



MEF
MOBILE ECOSYSTEM FORUM

**FULL
REPORT**

**7TH CONSUMER
TRUST STUDY**
**IT'S TIME TO SERVE
THE INDIVIDUAL**

2021

FOREWORD

We live in a connected, increasingly digital world. People are connected. They use multiple connected devices, e.g., smartphones, computers, and tablets, to navigate their life online. They are concerned. They are concerned for their privacy and security and how their data is used. And they want control. They want to take control of their data.

In this year's study, we find the industry is falling short of people's expectations across almost all privacy and security items measured. Roughly two-thirds of people expect organizations to respect their privacy and to keep their data secure, but far fewer agree that this is the experience they are having today.

In years past, and this year is no different, more and more people are taking steps to protect their personal data. Yet we find these steps do not appear to be helping people's sense of well-being. Around two-thirds of study respondents report they still feel at risk, overwhelmed, or that their actions take too much time and have unclear benefits. In other words, the majority of mobile subscribers are feeling impaired, helpless, or indifferent. There is also evidence that some of those who feel more self-assured may have misplaced confidence.

Little of this bodes well for the industry. What do mobile subscribers do in response to a lack of trust when they have concerns for their privacy and security? They delete an app or service, avoid using or stop using an app or service, avoid making a purchase, or may even use a competitive app or service which they trust more. The message from this year's trust study is clear. We can do better as an industry. It's time we step up to appropriately serve the connected individual.

It is imperative that the industry minds the trust gap. Mobile apps and services providers can and need to do more to help people feel safe. As an industry, we need to ensure people can obtain secure, cross-platform access to their apps, services, and data, and trust that they are truly being protected. We need to give them personal data management and exchange capabilities. We need to provide them with digital rights management and guardianship tools. We need to give them clear and transparent security utilities. And, perhaps most importantly, we need to provide them with easily accessible, unambiguous, and actionable personal information management education and support.

Let's give the people what they want. Let's help them conveniently get value from their apps and services, while simultaneously protecting themselves and controlling their personal data, so that they may live a safer, simpler, and more secure life online.



CRAIG THOLE
SENIOR VICE PRESIDENT, PRODUCT

THE ECOSYSTEM VIEW

You could spend hours admiring a work of art, but even more time describing the evolution of an artist's career. The same does apply to this report and the six that came before it. There are clear learnings from this year, but also uncomfortable trends shown over the seven years. The times are ready for change. I believe personal data will still be traded or exchanged in the future, but users seem to be asking for better customer experience and more security. Some parts of the industry seem to be taking notice too.

MEF's **7th Consumer Trust Study** is packed with real insight. **The problem in the industry is clear: customer expectations on privacy and security are not met.** It is true that overall users seem to accept the status quo, but the long-term stability of the trade-off 'personal data' vs. 'access to the Internet' does not look so certain. This year's study provided a segmentation highlighting how **emotional drivers as well as rational ones determine the smartphone user's reaction to security and privacy.** Mobile service providers really need to start understanding the **'trust profiles'** of their users. **There might not be a single solution but multiple ones.** Thinking about who you are talking to and how or what you should talk about is a real gap in the industry. This research makes some great points on starting that process.

However, reading the full set of the seven annual reports gives you a sense of the significance of the underlying trends. If people are saying that users do not care about their personal data, they should read our studies. The concern on personal data is growing steadily. One snapshot does not give you the sense of the velocity and the number of changes happening over time. Simply put, **our series of reports have shown deteriorating levels of trust, increasing protection activities, and disappointment for the complexity of existing solutions.** Things are moving fast, and the industry needs to take seriously the mismatch from user expectations and service delivery seriously.

I should also say that not all is negative. **Some companies are actively addressing these issues, and the 2021 study saw an improvement on the security of data year on year.** Most customers are ready to engage with new solutions and approaches. There is a clear threat to existing services but also an opportunity to differentiate in the market. **The main challenges remain customer experience and ease of use.**

The Mobile Ecosystem Forum will be active to review and discuss all developments in the coming years. **Join MEF's Personal Data & Identity Initiative to shape the agenda of the next personal data economy.**



DARIO BETTI
CEO



THE MOBILE
ECOSYSTEM FORUM
OFFERS MARKET
DATA TO ITS
MEMBERS AND TO
THE INDUSTRY TO
PROMOTE
CONSUMER
UNDERSTANDING
AND ADVANCING OF
LONG TERM
SUSTAINABLE
PRACTICES AND
BUSINESS MODELS

AN EXECUTIVE
SUMMARY IS
AVAILABLE FOR
FREE TO ALL

MEF MEMBERS
HAVE GOT ACCESS
TO THE FULL
REPORT AND THE
DATA SET

ABOUT MEF

Mobile Ecosystem Forum is a **not-for-profit 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 delivers trusted services worldwide. Established in 2000 and headquartered in the UK, MEF's members are active across Africa, Asia, Europe, the Middle East, and North and Latin America.

MEF provides a community that offers **Insight** (reports, surveys, market guidance); **Interaction** (events, networking, visibility) and **Impact** (advocacy, code of conducts, industry initiatives).

To join the MEF communities please email info@mobileecosystemforum.com.

Contact [Sam](#) if you'd like to contribute an article.

If you would like to explore the range of MEF Member sponsorship opportunities available at any MEF Connects then please contact [Susan](#).

Follow us on [LinkedIn](#), [register](#) for the member area and [subscribe](#) to MEF's newsletters to keep up to date with MEF activities throughout the month.

DARIO BETTI
CEO

SUSAN FINLAYSON-SITCH
DIRECTOR OF OPERATIONS

JAMES WILLIAMS
DIRECTOR OF PROGRAMS

EWA PEPPITT
GLOBAL MEMBER MANAGER

SAM HILL
GLOBAL COMMUNICATIONS MANAGER

CAROL BENITES
MEMBER & MARKETING COORDINATOR

MIKE ROUND
PROJECT DIRECTOR REGISTRY

NIKKI BAILEY
REGISTRY OPERATION MANAGER

ANDREW PARKIN-WHITE
ADVISOR IoT

DANIEL MENSİ
ADVISOR BLOCKCHAIN

SERAFINO ABATE
ADVISOR REGULATION

DHONI IBRAHİM
DESIGNER

CNTENTS

<u>FOREWORD</u>	<u>2</u>
<u>THE ECOSYSTEM VIEW</u>	<u>3</u>
<u>ABOUT MEF</u>	<u>5</u>
<u>METHODOLOGY AND DEFINITIONS</u>	<u>7</u>
<u>EXECUTIVE SUMMARY</u>	<u>8</u>
<u>PRIVACY AND SECURITY PERCEPTIONS</u>	<u>13</u>
<u>DATA PROTECTION ACTIONS</u>	<u>25</u>
<u>SEGMENTATION: A TOOL TO BETTER UNDERSTAND AND SERVE USERS</u>	<u>35</u>
<u>SMARTPHONE BEHAVIOUR AND CONNECTED DEVICES</u>	<u>49</u>
<u>METHODOLOGY</u>	<u>57</u>
<u>MORE FOR MEF MEMBERS</u>	<u>59</u>

METHODOLOGY AND DEFINITIONS

MEF’s 7th Annual Smartphone Study was carried out in January 2021 . On behalf of MEF, On Device Research surveyed 6,500 smartphone users, 650 in each of 10 markets. Where appropriate, year-on-year comparisons are made.



KEY DEFINITIONS

PERSONAL DATA: Any information which is unique to you that can be collected via the devices you interact with. Depending on what devices and services you use, examples include your contact details, buying history, social media updates, photos and videos, travel history as well as financial information, health and fitness information and education.

PRIVACY: Your ability to control your personal data and what data is shared about you when you use the devices.

SECURITY: Level of exposure to and risk of data harm such as identify theft or financial fraud.



STUDY SNAPSHOT: TIME TO SERVE THE INDIVIDUAL



**THE SILENT DISCONTENT: A HUGE GAP
EXISTS BETWEEN USER EXPECTATIONS AND
EXPERIENCE IN PRIVACY AND SECURITY**



**IN 2021 USERS REPORT IMPROVEMENT IN
MOBILE PRIVACY AND SECURITY**



**EVEN MORE USERS ARE TAKING STEPS TO
PROTECT THEMSELVES**



**CONFIDENCE IS NOT GROWING WITH EXPERIENCE
- MANY REMAIN APPREHENSIVE EVEN AFTER
PROTECTIVE MEASURES ARE TAKEN**



**USERS COULD BE MORE PROACTIVE IF TOOLS
WERE LESS EXPENSIVE, EASIER TO MAKE
SENSE OF AND NAVIGATE**



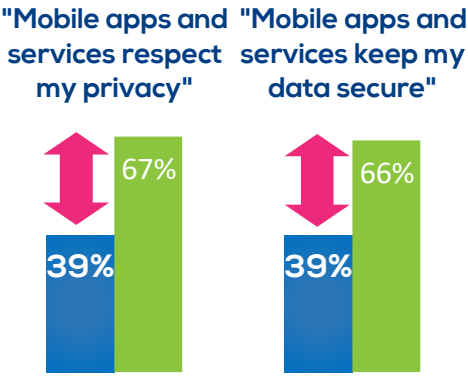
**TRANSPARENCY AND CONTROL ARE KEY
USER VALUES**

KEY FINDINGS 1/2

USERS SACRIFICE PRIVACY AND SECURITY FOR ACCESS TO VALUED SERVICES

While user expectations are generally met for ease and convenience, the perceived experience falls short when it comes to privacy and security, particularly for women and those aged over 45. Fewer than half are confident that mobile apps and services respect their privacy or keep their data secure, resulting in less openness to and usage of additional services. The privacy paradox remains.

- Agree that needs are met
- Consider factor as important



SMARTPHONE USERS BEGIN TO SENSE IMPROVEMENT IN THE MOBILE ENVIRONMENT

A significant minority (43%) believe that privacy controls and security have improved in the past year. However, many others do not perceive any change, resulting in an uneasy value equation when it comes to sharing personal data.



MORE AND MORE USERS TAKE PROTECTIVE STEPS, BUT REMAIN EXPOSED TO HARM

The trend for taking protective action has continued, with increasing numbers of smartphone users taking steps such as managing settings and masking their identity, in particular those who are younger or more affluent. However, exposure to data harm is as prevalent as ever and few consider themselves fully protected.

PROPORTION WHO HAVE TAKEN ONE OR MORE PROTECTIVE STEPS



KEY FINDINGS 2/2

PROTECTIVE ACTIONS DO NOT NECESSARILY DRIVE CONFIDENCE

Smartphone users' sense of well being is mixed. Protective actions do not necessarily correlate with a sense of privacy, security, or control. Our new segmentation reveals that those who take the most protective action still feel at risk, while those who consider themselves most confident are in fact the least likely to have taken protective actions or to have experienced harm.

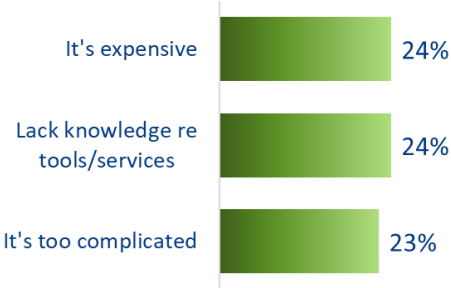
NO.1 ATTITUDE GLOBALLY:

"I take a number of actions to protect my personal data but I still feel at risk"

COST, KNOWLEDGE AND PERCEIVED COMPLEXITY ARE KEY BARRIERS

Users could take more preventive action to defend their personal data. In addition to lower confidence and motivation among some users, many lack the knowledge to navigate their options or report that services are too expensive.

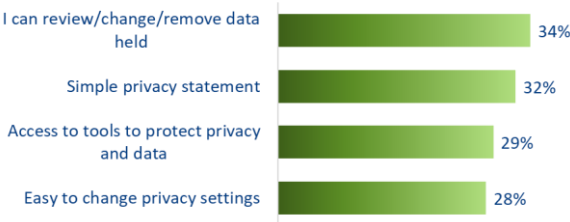
WHAT PREVENTS YOU FROM TAKING ADDITIONAL ACTION TO PROTECT YOUR PERSONAL DATA AND IDENTITY? (TOP 3 REASONS)



TRANSPARENCY AND CONTROL ARE KEY VALUES FOR USERS

To increase user confidence when sharing personal data with mobile apps and services, the top requirement is transparency and control over what data is stored. As seen in previous studies, many smartphone users do not feel in full control of their data.

FACTORS WHICH WOULD GIVE GREATER CONFIDENCE WHEN SHARING PERSONAL DATA (TOP 4)



LESSONS FOR THE INDUSTRY

COMMUNICATE POSITIVE CHANGES IN THE MOBILE ENVIRONMENT

There is already some positive momentum in terms of users feeling that some parts of the industry are evolving in a positive direction on privacy and security, but there is an opportunity to drive this perception more broadly.

BUILD TRUST WITH DIFFERENT EMOTIONAL ENGAGEMENT STRATEGIES

There is no 'one-size-fits-all' solution to address privacy and security in the smartphone economy. Strategies should take account of both rational and emotional variables: MEF's segmentation is a tool to facilitate this.

DESIGN BETTER CUSTOMER EXPERIENCES

While the vast majority of smartphone users now understand that they should act to protect themselves, few understand how to do so in a comprehensive way. The industry must support knowledge building and provide evidence of efficacy.

PROMOTE IMPARTIAL GUIDANCE

To address the perceived complexity in terms of tools and services, users would benefit from a trusted, impartial voice to advise on risk reduction tailored to their needs.

OPPORTUNITY TO DIFFERENTIATE ON TRUST

Vendors are underserving key user values around privacy and security: simply meeting user needs in this area could be a source of differentiation. Reflecting the fact that transparency and control are key user values, best-in-class services will make enacting privacy rights the simplest of user tasks.



