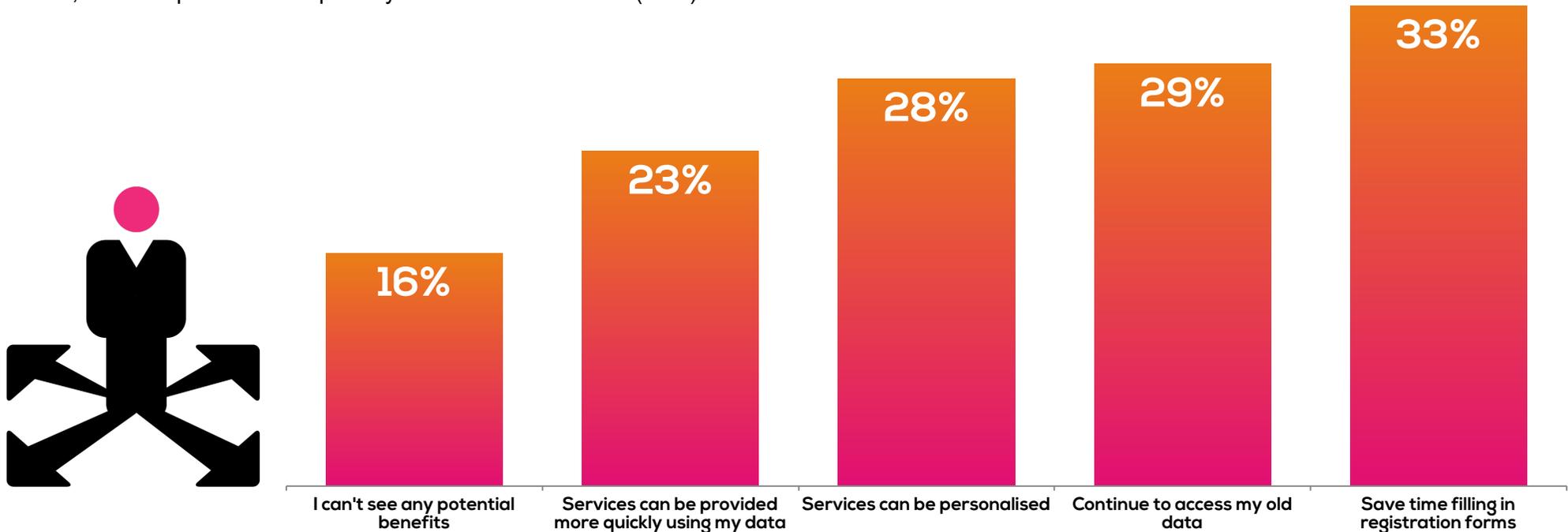
Data portability is some way off becoming operational reality. Challenges around interoperability and the technical questions around portability mean that it is one of the more difficult elements of data protection best practice to implement. However, it appears the investment will be worthwhile.

MEF’s research reveals that many mobile users can already picture how it might make their life more convenient. One in three (33%) understand that it might help them save time filling in registration forms, for example. This is especially true of South Africans (40%).

29% see value in being able to access old data rather than starting from scratch. For users of medical and fitness apps it’s 36%. 28% see the benefits of personalised services, not least in China (46%).

Users of certain kinds of services are most likely to recognise time saving benefits. 42% of banking app users, for example, see the benefit of the help data portability would provide in filling in forms (as opposed the global total of 33%).

IF IT WERE EASIER TO TRANSFER PERSONAL DATA BETWEEN APPS OR SERVICES WHICH OF THE FOLLOWING BENEFITS WOULD BE IMPORTANT?

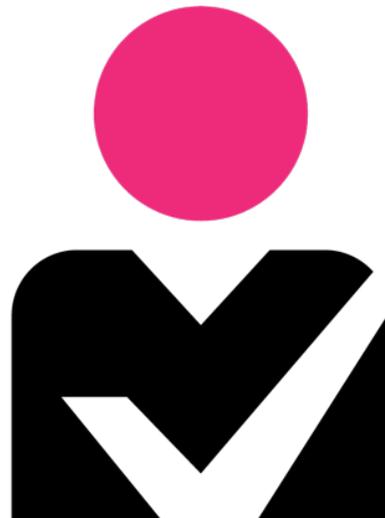


SAVVY CONSUMERS OPEN TO PERMISSION MANAGEMENT OPTIONS

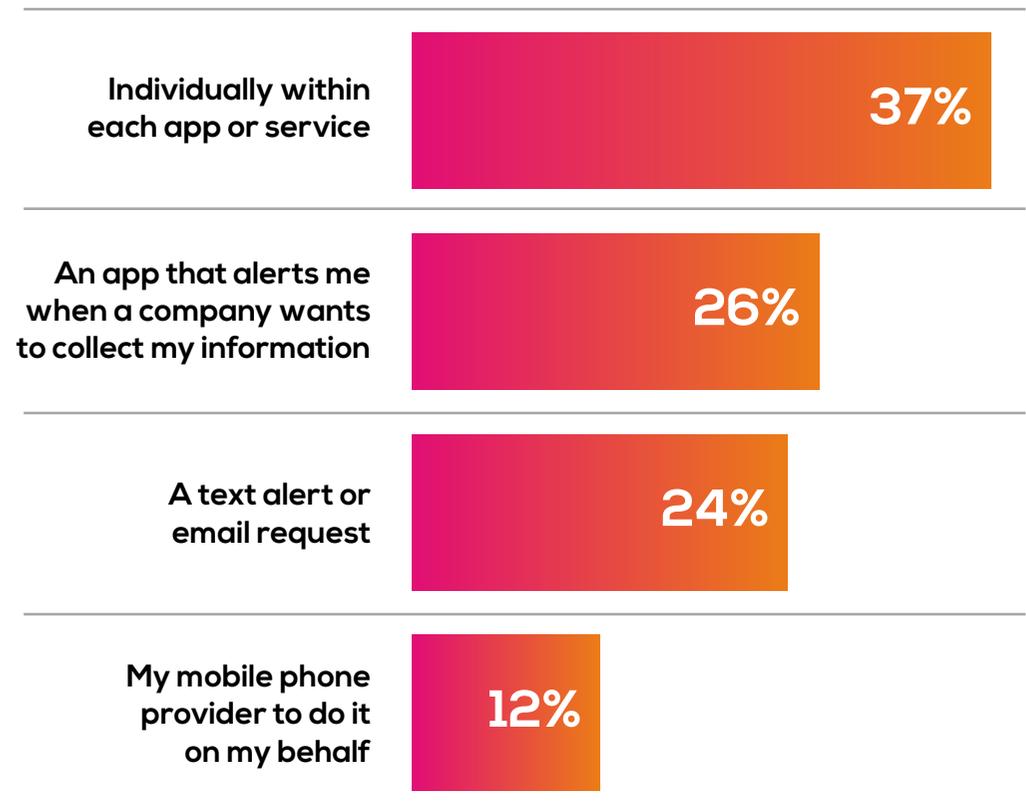
Consumers were asked *how* they should be asked permission to collect and process their personal data. Most (37%) suggested the most convenient way would be within each individual app or service.