MEF
MOBILE ECOSYSTEM FORUM

PRIVACY AND SECURITY PERCEPTIONS

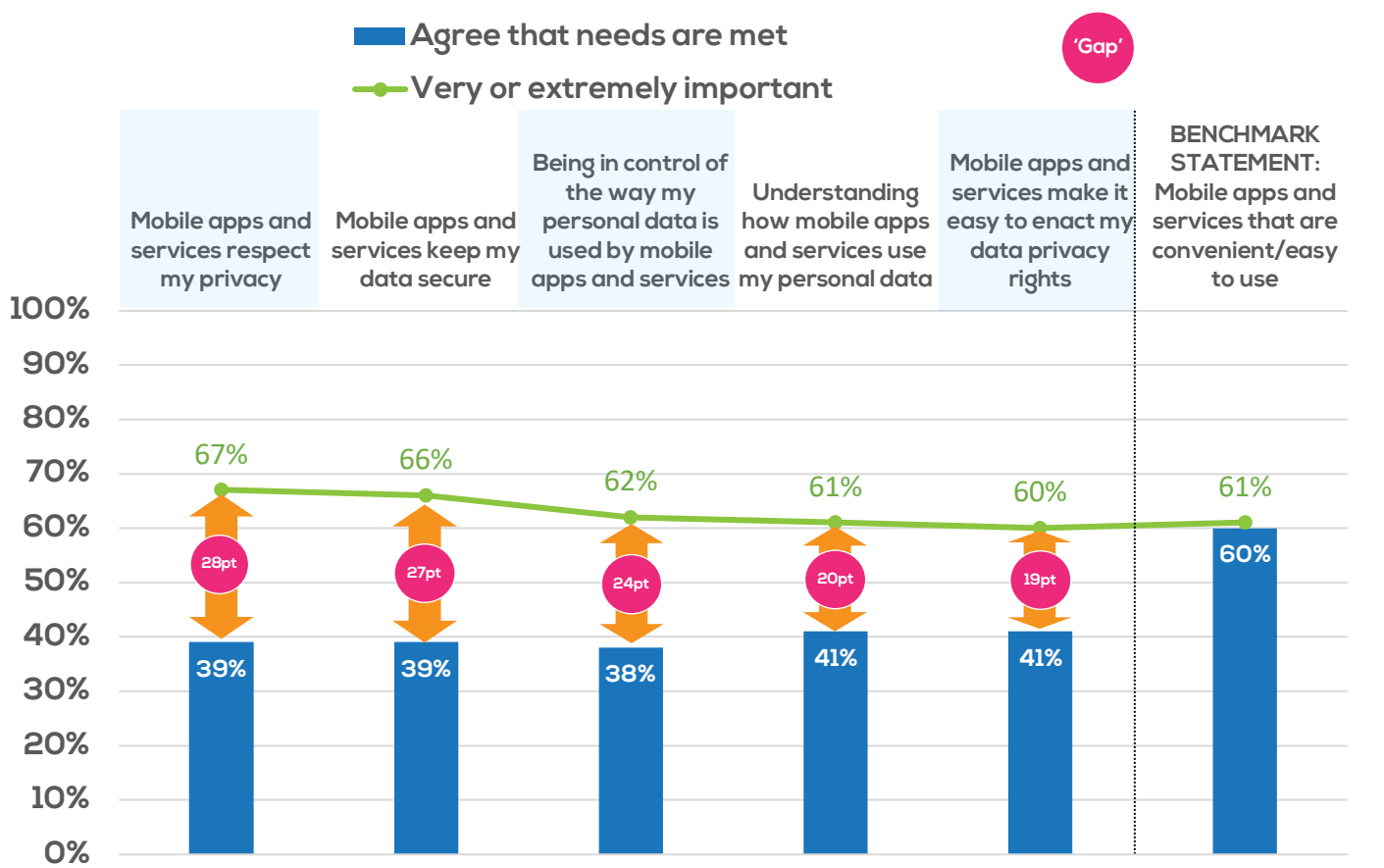


CHASM BETWEEN EXPECTATIONS AND DELIVERY WHEN IT COMES TO DATA PRIVACY AND SECURITY

When it comes to data privacy and security, a significant gap exists between what is perceived to be important and what is perceived to be delivered.

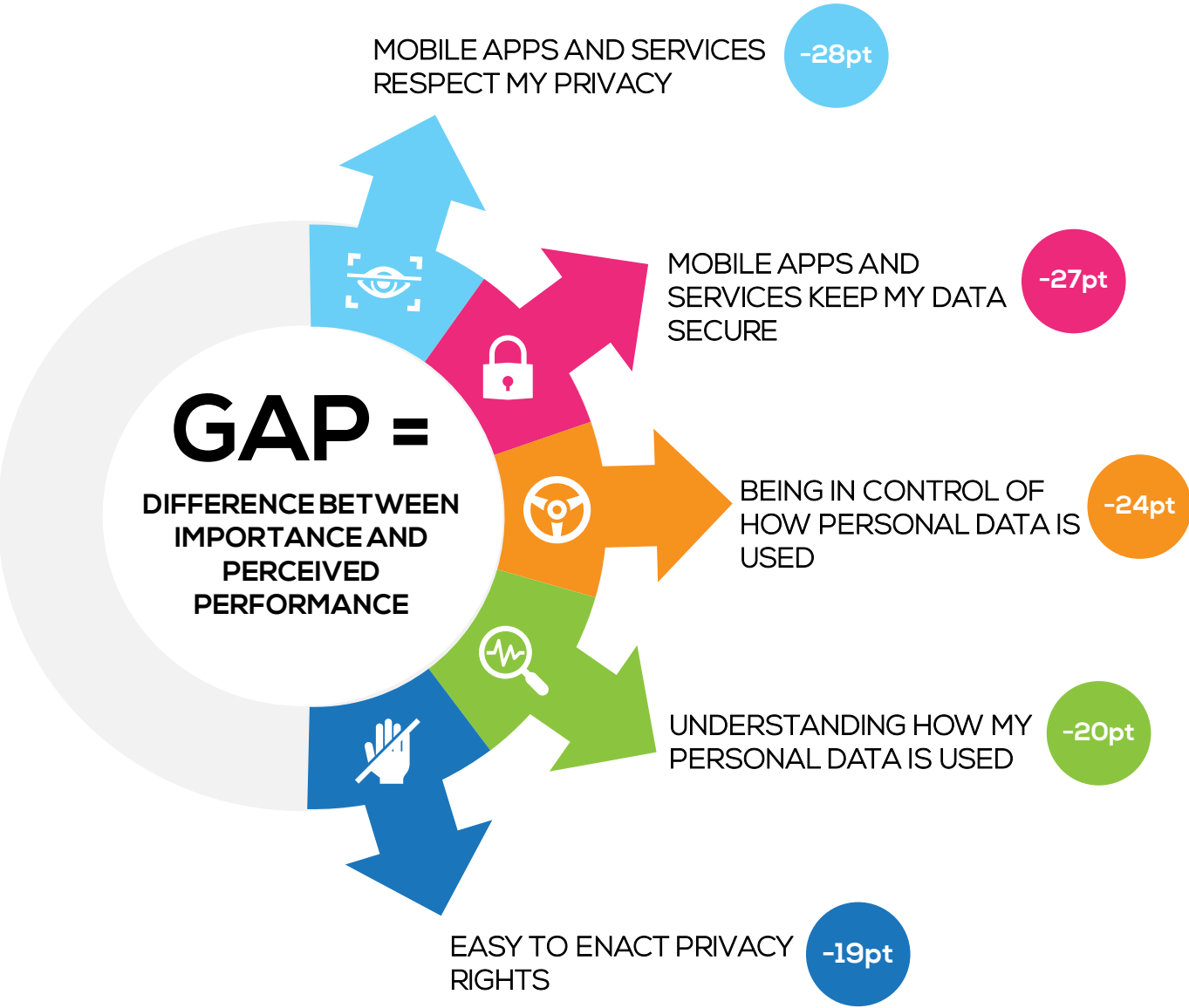
Privacy and security are equally valued (two thirds recognise these as very or extremely important) and over 3 in 5 smartphone users desire control and transparency regarding how their personal data is used. Yet far fewer can agree that their needs are met on any of these factors, in contrast to perceptions of apps being easy and convenient to use.

GAP ANALYSIS: IMPORTANCE VS. PERCEIVED PERFORMANCE



Base: All respondents, n=6,500. Gap = 'Extremely or very important' minus 'Agree strongly or slightly'
Importance question: To what extent do you agree with the following statements? Scale from 'Not at all important' to 'Extremely important'
Performance question: To what extent do you agree with the following statements? Scale from 'Disagree strongly' to 'Agree strongly'



THE INDUSTRY IS NOT MEETING USER NEEDS, RESULTING IN A TRUST EXPECTATION 'GAP'



THE EXPECTATION 'GAP' IS WIDEST FOR WOMEN AND THOSE AGED OVER 45

Women are more likely than men to be disappointed by today's mobile apps and services in terms of both privacy and security, i.e. there is a more significant gap between what is important to them and what they perceive is offered. Smartphone users aged over 45 are also more likely than younger cohorts to find that apps and services fall short, while income appears to be much less differentiating factor.

GAP BETWEEN IMPORTANCE AND PERCEIVED PERFORMANCE

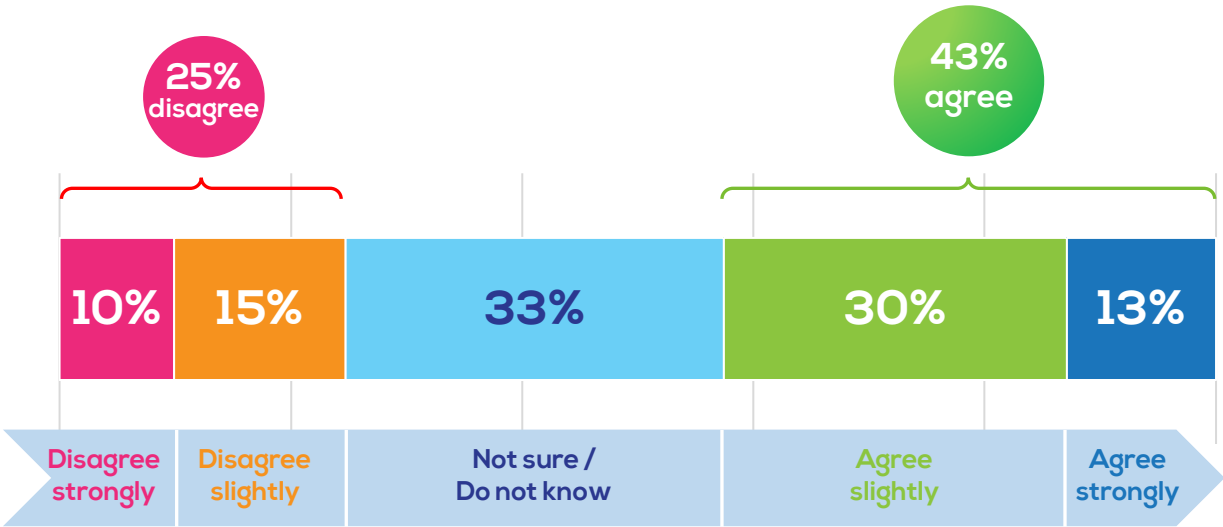
		"MOBILE APPS AND SERVICES RESPECT MY PRIVACY"	"BEING IN CONTROL OF HOW MY DATA IS USED"	"UNDERSTANDING HOW MY DATA IS USED"	"MOBILE APPS AND SERVICES KEEP MY DATA SECURE"
	N=3243	23pt	20pt	16pt	22pt
	N=3048	34pt	29pt	24pt	32pt
16-24	N=2223	23pt	17pt	13pt	19pt
25-34	N=2338	28pt	25pt	21pt	28pt
35-44	N=1151	31pt	30pt	24pt	29pt
45-54	N=551	39pt	32pt	33pt	37pt
55+	N=237	38pt	33pt	32pt	40pt
\$	Low income N=2052	26pt	20pt	18pt	24pt
\$ \$	Medium income N=2026	29pt	26pt	21pt	28pt
\$ \$ \$	High income N=1867	28pt	26pt	21pt	28pt

Bases indicated in table. Gap = 'Extremely or very important' minus 'Agree strongly or slightly'
Importance question: To what extent do you agree with the following statements? Scale from 'Not at all important' to 'Extremely important'
Performance question: To what extent do you agree with the following statements? Scale from 'Disagree strongly' to 'Agree strongly'

MANY BELIEVE TRADING THEIR DATA IS A GOOD DEAL – BUT OVER HALF STILL NEED TO BE CONVINCED

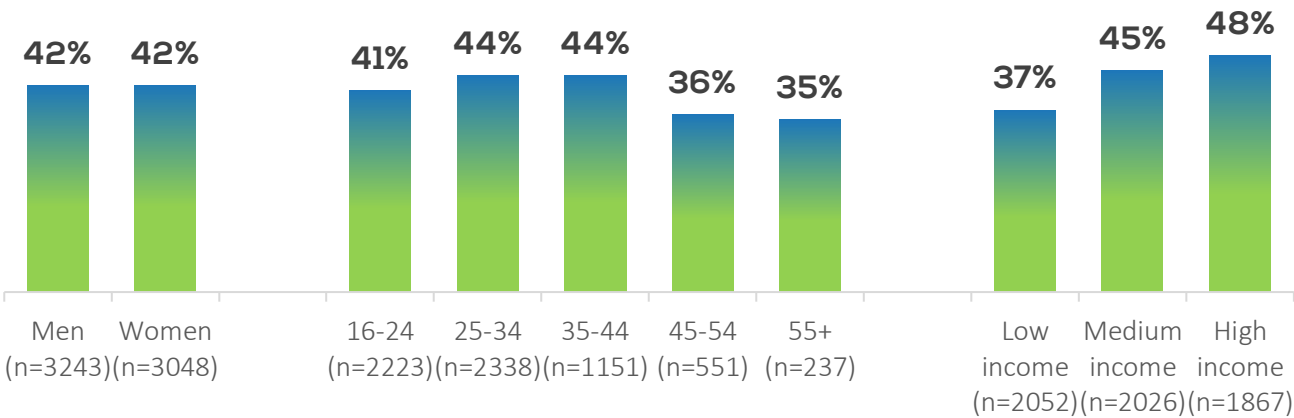
Why do users accept the deficit on personal data and security? Some believe that they do get a fair exchange. Over 2 in 5 smartphone users agree that they get valuable services in return for sharing their data with apps and services, with the proportion stronger among younger cohorts and those on higher incomes. However, there is a spread of views: 1 in 3 are unsure that the services they access in return for their data are valuable, while 1 in 4 is clear that the deal is imbalanced.