Again however, Savvy Consumers showed encouraging levels of sophistication and an innate understanding of the Personal Data Ecosystem proposition. 1 in 4 (26%) suggested the best way to give permission is within a 'single app' that alerts them whenever any company wants to collect their information.

A further one in ten (12%) are happy for their mobile phone provider to manage permissions on their behalf. This is especially true of those who have had a bad experience in the past, or are put off my mobile services because they are too complicated (both 17%).



WHAT WOULD BE THE MOST CONVENIENT WAY FOR YOU TO GIVE PERMISSION?



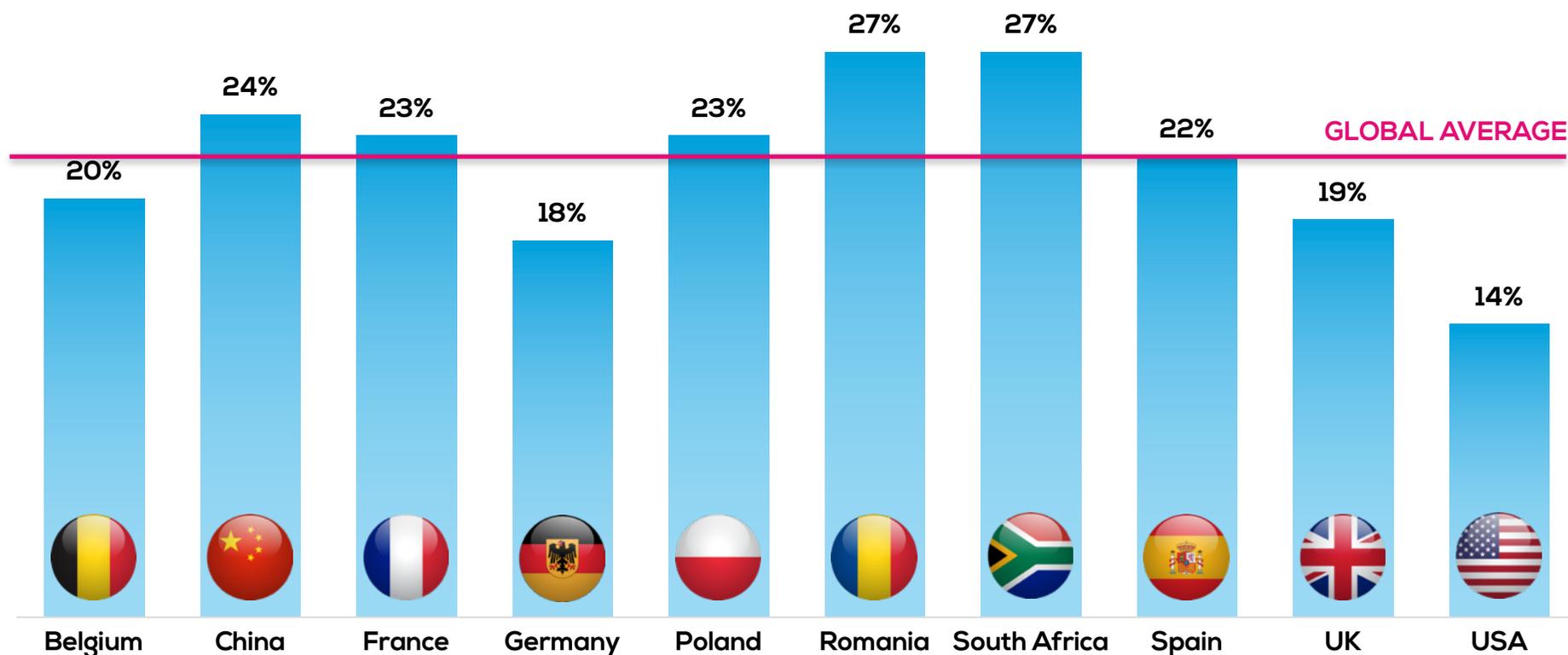
A person is shown from the side, holding a white smartphone. They are wearing a dark jacket and a silver metal watch. The background is a bright, hazy outdoor setting, likely a beach or park, with a warm, golden light from the sun setting or rising. The overall mood is serene and modern.