“I SHARE MY PERSONAL DATA ONLINE BUT I DO GET VALUABLE SERVICES IN RETURN” AGREEMENT SCALE



Base: All respondents, n=6,500

PROPORTION WHO AGREE: GET VALUABLE SERVICES IN RETURN DEMOGRAPHIC VIEW

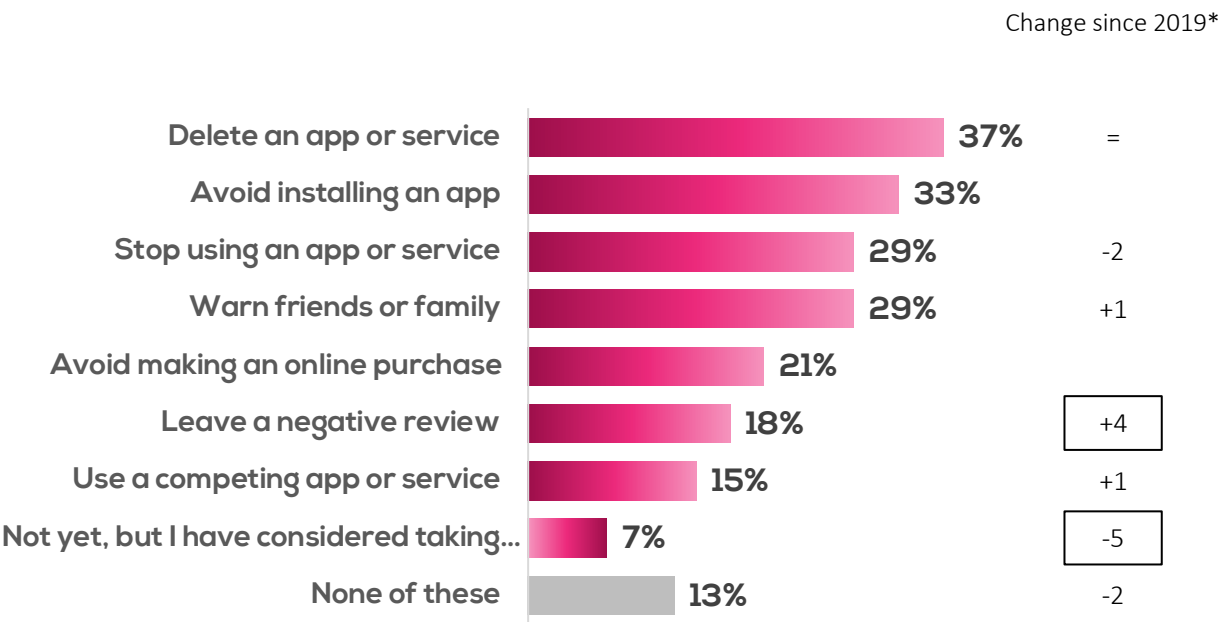


Bases indicated in chart

THE COST OF LOW TRUST: CONCERNED USERS ARE LIKELY TO DELETE OR AVOID APPS

Similar to findings in MEF’s previous studies, a significant proportion of smartphone users have deleted an app or service due to concerns over privacy and/or security. They are almost equally likely to have refrained from installing an app in the first place, suggesting that some form of reassurance is needed very early in the user journey.

IN THE PAST YEAR, HAVE CONCERNS OVER PRIVACY AND/OR SECURITY CAUSED YOU TO DO ANY OF THE FOLLOWING?



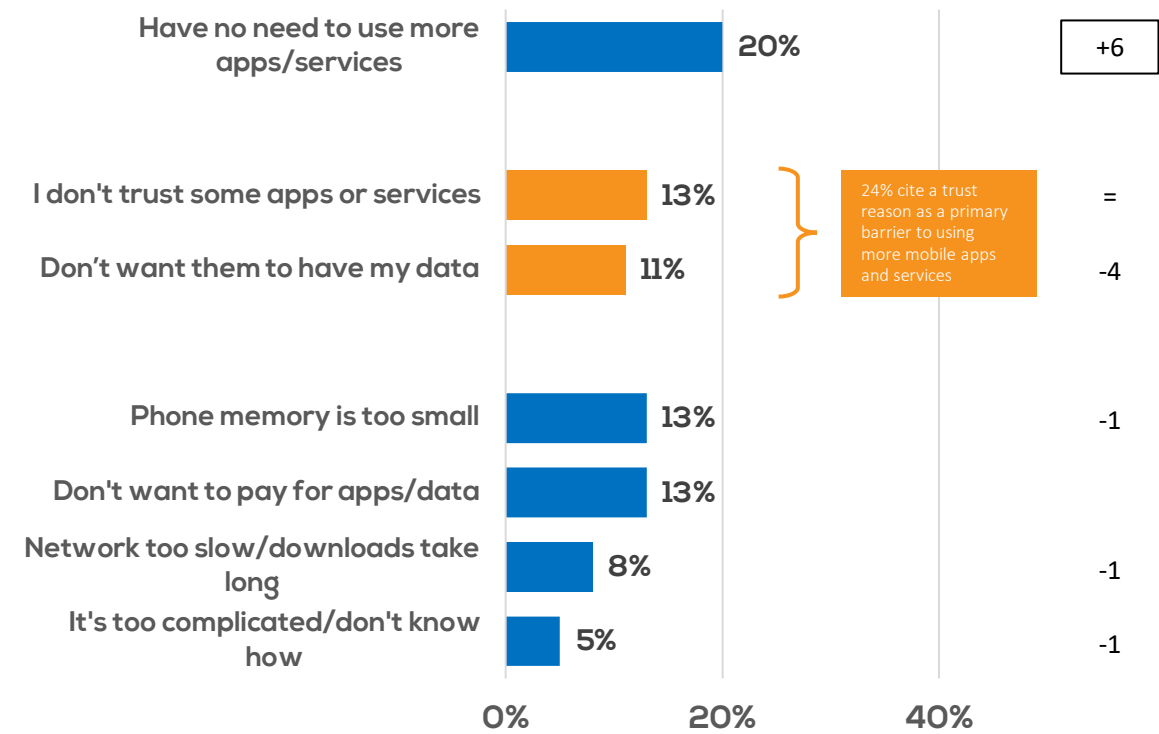
Base: All respondents, n=6,500 *Not all options were available for selection in the previous study

APP SATURATION: AN INCREASING NUMBER SAY THEY HAVE NO NEED FOR MORE APPS

The most common reason for not using more mobile apps and services is ‘no need’, a proportion which has increased since 2019. 1 in 4 smartphone users cite trust as the key barrier, expressing this either as a general lack of trust or as concern over sharing personal data.

WHAT IS THE MAIN REASON YOU DON'T USE MORE APPS AND SERVICES?

Change since 2019*



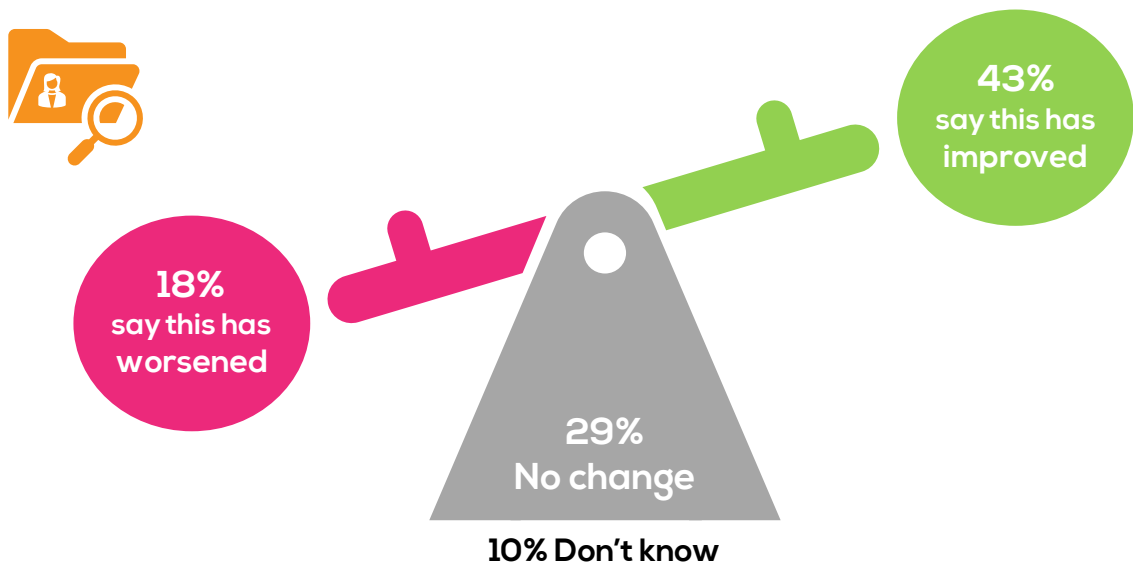
Base: All respondents, n=6,500 *Not all options were available for selection in the previous study

ENCOURAGING, MANY BELIVE THAT PRIVACY OPTIONS ARE IMPROVING

Over 2 in 5 smartphone users believe that options to keep their personal data private have improved during the past year. However, there is an opportunity for this to be felt by more users, since some do not perceive any change and a minority believe the situation has in fact worsened.

PRIVACY: OPTIONS TO KEEP PERSONAL DATA PRIVATE WHILE ON THE INTERNET

IMPROVED VS WORSENERD



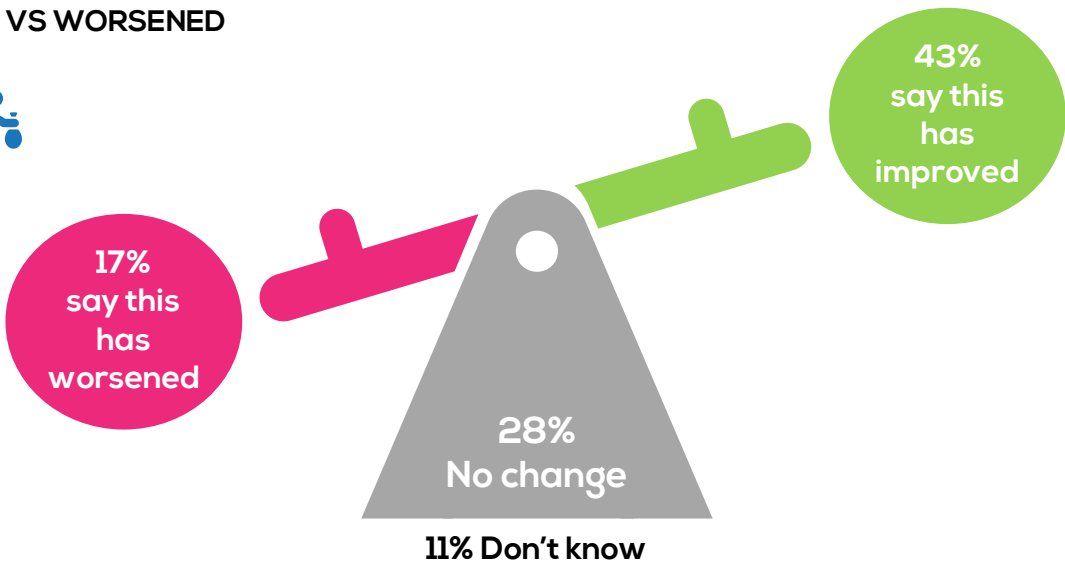
Base: All respondents, n=6,500

MANY ALSO BELIEVE THE THREAT OF FINANCIAL FRAUD OR MALWARE/VIRUSES HAS REDUCED

Similarly, over 2 in 5 smartphone users believe that security from financial fraud, and protection from malware and viruses, have improved during the past year. As with privacy perceptions, there remains an opportunity to extend this positive momentum.

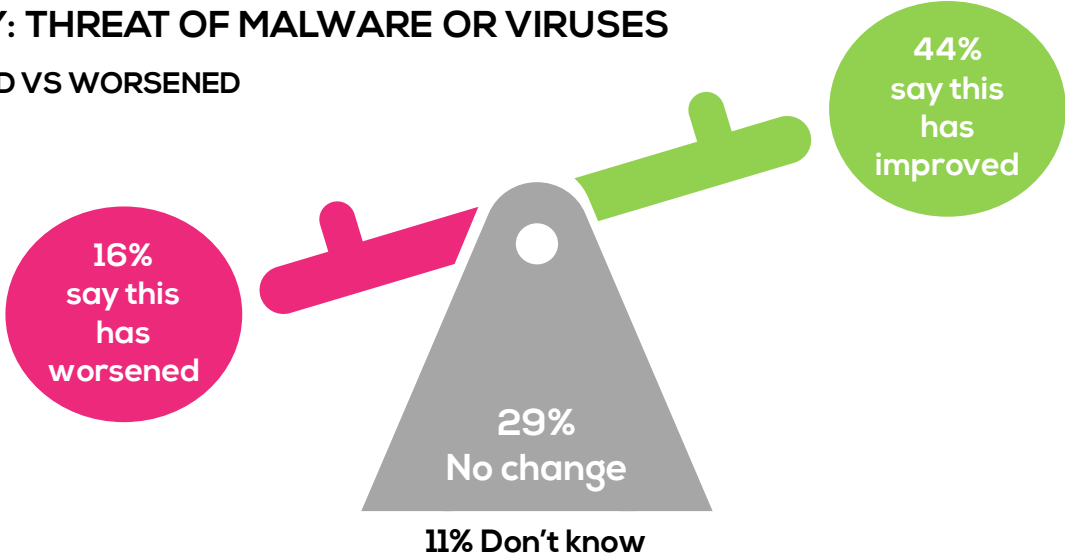
SECURITY: FINANCIAL FRAUD ON INTERNET

IMPROVED VS WORSENERD



SAFETY: THREAT OF MALWARE OR VIRUSES

IMPROVED VS WORSENERD

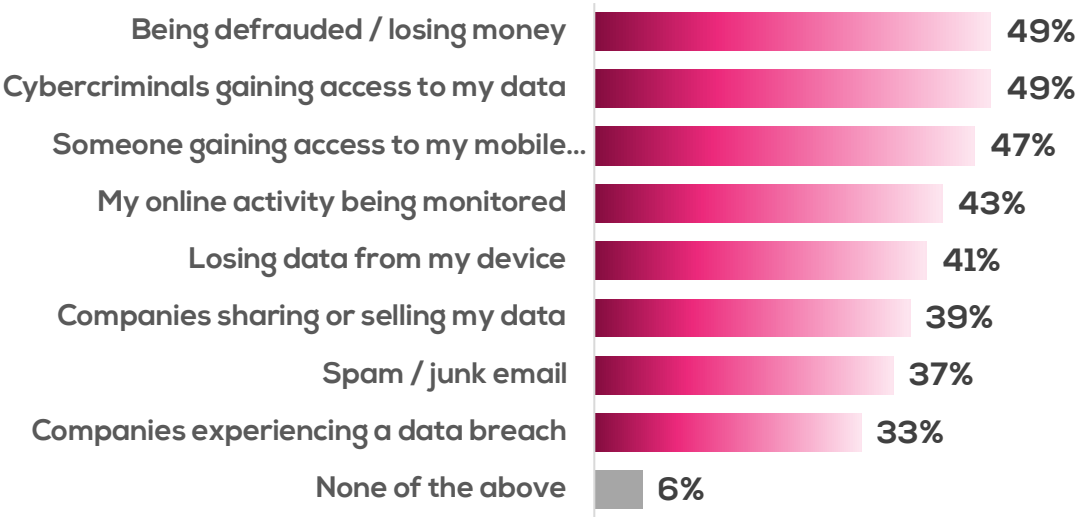


Base: All respondents, n=6,500

WHEN IT COMES TO SECURITY, EXPOSURE TO CRIMINAL ACTIVITY IS THE BIGGEST CONCERN

The most commonly cited security concerns are those perceived to have the most damaging consequences, namely being defrauded or cybercriminals gaining access to data. While issues such as spam/junk email may be an annoyance, they are perceived as less of a risk.

WHICH RISKS CONCERN YOU?



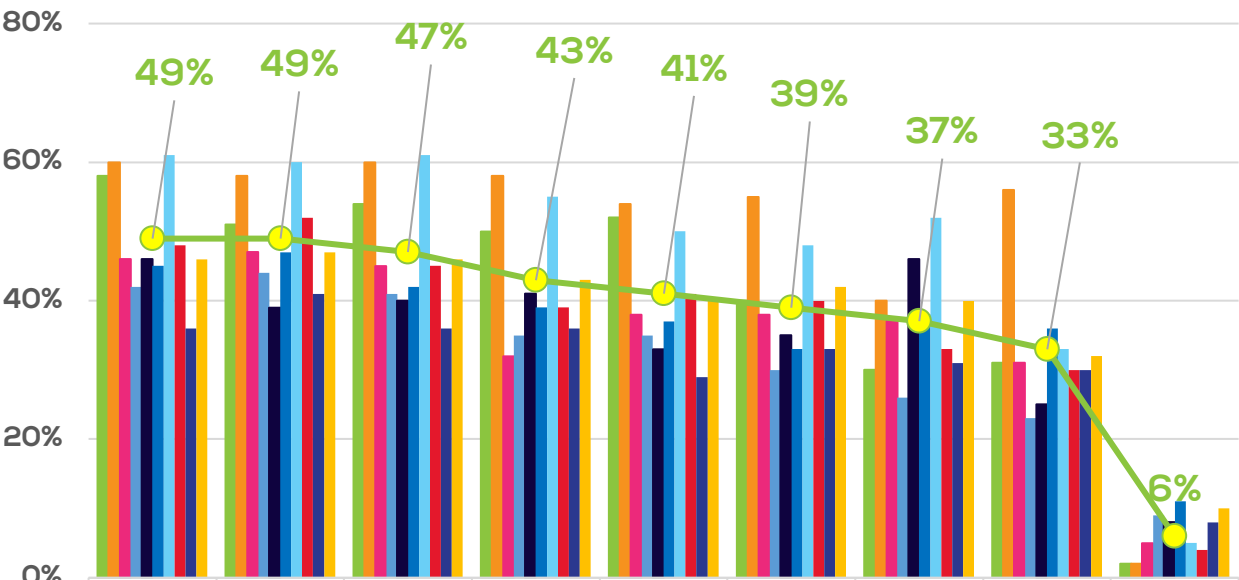
Base: All respondents, n=6,500

SEVERAL RISKS ARE MORE TOP OF MIND IN CHINA, SOUTH AFRICA AND BRAZIL

Overall, risks are more likely to be top of mind in China, South Africa and Brazil, including serious cybercrime.

In China there is also a particularly high level of concern about companies experiencing a data breach, while South Africa and India report higher than average concern about junk email.

WHICH RISKS CONCERN YOU? MARKET VIEW



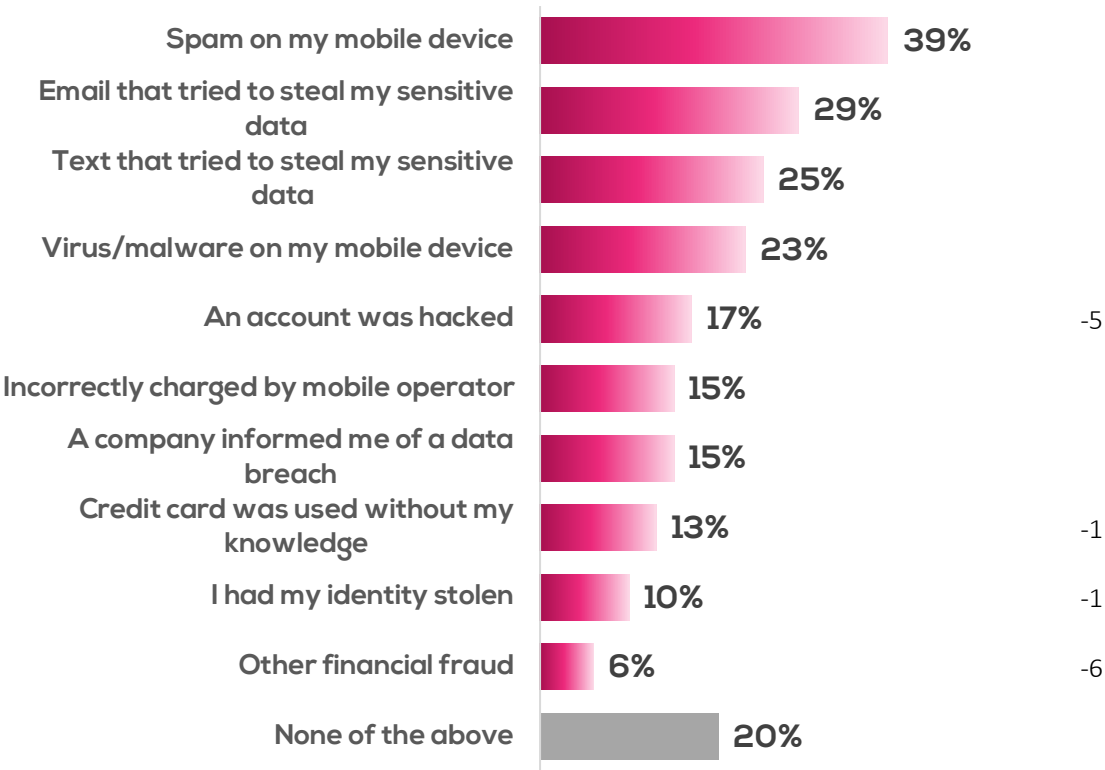
Base: n=650 per market, total 6,500

4 IN 5 HAVE EXPERIENCED SOME FORM OF ACTUAL OR ATTEMPTED DATA HARM

The most common ‘data harm’ is mobile spam, followed by phishing emails and texts (smishing). Overall, 4 in 5 smartphone users have experienced an issue, at similar levels to previous studies, however a slight decline is observed for account hacking and ‘other’ financial fraud.

HAVE YOU EVER EXPERIENCED ANY OF THE FOLLOWING?

Change since 2018*



Base: All respondents, n=6,500
*Not all options were available for selection in previous studies. Indicative comparisons only – 2018 study included 2 different markets (out of 10)

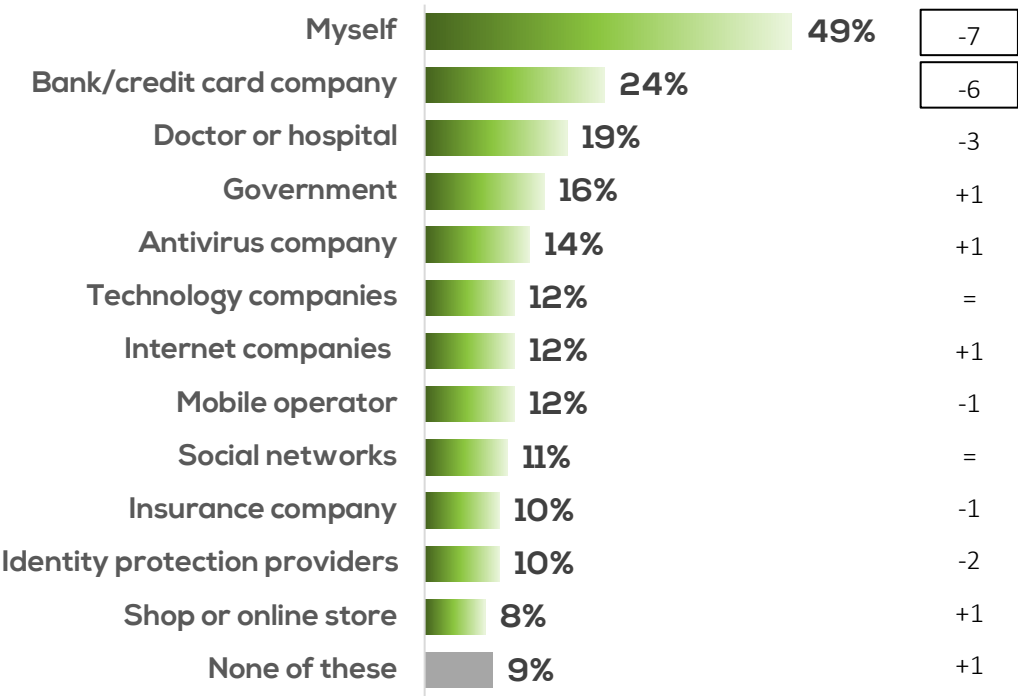


USERS STILL DO NOT TRUST OTHERS TO MANAGE DATA FOR THEM

Smartphone users are far more likely to trust themselves to manage their data, than any external organisation. While the proportion selecting ‘myself’ has declined since 2019, it remains by far the most popular response. Companies specialising in antivirus or identity protection services are no more likely to be trusted than in previous waves.

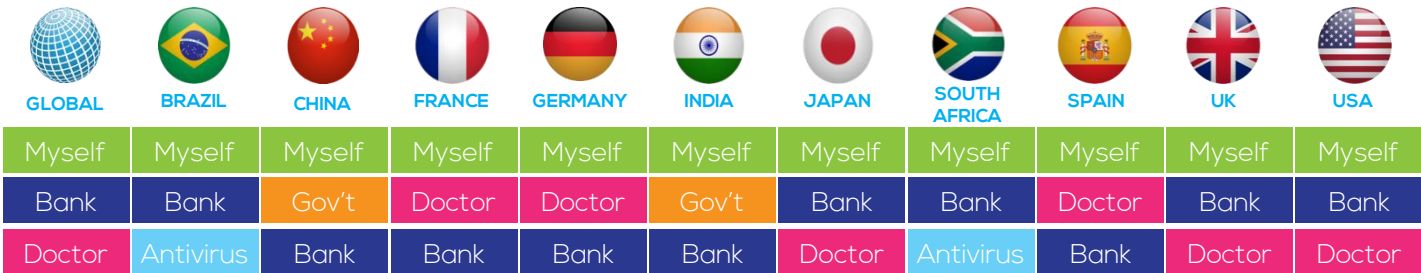
WHEN IT COMES TO YOUR PERSONAL DATA, WHO WOULD YOU TRUST TO MANAGE IT? (MAX 3)

Change since 2019



Base: All respondents, n=6,500

TOP 3 BY MARKET



Base: n=650 per market, total 6,500

LARGE MAJORITY OF SMARTPHONE USERS TAKE ACTION TO PROTECT THEMSELVES

The proportion of smartphone users taking preventative action has consolidated in 2021, rising further to 84% following a significant increase between 2018 and 2019. A full breakdown of actions taken is shown on pages [28-29](#): the most common individual actions are changing privacy settings, cookie management, enabling multi-factor authentication or private browsing, and installing antivirus or anti-malware software.