APPENDIX

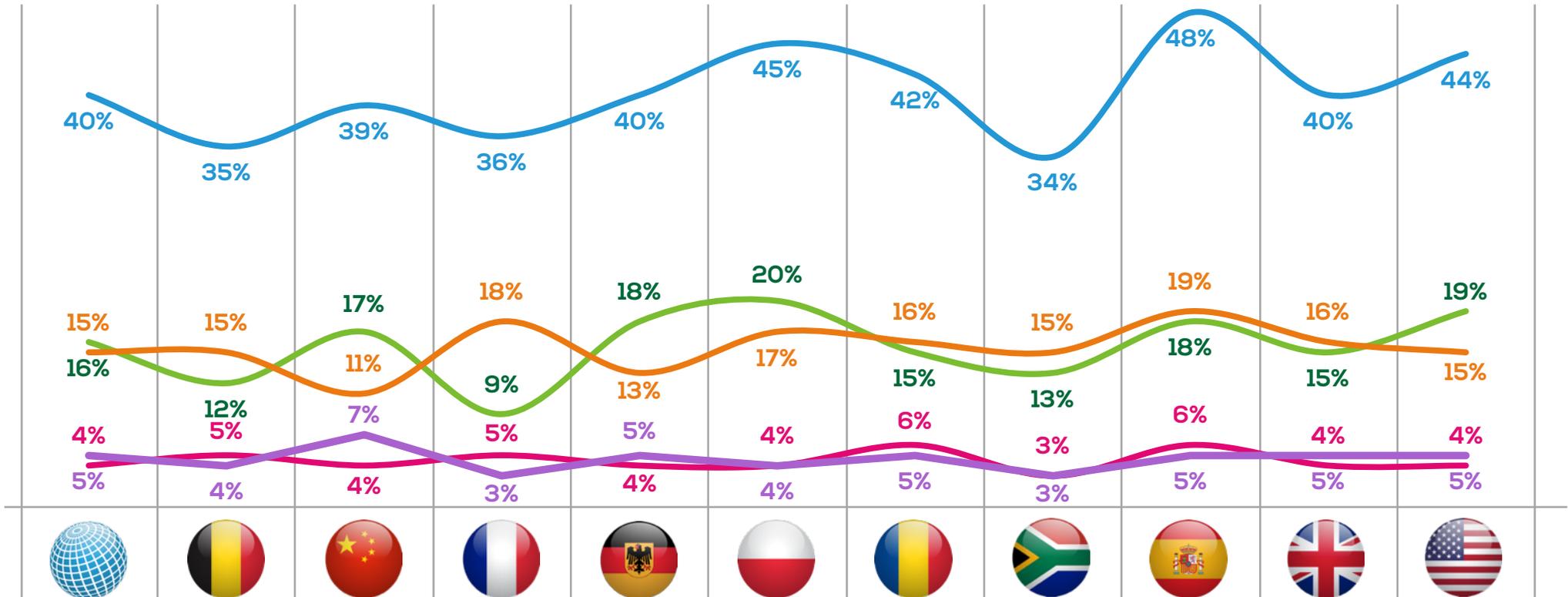
#GCTS17

WHO DO YOU TRUST TO MANAGE YOUR DATA?

I TRUST MY MOBILE OPERATOR MOST TO MANAGE MY DATA

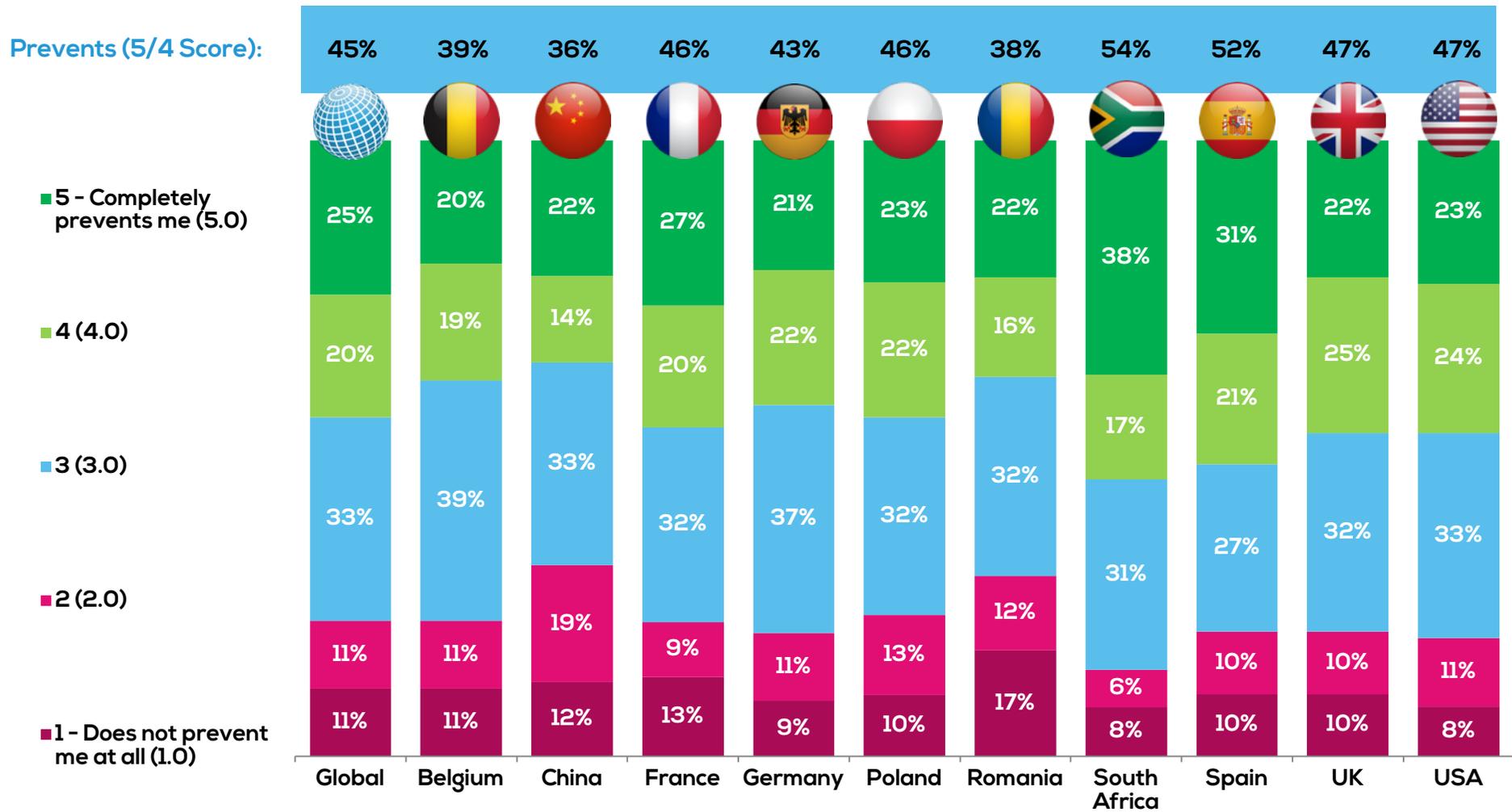


WHAT IS THE MAIN REASON YOU DON'T DOWNLOAD AND/OR USE MORE MOBILE APPS AND SERVICES?

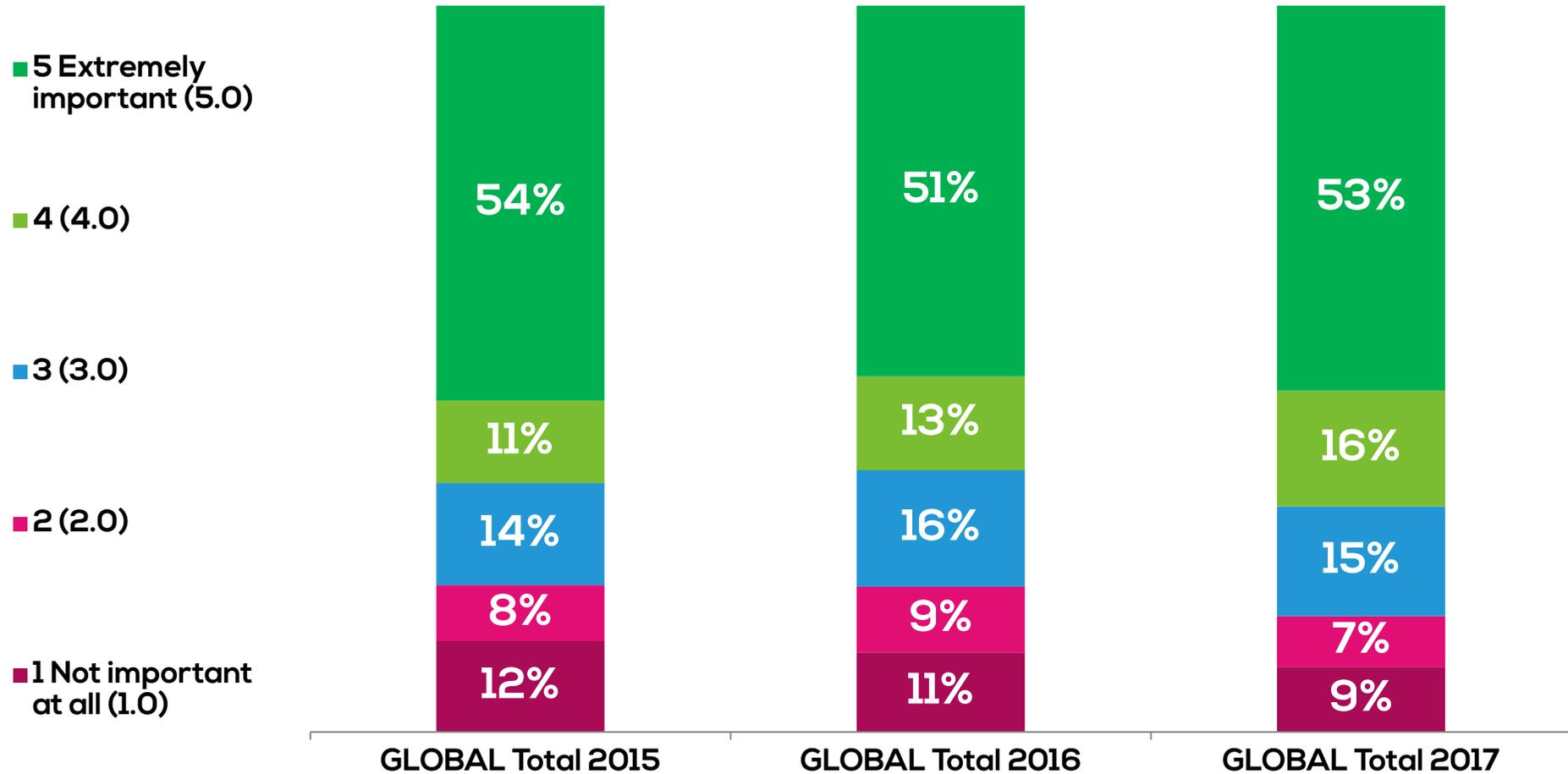


- NET Trust
- I don't want to share personal information like my location or browsing history.
- I don't trust the security
- I've read or heard negative news stories in the media
- I had a previous bad experience

TO WHAT EXTENT DOES A LACK OF TRUST PREVENT YOU FROM BUYING, DOWNLOADING OR USING SOME OR ALL APPS IN YOUR PHONE?