PROPORTION WHO HAVE TAKEN ONE OR MORE PREVENTATIVE ACTIONS E.G. CHANGING SETTINGS, INSTALLING ANTI-VIRUS SOFTWARE ETC



NETS OF TYPES OF ACTION TAKEN % WHO DID ONE OR MORE ACTION WITHIN EACH GROUP

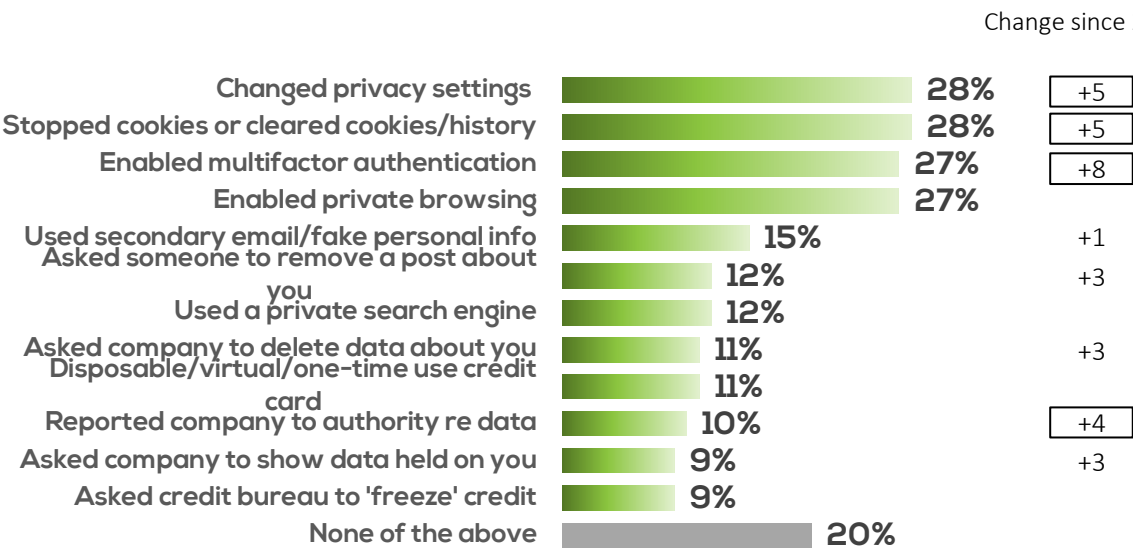
- 53%**
Managed settings
Changed privacy settings for apps and services, enabled multifactor authentication or set browser to stop cookies/history.
- 50%**
Masked ID or activity
Signed up to a service using a secondary/fake email address, used a disposable, virtual or one-time use credit card, contacted a credit bureau to 'freeze' credit, enabled private browsing or used a private search engine.
- 30%**
Reviewed/ reported
Reported company/organisation to authority, asked someone to remove something posted about you, asked company/organisation to delete data on you, asked a company/organisation to provide a record of data held.
- 72%**
Used other tools
Anti-virus/malware, VPN, adblocker/tracker blocker, cloud data backup, password manager, took a class, phone or email aliasing/masking service, credit monitoring, info management/data store, data removal service, ID insurance, darknet monitoring

Base: All respondents, n=6,500

MORE USERS ARE CHANGING THEIR PRIVACY AND COOKIE SETTINGS THAN IN THE PAST

A large majority of smartphone users have taken at least one of the listed actions to protect their data, most commonly changing their privacy and cookie settings. There have been increases in some areas including managing settings and the enabling of multifactor authentication. In China, a larger proportion of smartphone users have taken actions related to privacy settings or masking their identity – around two thirds have taken these actions compared to half globally (see page [31](#)).

ACTIONS TAKEN IN PAST YEAR TO PROTECT PERSONAL DATA: MANAGING SETTINGS / MASKING ID / REPORTING OR REVIEWING

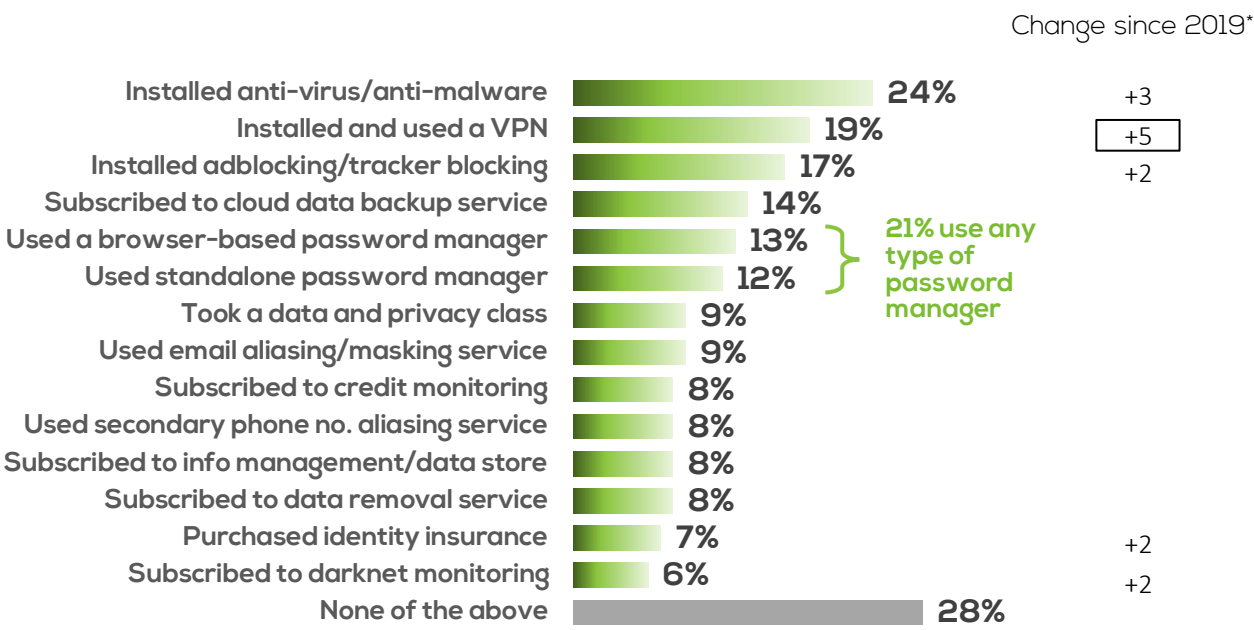


Base: All respondents, n=6,500 *Not all options were available for selection in the previous study

MOST COMMON TOOLS: ANTIVIRUS, VPN ADBLOCKING

The most common other tool/service used is anti-virus or anti-malware software, the prevalence of which has increased slightly since 2019. While small increases are also observed in other areas, less than a quarter engage in any individual activity, suggesting that protection may not be comprehensive for many smartphone users.

TOOLS AND SERVICES INSTALLED AND USED IN PAST YEAR

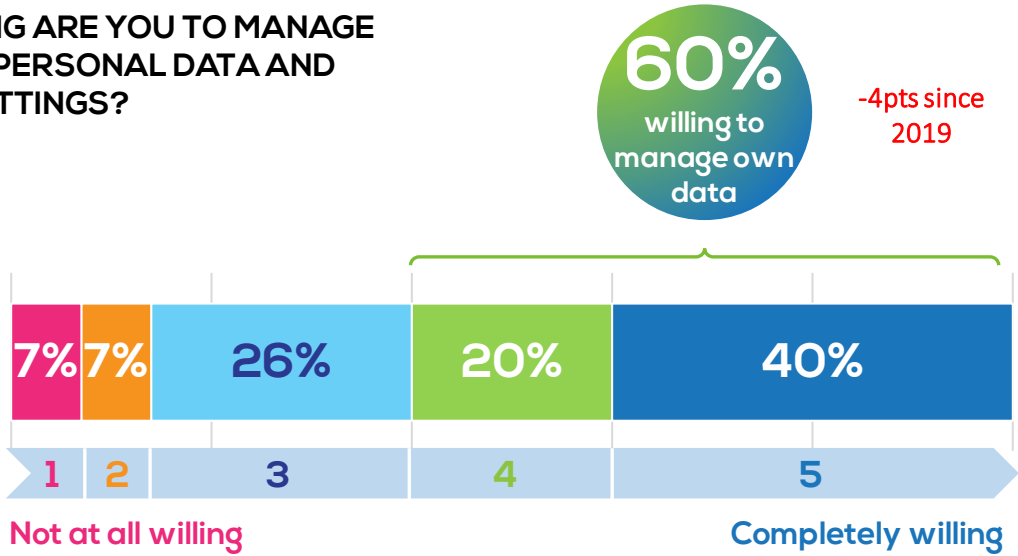


Base: All respondents, n=6,500 *Not all options were available for selection in the previous study

LARGE APPETITE TO MANAGE OWN DATA, BUT WANING

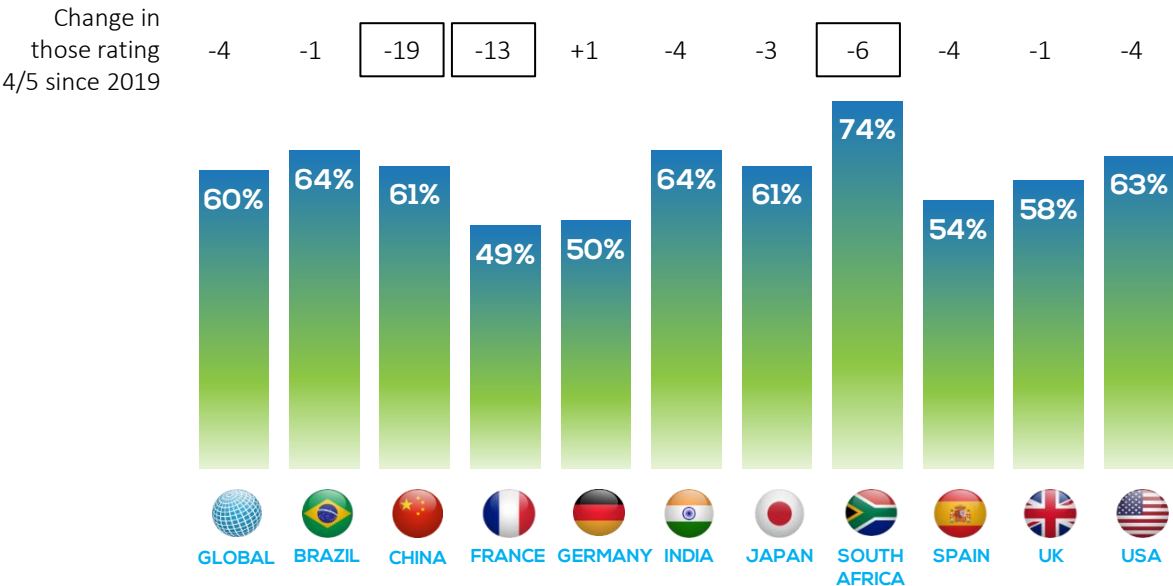
While the majority continue to claim they are willing to manage their own data, there is a decline in willingness in some markets, which is most marked in China and France.

HOW WILLING ARE YOU TO MANAGE YOUR OWN PERSONAL DATA AND PRIVACY SETTINGS?



Base: All respondents, n=6,500

THOSE 'WILLING' MARKET VIEW



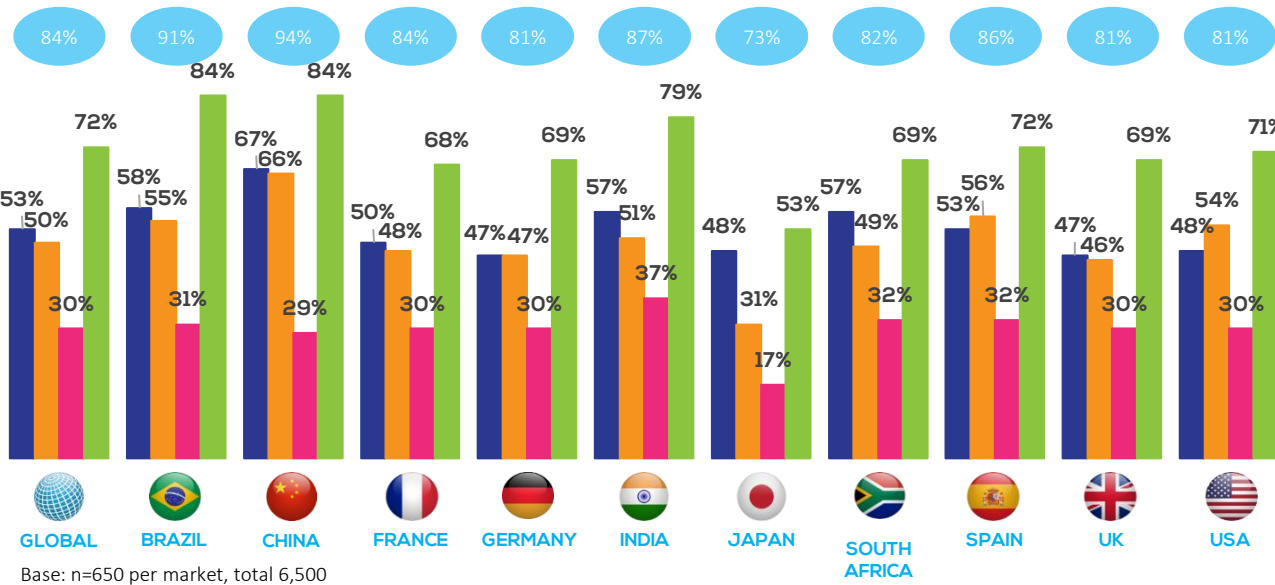
Base: n=650 per market, total 6,500

YOUNGER AND MORE AFFLUENT USERS TAKE MORE PROTECTIVE ACTIONS

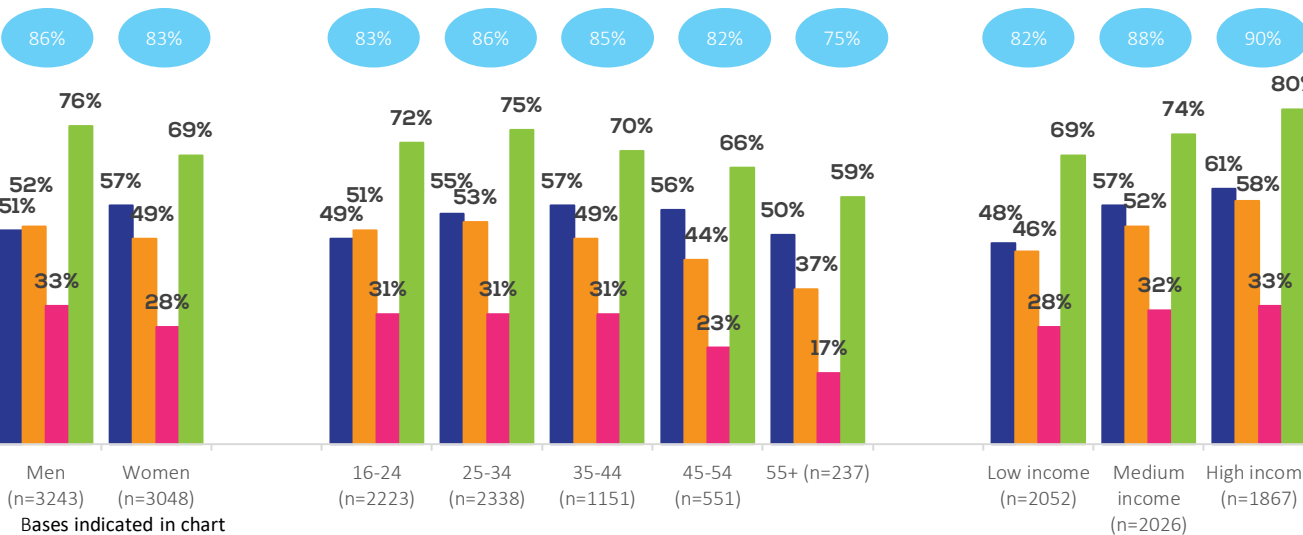
Smartphone users in China are the most likely to have taken all types of protective action, followed by Brazil. From a demographic perspective, younger and more affluent users tend to take more protective actions, despite the fact that older users have the greatest expectation 'gap' in the area of security and privacy (see page 16).