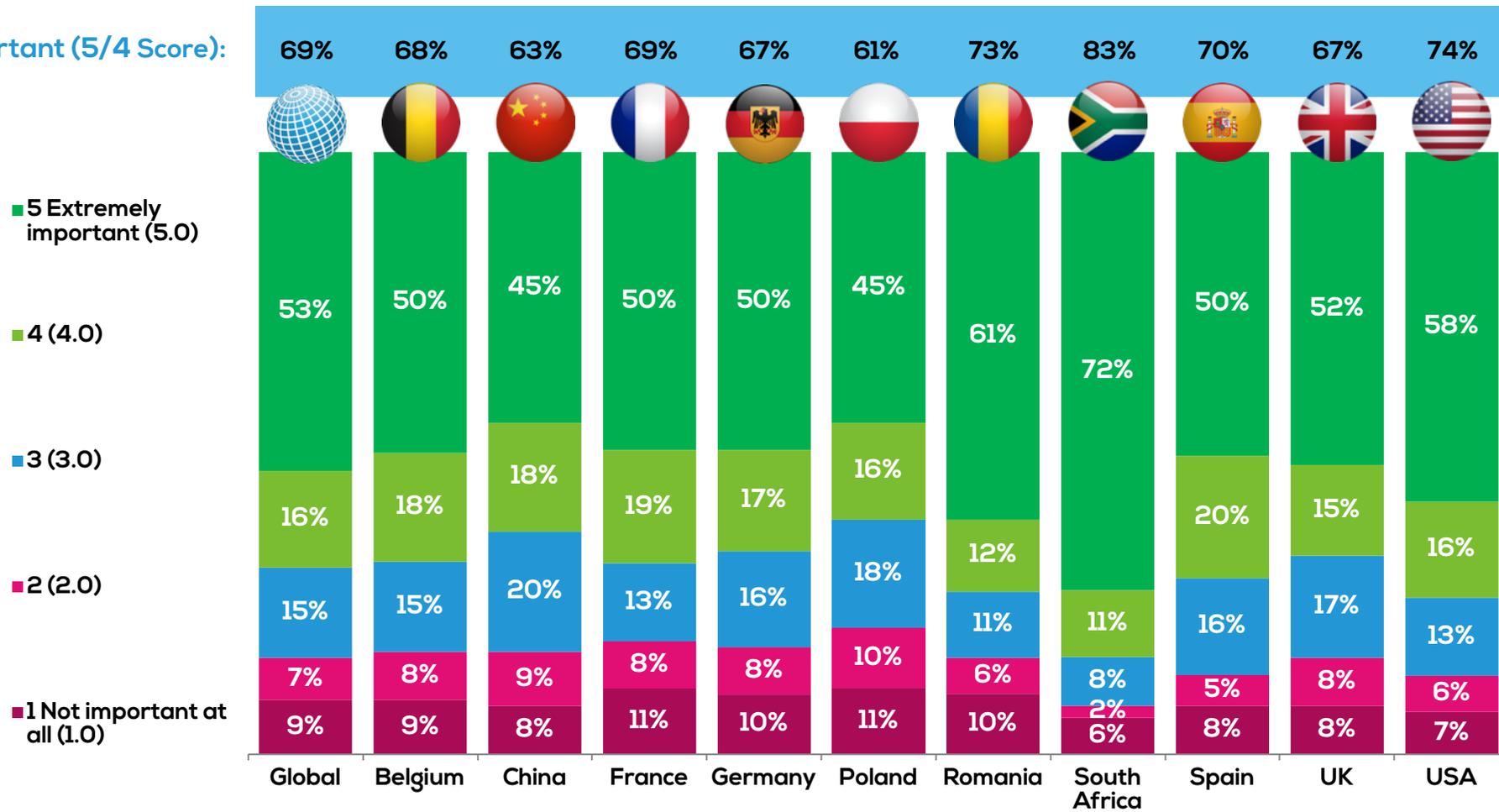


HOW IMPORTANT IS IT TO KNOW AN APP OR SERVICE IS USING YOUR DATA



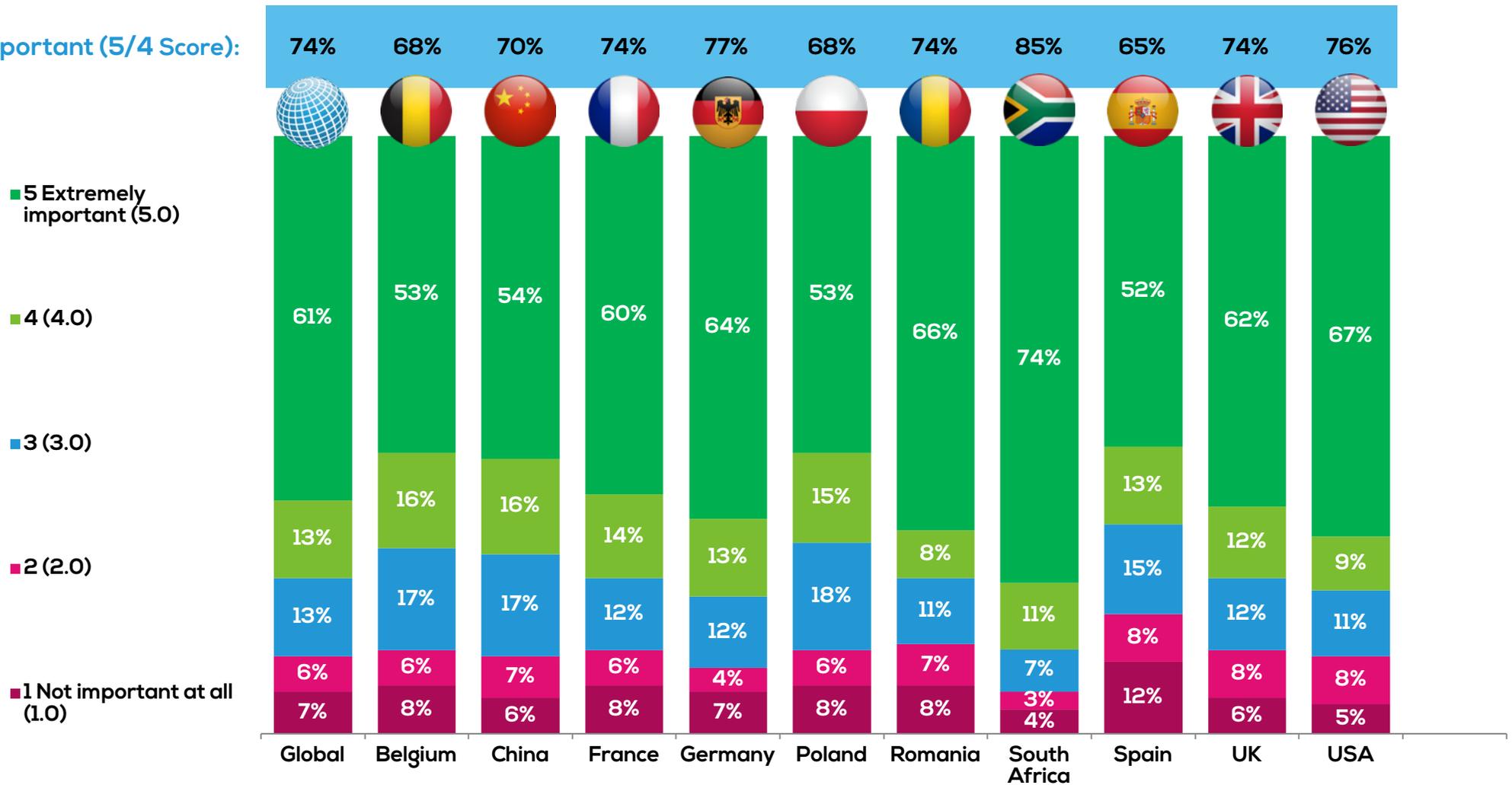
HOW IMPORTANT IS IT TO YOU TO KNOW THAT A MOBILE APP OR SERVICE IS USING YOUR PERSONAL DATA?

Important (5/4 Score):