ACTIONS TAKEN MARKET VIEW



ACTIONS TAKEN DEMOGRAPHIC VIEW



USERS FEEL SAFER FOR TAKING SOME FORM OF ACTION, BUT FEW FEEL FULLY PROTECTED

Among those who have taken action to protect their data, the most common impact is to feel 'slightly safer'. Around 1 in 4 feel 'a lot safer', with the remainder unclear that they are more protected than previously.

TO WHAT EXTENT DO ACTIONS YOU HAVE TAKEN MAKE YOU FEEL SAFER WITH RESPECT TO THE SECURITY AND PRIVACY OF YOUR DATA?

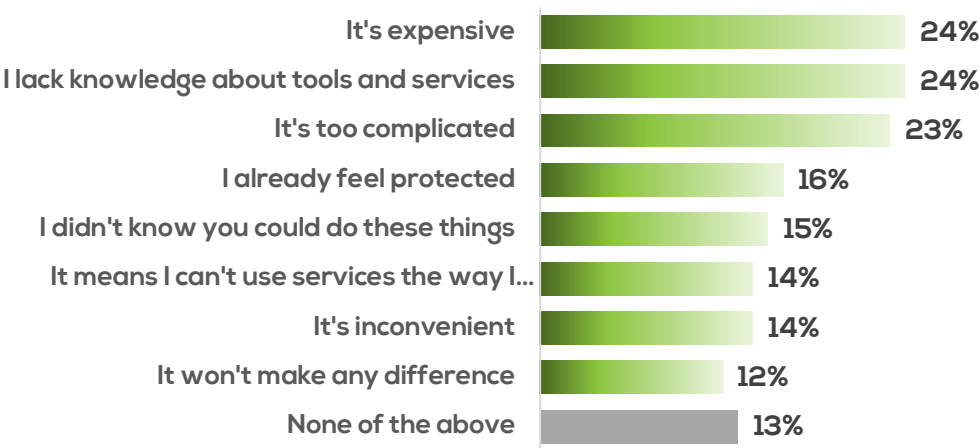


Base: All respondents who took action to protect personal data, n=5,465

EXPENSE, LACK OF KNOWLEDGE AND COMPLEXITY DETER USERS FROM TAKING PROTECTIVE ACTION

The most common barriers to taking further protective action are the perceived expense, and a lack of knowledge about the tools and services that are available and appropriate to them.

WHAT PREVENTS YOU FROM TAKING ADDITIONAL ACTION TO PROTECT YOUR PERSONAL DATA AND IDENTITY?

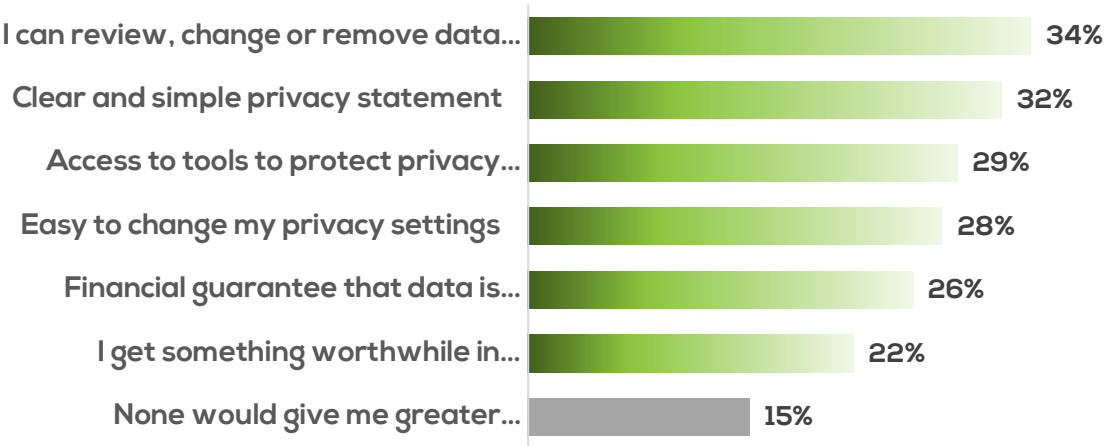


Base: All respondents, n=6,500

IN ORDER TO FEEL MORE CONFIDENT ABOUT SHARING DATA, USERS REQUIRE TRANSPARENCY AND CONTROL

To increase user confidence when sharing personal data with mobile apps and services, the top requirement is transparency and control over what data is stored. However, there appears to be no silver bullet, with relatively little difference in absolute mentions for each prompted option.

SELECT UP TO 3 FACTORS WHICH WOULD GIVE YOU GREATER CONFIDENCE WHEN SHARING PERSONAL DATA WITH A MOBILE APP OR SERVICE



Base: All respondents, n=6,500



INTRODUCTION TO THE SEGMENTATION AND CRITICAL TAKEAWAYS

INTRODUCTION

For the first time, this year's study quantifies user "segments" based on attitudes and perceived efficacy of actions taken in the area of privacy and security. Respondents were asked to self-identify with one of the following statements (labels were not shown):

- There is no need for me to take any action to protect my personal data ["Unaware"]
- I take few actions to protect my personal data, because it takes time, and the benefit is unclear ["Indifferent"]
- I take few actions to protect my personal data, because I feel overwhelmed and don't know where to start ["Helpless"]
- I take a number of actions to protect my personal data, but I still feel at risk ["Impaired"]
- I take a number of actions to protect my personal data, and these mitigate my risk to a reasonable extent ["Empowered"]
- Taking steps to protect my personal data is a priority and I am confident that the actions I take are as comprehensive as they can be ["Self-assured"]

Segmenting smartphone users in this way provides an additional lens through which to understand and address target users. In the subsequent pages we outline key segment characteristics, but below are some high-level take-aways.

CRITICAL TAKEAWAYS

1

The Impaired and Empowered segments appear most open to considering data protection services and tools, and should be a priority for marketing and product development. These segments understand the need to act and appreciate the ever-evolving risk environment.

2

Those in the Helpless segment are key to address due to their above average smartphone activity, but require guidance and hand-holding in order to protect themselves. Their negative emotion and confusion surrounding where to start must be acknowledged.

3

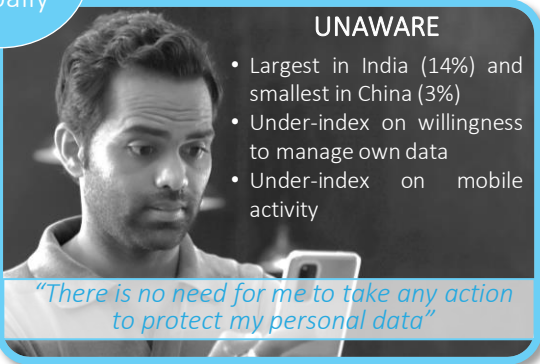
Those classifying as Self-assured are emotionally content but may in fact have significant gaps in protection. The challenge is to speak to their confidence while further educating on beneficial protective steps.

4

The Unaware and Indifferent segments have yet to be convinced of the need to protect themselves. As less active smartphone users, it is likely to be more challenging to engage with them, and return on investment may be lower than for other segments.

SEGMENT OVERVIEW

8%
globally



UNAWARE

- Largest in India (14%) and smallest in China (3%)
- Under-index on willingness to manage own data
- Under-index on mobile activity

"There is no need for me to take any action to protect my personal data"

24%
globally

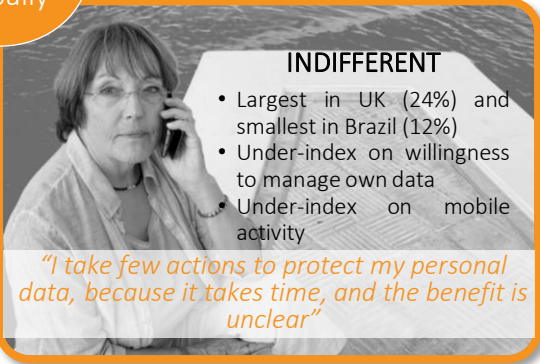


IMPAIRED

- Largest in China (40%) and smallest in India (16%)
- Over-index on willingness to manage own data
- Over-index on mobile activity

"I take a number of actions to protect my personal data, but I still feel at risk"

19%
globally



INDIFFERENT

- Largest in UK (24%) and smallest in Brazil (12%)
- Under-index on willingness to manage own data
- Under-index on mobile activity

"I take few actions to protect my personal data, because it takes time, and the benefit is unclear"

17%
globally



SELF ASSURED

- Largest in India & South Africa (24%); smallest in France (11%)
- Over-index on willingness to manage own data
- Slightly under-index on mobile activity

"Taking steps to protect my personal data is a priority and I am confident that the actions I take are as comprehensive as they can be"

17%
globally



HELPLESS

- Largest in Spain & UK (22%); smallest in Japan & China (10%)
- Under-index on willingness to manage own data
- Slightly over-index on mobile activity

"I take few actions to protect my personal data, because I feel overwhelmed and don't know where to start."

15%
globally



EMPOWERED

- Largest in Japan (23%); smallest in India & USA (12%)
- Over-index on willingness to manage own data
- Over-index on mobile activity

"I take a number of actions to protect my personal data, and these mitigate my risk to a reasonable extent"

KEY SEGMENT INSIGHTS AND OPPORTUNITIES

SEGMENT
INSIGHTS

OPPORTUNITY

UNAWARE 8%	IMPAIRED 24%
Less active smartphone users and taking fewer protective actions, this segment also has the lowest income.	Very active users, making efforts to protect data but still concerned. Higher than average income.
Deprioritise active communications. Laggards with lower mobile activity: will follow the market	Communicate on efficacy and highlight gaps in protection.

SEGMENT
INSIGHTS

OPPORTUNITY

INDIFFERENT 19%	SELF-ASSURED 17%
Lower than average smartphone activity and unconvinced about the efficacy of protective actions.	Confident, having experienced less data harm than others, but less likely to take protective steps.
Demonstrate the benefit of acting. They do not see a clear value trade-off. Need for a fast pay-off.	Leverage their confidence and engagement to educate on beneficial protective actions.

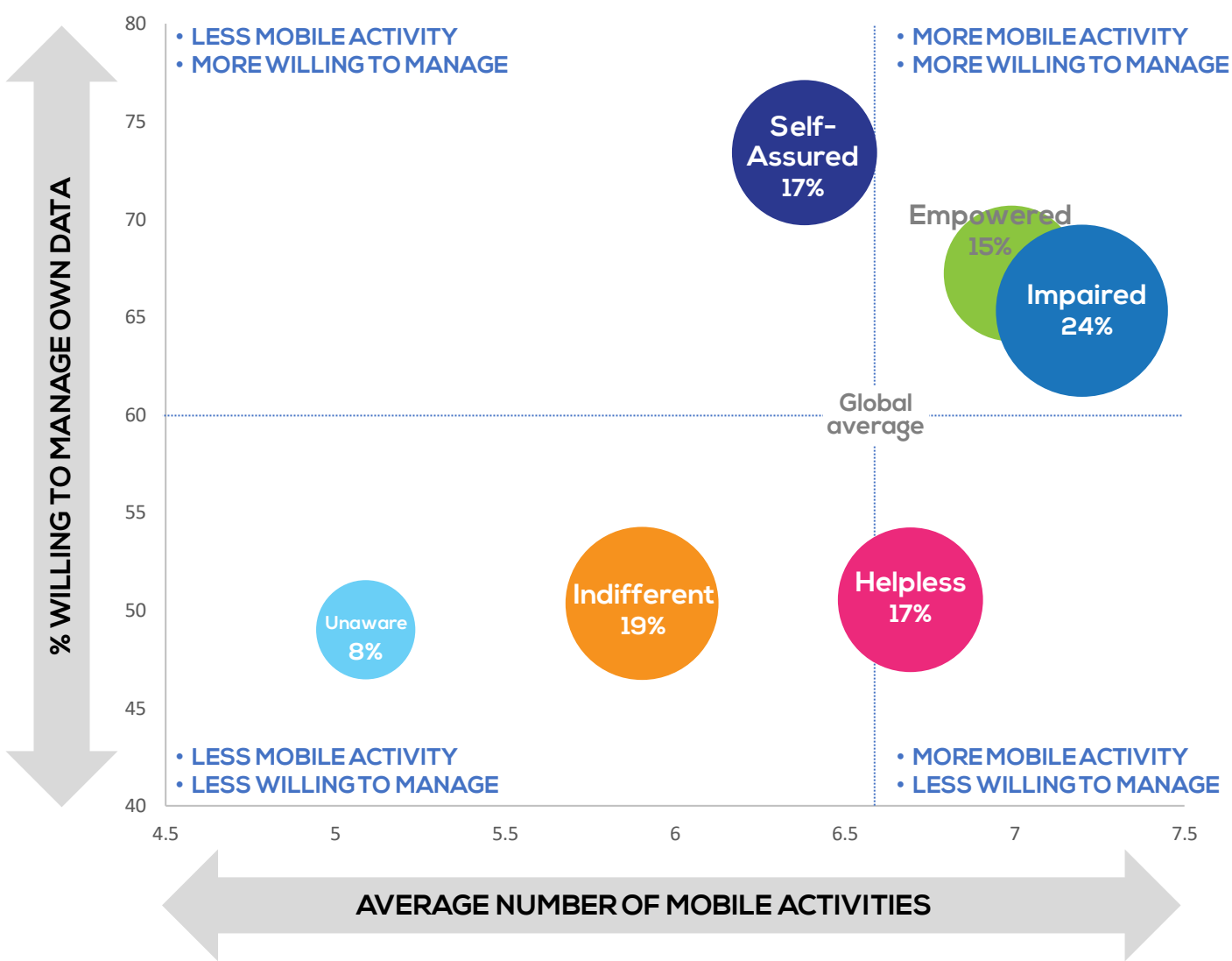
SEGMENT
INSIGHTS

OPPORTUNITY

HELPLESS 17%	EMPOWERED 15%
Active smartphone users, commonly experiencing data harm and at a loss on how to be protected.	Very active users, feeling more confident due to protective actions. Slightly higher than average income.
Show them where to begin. Be a trusted and reassuring voice with simple steps to empower.	Address in a similar way to the Impaired; opportunity to provide more holistic data management tools.