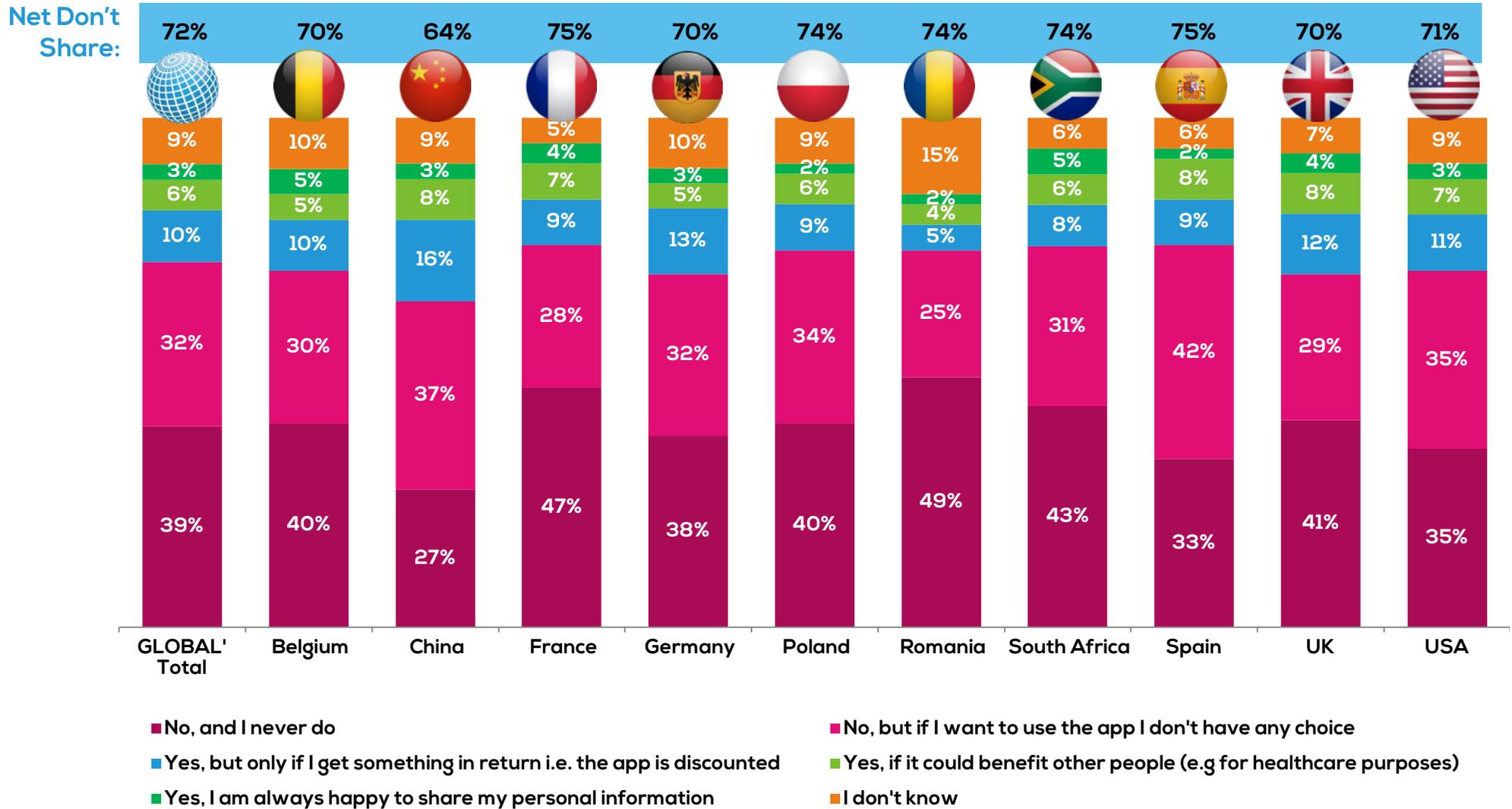


How important is it that a company deletes the personal data it has collected from you when asked?

Important (5/4 Score):

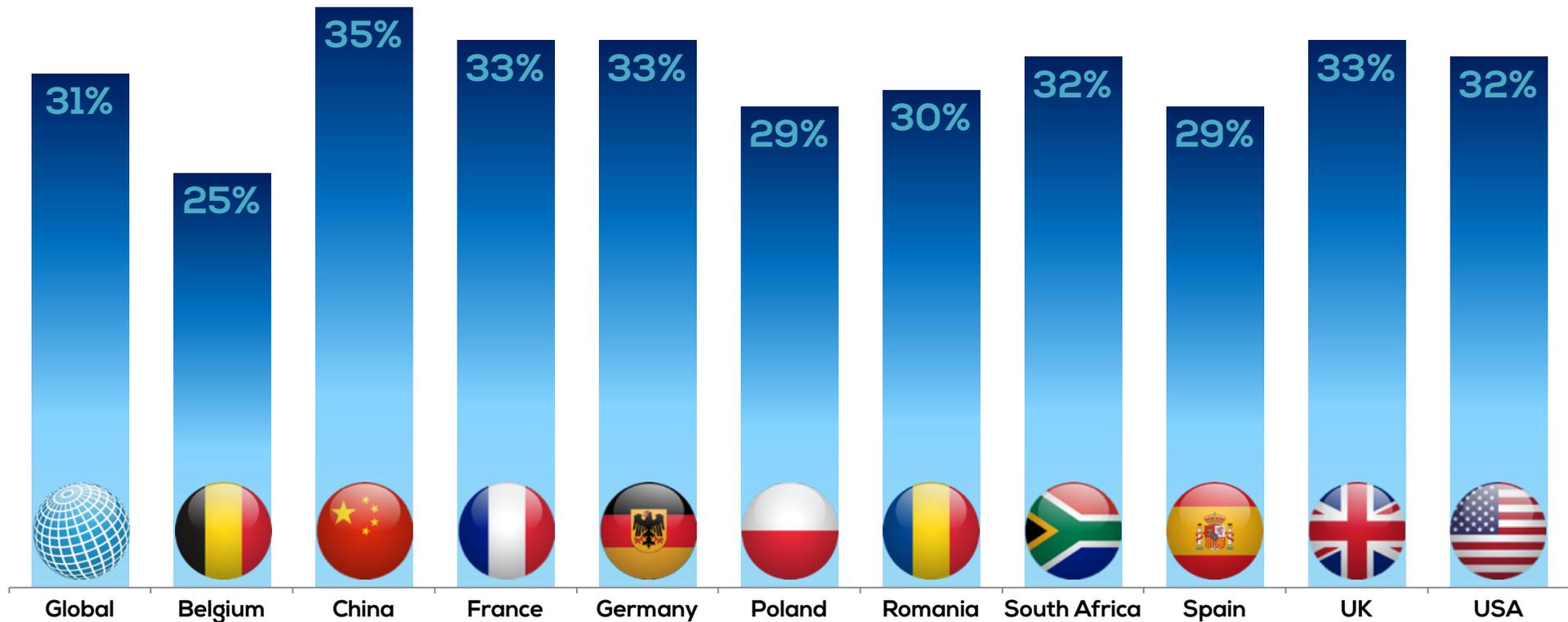


ARE YOU COMFORTABLE SHARING YOUR PERSONAL DATA WHEN YOU USE A MOBILE APP OR SERVICE?