2 MAIN FACTORS: MOTIVATION TO ENGAGE IN DATA MANAGEMENT AND LEVEL OF MOBILE ACTIVITY

The segments can be mapped along two key axes – how motivated they are to manage their own data, and how active they are on their mobile in general. Depending on where segments are positioned on the map, different communication and product strategies may be appropriate to consider, for example those segments less willing to manage their own data may require more education and emotional persuasion.



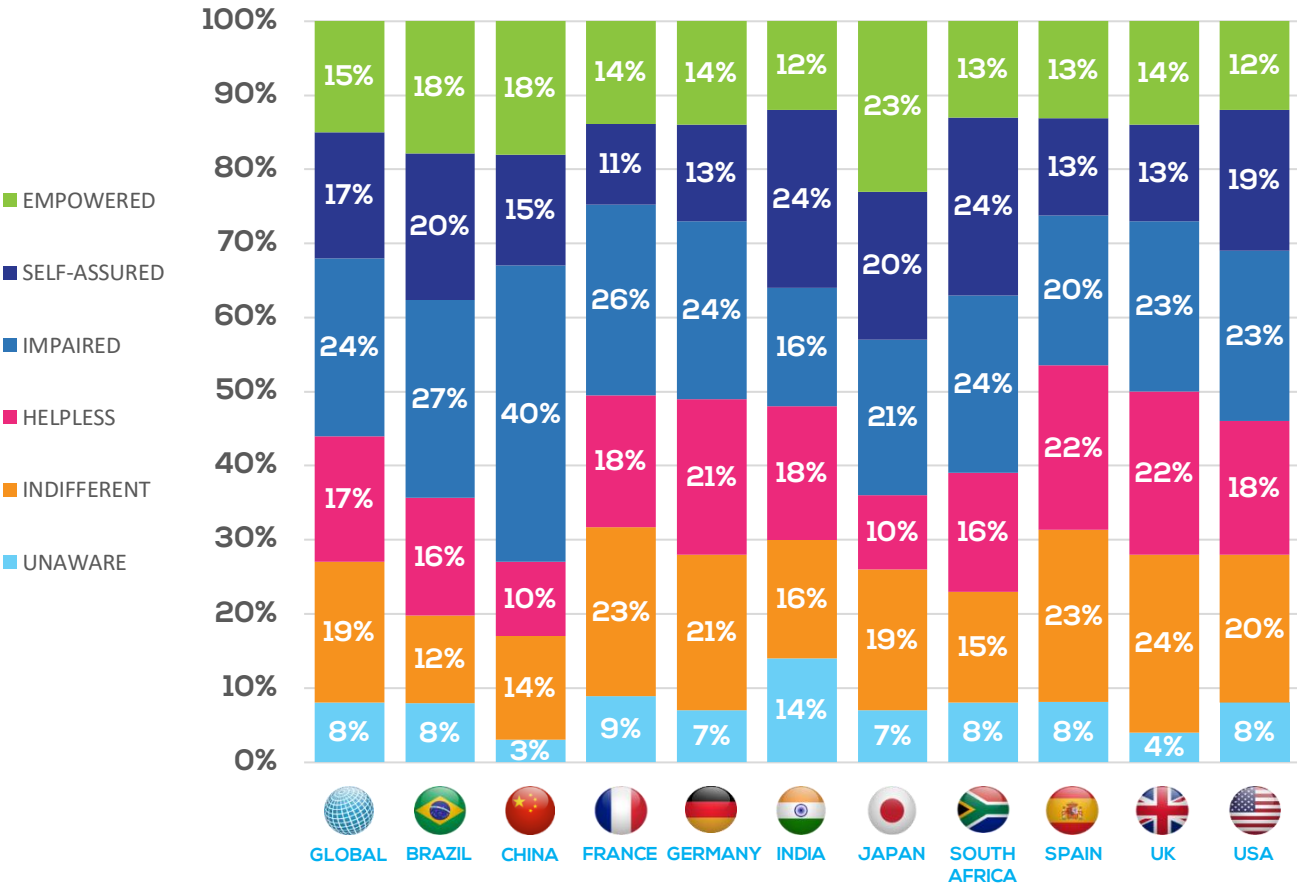
Base: All respondents self-identifying with each segment statement, for bases and full statements see page 36

“IMPAIRED” SEGMENT IS LARGEST GLOBALLY: THOSE WHO TAKE ACTION BUT STILL FEEL AT RISK

A broad spread of attitudes is present in every market, but the largest segment at a global level is the Impaired – those who consider themselves at risk despite making efforts to protect their personal data. This segment accounts for almost 1 in 4 smartphone users.

Users in China are considerably more likely to fall into the Impaired segment, at 40%. It is also noteworthy that the Self-Assured segment is larger in non-European markets – in particular India and South Africa where it is the largest or joint largest segment. This segment represents those who claim to prioritise taking protective action, however this confidence does not necessarily translate into behaviour as observed on page [45](#).

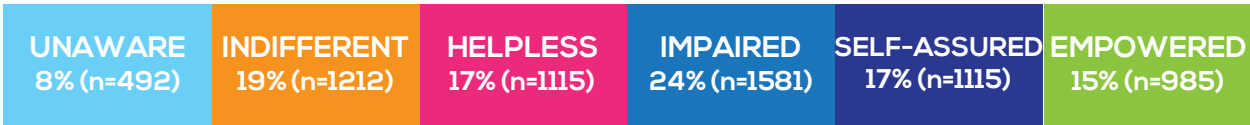
WHEN IT COMES TO YOUR DATA PRIVACY AND SECURITY, WHICH ONE OF THE FOLLOWING STATEMENTS DO YOU MOST AGREE WITH?* MARKET VIEW



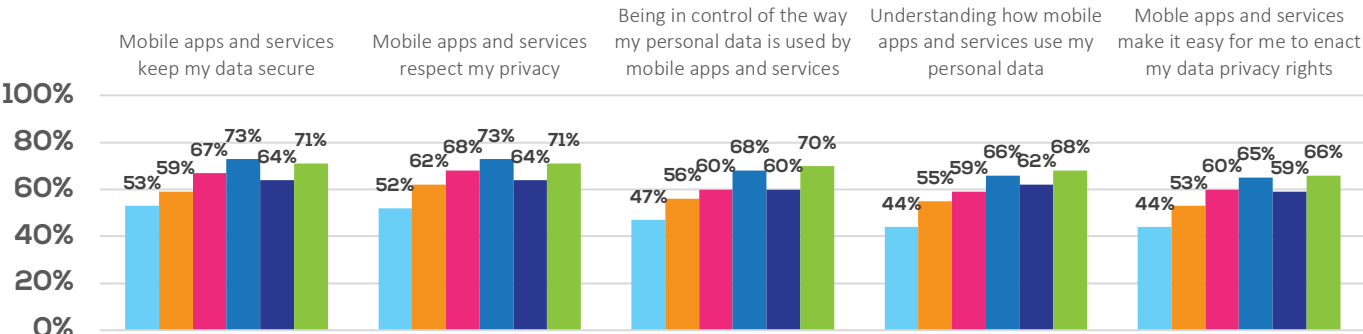
Base: n=650 per market, total 6,500 *For full statements see page [36](#)

"IMPAIRED" AND "EMPOWERED" SEGMENTS MOST CONCERNED BY PRIVACY AND SECURITY

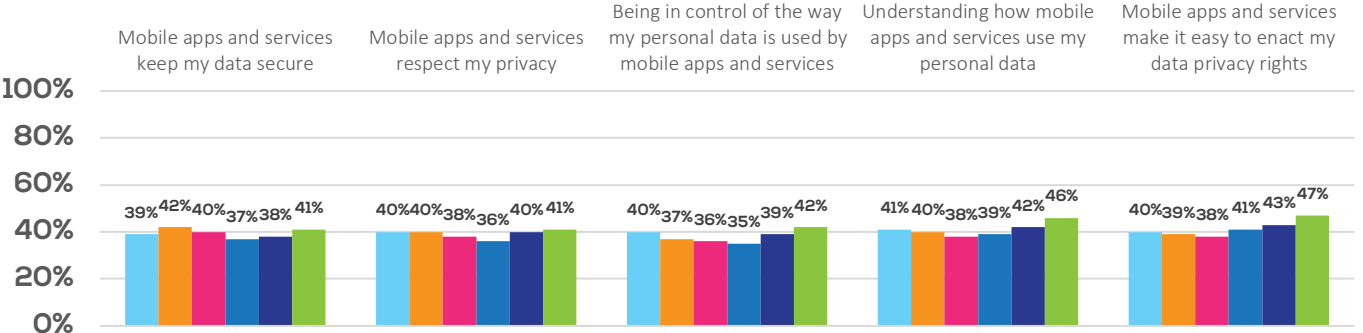
There is some variation between segments in terms of how important privacy and security are deemed to be. The Impaired and the Empowered are the most likely to rate all aspects as important, while those who are Unaware or Indifferent are somewhat less likely to do so. In contrast, there is consistency between segments in terms of how well they feel mobile apps and services currently meet these needs, at relatively lower levels.



RATE EACH ASPECT AS VERY OR EXTREMELY IMPORTANT



SLIGHTLY OR STRONGLY AGREE THAT NEEDS ARE MET



Base: All respondents self-identifying with each segment statement, bases indicated in legend. For full statements see page 36
Importance question: To what extent do you agree with the following statements? Scale from 'Not at all important' to 'Extremely important'
Performance question: To what extent do you agree with the following statements? Scale from 'Disagree strongly' to 'Agree strongly'

"HELPLESS" SEGMENT IS PARTICULARLY AT RISK FROM HARM BASED ON MOBILE USAGE AND ATTITUDES

The Impaired, Empowered and Helpless segments engage in the widest variety of mobile activity. Given that the Helpless claim to be deterred from protecting their data due to feeling overwhelmed, their relatively high level of mobile activity may put them at risk; indeed, they are the segment most likely to have experienced data harm (page 44).

WHICH OF THESE HAVE YOU DONE ON YOUR MOBILE DEVICE IN THE PAST SIX MONTHS?