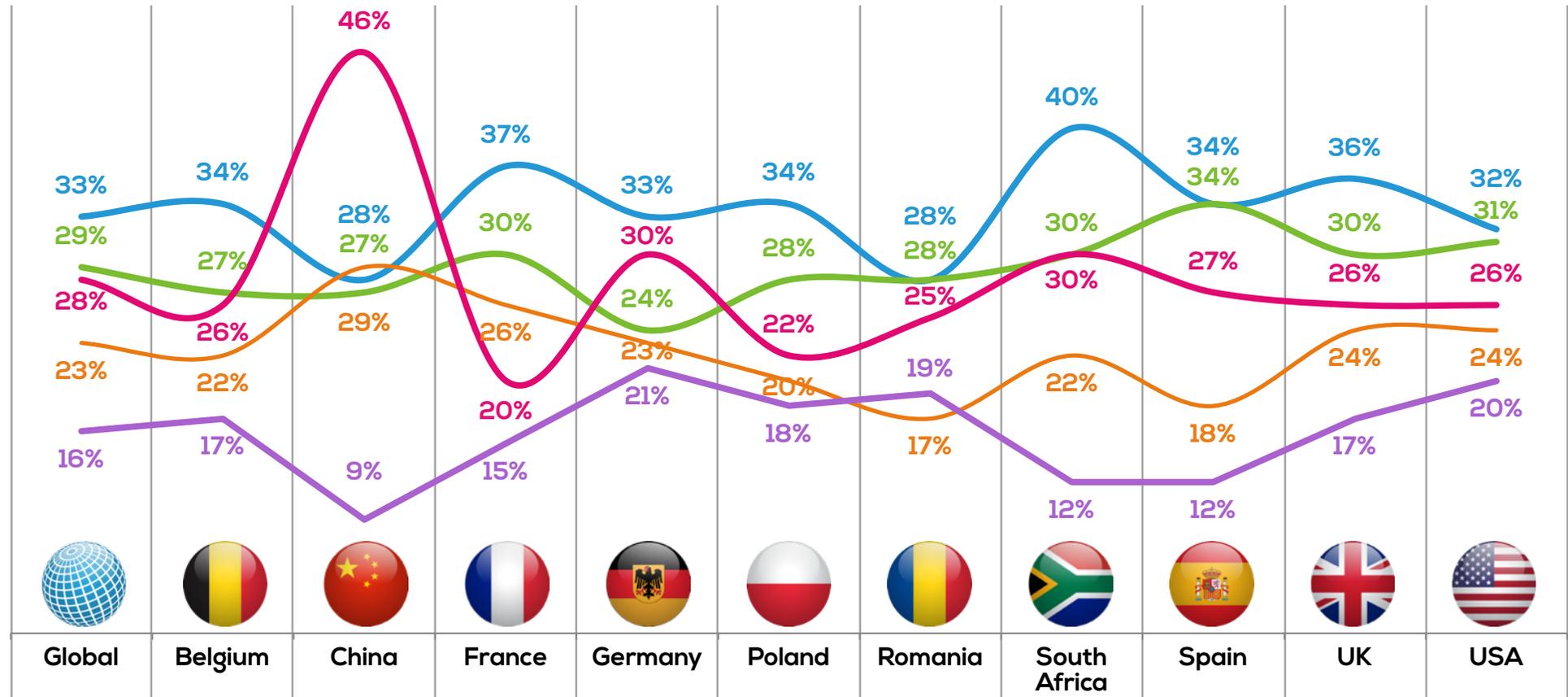


WHAT COULD COMPANIES OFFER IN EXCHANGE FOR USING YOUR PERSONAL DATA?

The ability to have your personal information returned to you or deleted at a time of your choosing

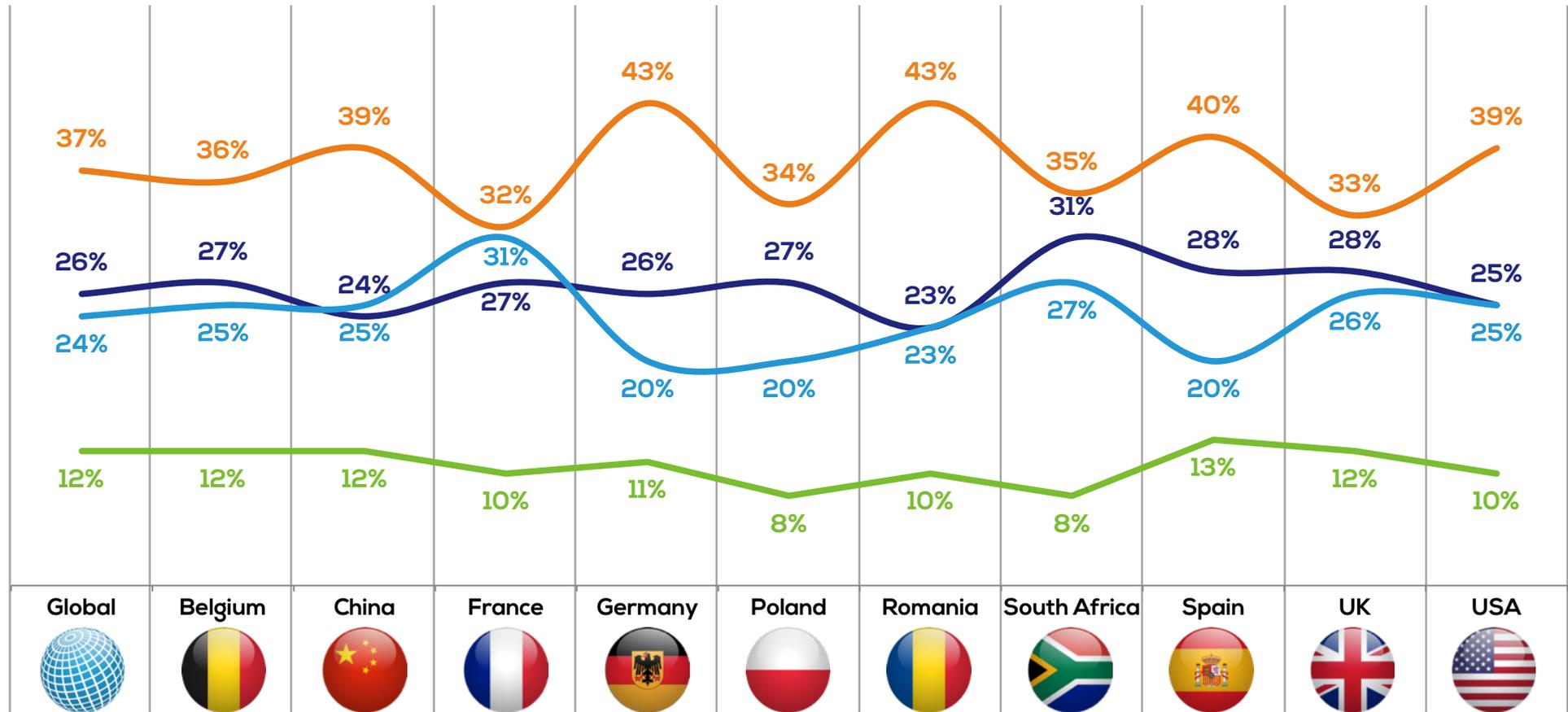


IF IT WERE EASIER TO TRANSFER PERSONAL DATA BETWEEN APPS OR SERVICES WHICH OF THE FOLLOWING BENEFITS WOULD BE IMPORTANT?



- Save time filling in registration forms
- Continue to access my old data (e.g. fitness tracking), rather than starting from scratch
- Services can be provided more quickly using my data
- Services can be personalised
- I can't see any potential benefits

WHAT WOULD BE THE MOST CONVENIENT WAY FOR YOU TO GIVE PERMISSION?



- Individually within each app or service
- A single app that alerts me when a company wants to collect my information
- A text alert or email request
- I'd like my mobile phone provider to do it on my behalf

ABOUT THE STUDY



#GCTS17

ABOUT THE STUDY

MEF's Global Consumer Trust Study

- Commissioned by global trade body Mobile Ecosystem Forum the field study was carried out by On Device Research in Q2 2017.
- It questioned over 6,500 Smartphone users in 10 countries: Belgium, China, France, Germany, Poland, Romania, South Africa, Spain, UK and USA.



About On Device Research

On Device Research is a research company that gathers responses on mobile devices - so far we've sent over 2.3 million surveys across 53 countries.

By conducting research on mobile phones and tablet computers we can reach consumers wherever they are, at any time and in any location.

Mobile research also brings fresh, instant responses that accurately capture consumers' feelings, thoughts and opinions.

For more information visit www.ondiceresearch.com

Methodology & Sampling

- Mobile panellists are sent an SMS invite to take part in the survey via their mobiles.
- The survey is automatically scaled to device type to enable the best survey experience for respondents.
- To ensure that results are robust and reflective, a sample frame was created for each market using key demographic and device information: Age, gender and device type.
- The framework served as the quotas for survey respondent for each market to ensure each of these above quota groups was designed to be representative of Mobile Media Users in each local market.
- Sources consulted to construct this sample frame include, but were not limited to: On Device Research panel demographics, network partners, MEF members and previous MEF research.
- A smartphone is defined as a device which has an operating system (iOS or Android) that provides the capability to download applications, synchronize with computers and connect to corporate networks.

THANKS TO OUR REPORT PARTNER



FORGEROCK®

ABOUT FORGEROCK

ForgeRock® is the Digital Identity Management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia. Get free downloads at <https://www.forgerock.com/> and follow us on social media: [Facebook](#) | [Twitter](#) | [LinkedIn](#)

STUDY PARTNERS



ABOUT ORANGE

Orange is one of the world's leading telecommunications operators with sales of 41 billion euros in 2013 and 159,000 employees worldwide at 30 September 2014, including 99,800 employees in France.

Present in 30 countries, the Group has a total customer base of 240 million customers worldwide at 30 September 2014, including 182 million mobile customers and 16 million fixed broadband customers. Orange is also a leading provider of global IT and telecommunication services to multinational companies, under the brand Orange Business Services.



digi.me

ABOUT DIGI.ME

Digi.me is a personal data exchange platform that allows consumers to gather together information currently scattered around the web and share it on their terms under the company's bespoke Consent Access process.

Digi.me is working with world-leading businesses in the health, finance, FMCG and telco sectors on projects unlocking the benefits of targeted and consented data sharing for both consumers and organisations. To date digi.me has raised more than \$10 in investor funding and has teams in the UK, Europe and North America.



QUESTIONNAIRE

1. What is the main reason you don't use more mobile apps and services?
2. Are you comfortable sharing your personal data when you use a mobile app or service?
3. When using mobile apps and services, which of the following concern you?
4. Have concerns over privacy and/or security ever caused you to:
 - Stop using an app or service
 - Delete an app or service
 - Leave a negative review
 - Warn friends or family
 - Use a competitive app or service
5. What personal information do you consider most sensitive?
6. When it comes to your personal data who do you trust to manage it?
7. Which personal data related would concern you the most?
8. How important is it to you to know that a mobile app or service is using your personal data?
9. When signing up to use a mobile app or service, do you
 - Always read a privacy policy or terms & conditions first
 - Sometimes read a privacy policy or terms & conditions first
 - Never read a privacy policy or terms & conditions
10. How much time would you spend managing how apps you use your data?
11. What information do you need to know in order to feel comfortable using a mobile app or service?
12. To what extent do you feel you are in control of the way your personal data is used by third parties?
13. In what circumstances should a mobile app or service ask permission before using your personal data?
14. When is the best time to ask for your permission regarding accessing or using your personal data?
15. What would be the most convenient way for you to give permission?
16. How important is it that a company deletes the personal data it has collected from you when asked?
17. How often do you think you might ask a company to delete the data it has collected from you?
18. If it were easier to transfer personal data between apps or services which of the following benefits would be important?
 - Save time filling in registration forms
 - Continue to access my old data (e.g. fitness tracking), rather than starting from scratch
 - Services can be provided more quickly using my data
 - Services can be personalised

QUESTIONNAIRE

19. Which of the following data driven services would you be interested in?
- When I move address I could update all the organisations that need to know my information once only
 - Having access to all my medical records in one place, I could immediately provide relevant information to a doctor or hospital
 - An app that could show me exactly what personal data is being collected by all my connected devices
 - Personalised car insurance based on my driving habits
 - Personalised healthcare treatments based on fitness data
 - A service that proves my identity more quickly when I register for a new service
20. What could companies offer in exchange for using your personal data?
21. To what extent does a lack of trust prevent you from buying, downloading or using some or all apps in your phone?
22. What is it about an app or service that makes it trustworthy?
23. And what makes you lose trust in an app or service?
24. Which of the following would help you have more trust in how an app or service uses your data?
- It tells me clearly exactly what information is being collected and what is done with it
 - I can choose which types of information are being collected
 - I can decide how long that information is stored for before it is deleted
 - I can decide whether it is shared with third parties
 - I can request that all information is deleted
 - I can request that my information is returned to me or sent to another provider
 - I can withdraw permission to use my data
 - There's a easy contact mechanism for me to talk to the company collecting the information
25. How might you reward an mobile app or service you trust?



MEF

MOBILE ECOSYSTEM FORUM

ABOUT MEF

The Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. We provide our members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that drives inclusion for all and delivers trusted services that enrich the lives of consumers worldwide. Established in 2000 and headquartered in the UK, MEF has Regional Chapters across Africa, Asia, Europe and Latin America.



The editorial and analysis in MEF's Global Consumer Trust Survey 2016/7 contains references to third party products, services and metrics. This data is sourced by the author from official press material distributed by the companies concerned. Its inclusion does not represent a recommendation by the MEF or the authors of this report in anyway. All other trademarks are the property of their respective owners.

© 2017 Mobile Ecosystem Forum Ltd. All Rights Reserved. No part of this publication may be reproduced, distributed or made available without permission of the copyright owner.