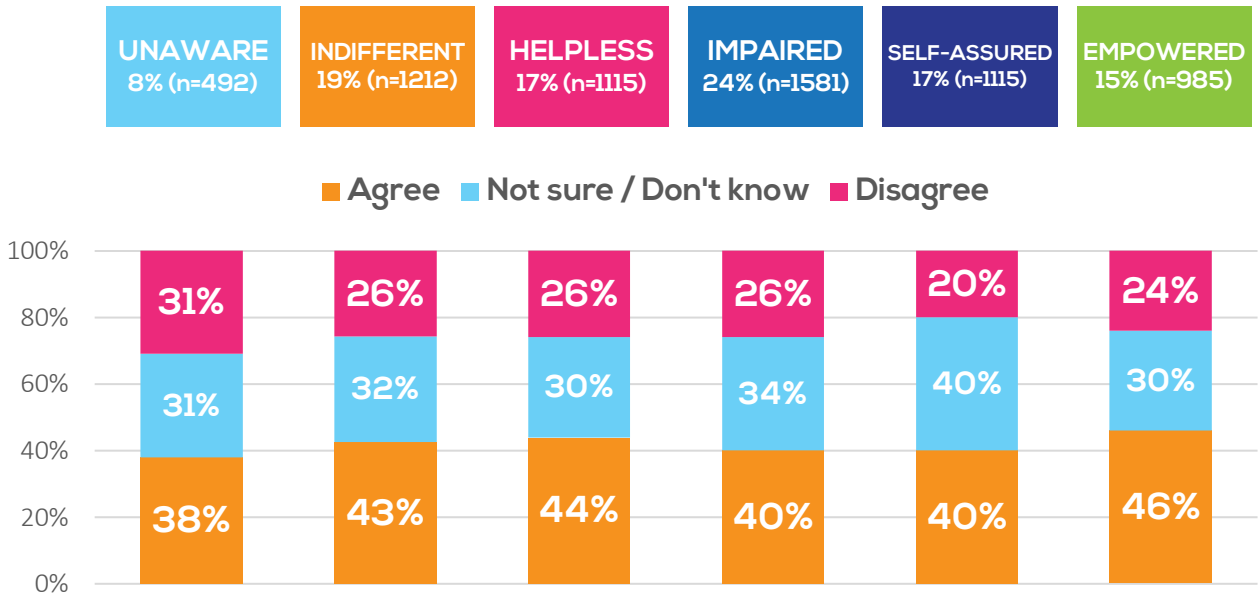


Base: All respondents self-identifying with each segment statement, bases indicated in legend. For full statements see page 36

“HELPLESS” AND “EMPOWERED” MOST LIKELY TO FEEL THEY GET VALUABLE SERVICES IN EXCHANGE FOR DATA

“I SHARE MY PERSONAL DATA ONLINE BUT I DO GET VALUABLE SERVICES IN RETURN”

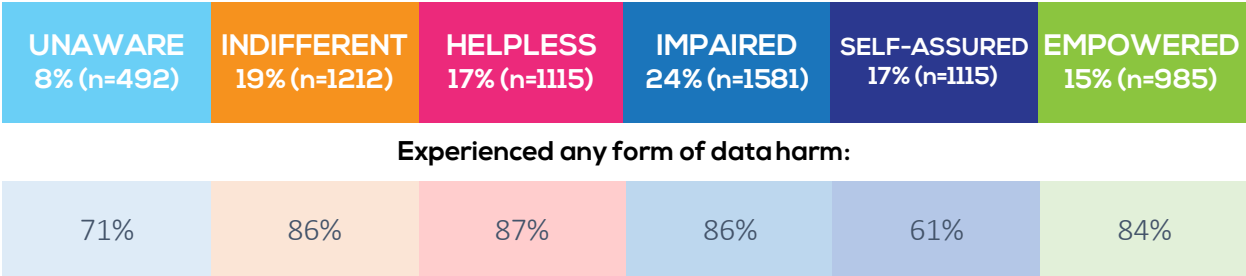
AGREEMENT SCALE



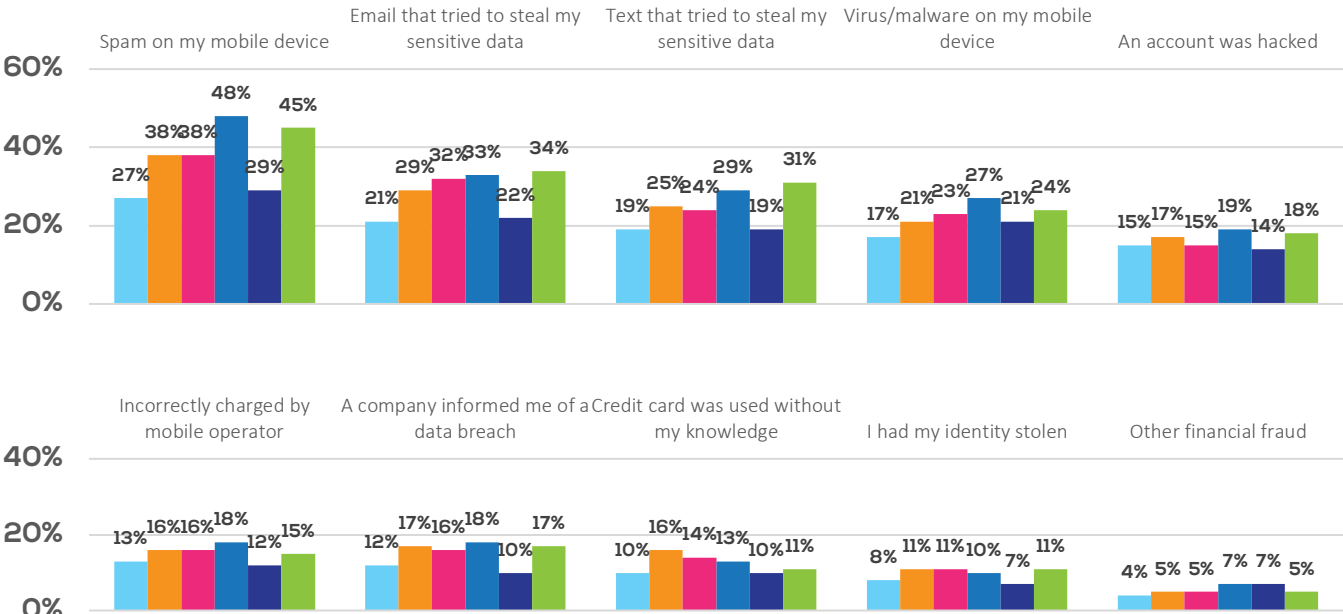
Base: All respondents self-identifying with each segment statement, bases indicated in legend. For full statements see [page 36](#)

NO SEGMENT IS UNTOUCHED BY DATA HARM BUT “SELF-ASSURED” CITE FEWEST PROBLEMS

Different segments claim to have had varying levels of exposure to data harm. The Self-Assured followed by the Unaware are the least likely to have experienced issues (61% and 71% respectively). While the Helpless are most likely to cite one or more issues overall (87% do so), there is no obvious spike for any individual issue, suggesting that they may be less able to recall or describe the specific problems experienced.



HAVE YOU EVER EXPERIENCED ANY OF THE FOLLOWING?



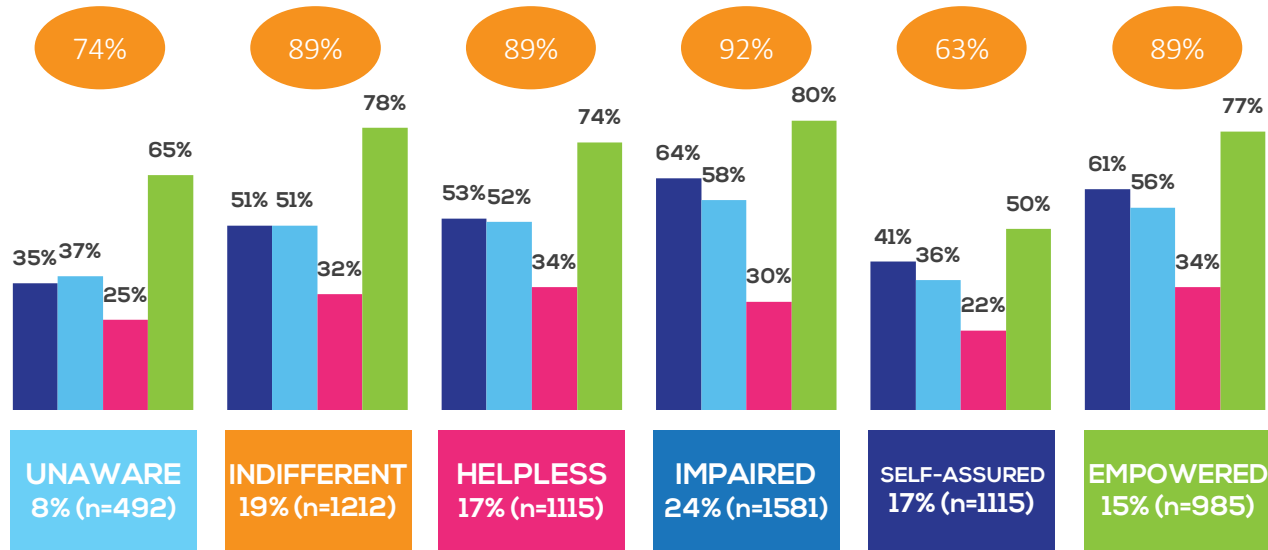
Base: All respondents self-identifying with each segment statement, bases indicated in legend. For full statements see page 36

"SELF-ASSURED" SEGMENT TAKES FEWEST PROTECTIVE ACTIONS YET MOST LIKELY TO FEEL SAFER

While the Self-Assured claim that taking steps to protect their personal data is a priority, in fact they take significantly fewer actions than other segments. They may feel they are taking actions that are particularly effective, since they are also the most likely segment to feel 'a lot safer' as a result of steps taken.

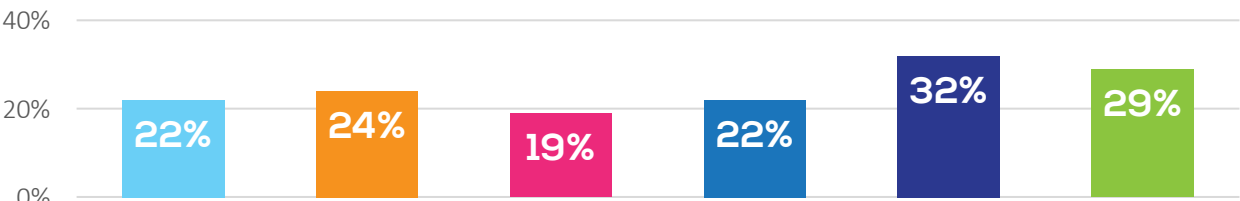


ACTIONS TAKEN



Base: All respondents self-identifying with each segment statement, bases indicated in legend. For full statements see page [36](#)

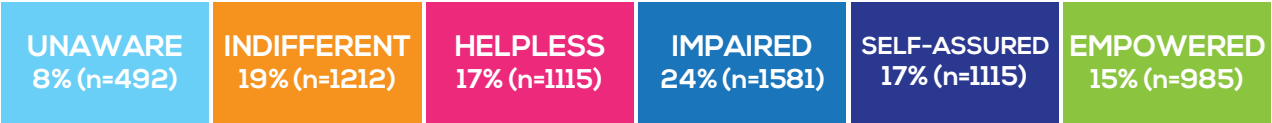
FEEL A 'A LOT SAFER' DUE TO ACTIONS



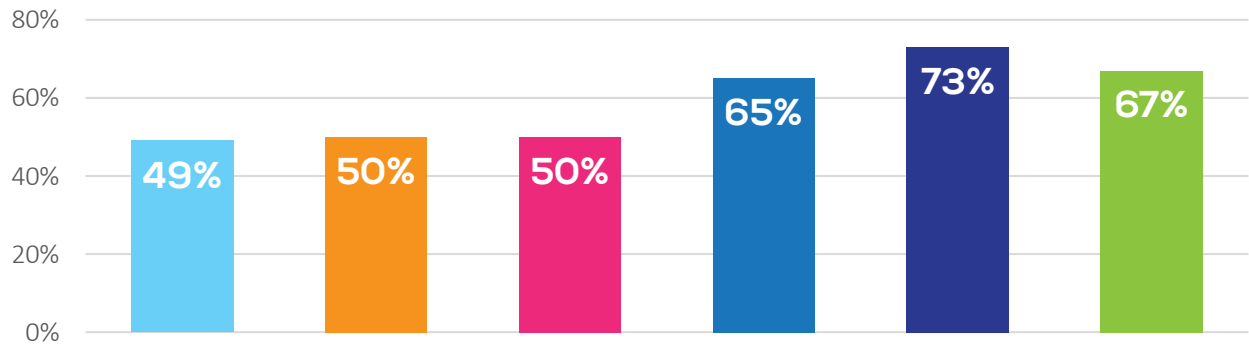
Base: Those in each segment who took any action

"SELF-ASSURED" CLAIM TO BE MOST WILLING TO MANAGE OWN DATA, DESPITE TAKING FEWER ACTIONS

The Self-Assured segment are most likely to claim they are willing to manage their own data, however this does not translate into taking a larger number of actions (see page 45). This inconsistency between attitudes and behaviour may be the result of ill-founded confidence for some within this segment.

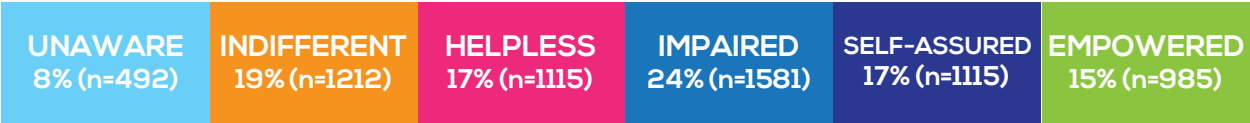


'WILLING TO MANAGE PERSONAL DATA AND PRIVACY SETTINGS'

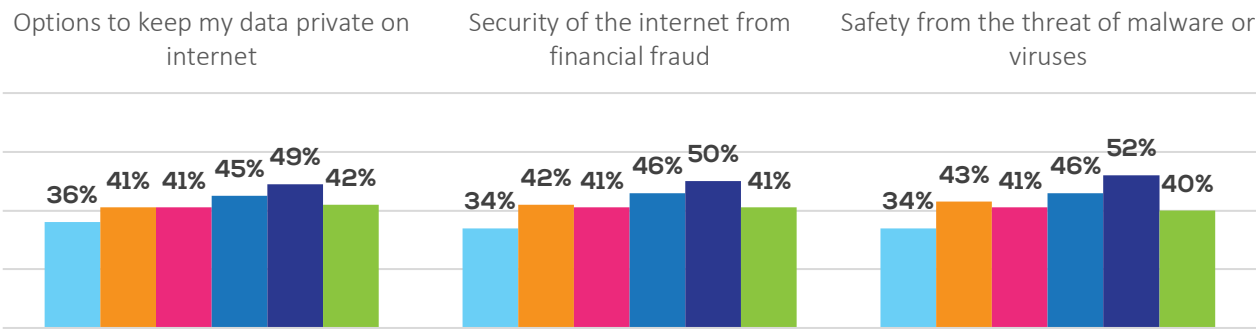


Base: All respondents self-identifying with each segment statement, bases indicated in legend. For full statements see page 36

"SELF-ASSURED" MOST CONFIDENT THAT PRIVACY AND SECURITY CONDITIONS ARE IMPROVING



PROPORTION WHO AGREE EACH ASPECT IS IMPROVING



Base: All respondents self-identifying with each segment statement, bases indicated in legend. For full statements see [page 36](#)

SUMMARY OF KEY SEGMENT CHARACTERISTICS

The table below provides an overview of segment characteristics, most of which are shown in more detail on previous pages. The Unaware segment – those who see little need to take protective action – are least likely to engage in a wide range of smartphone activities, but still highly likely to have experienced data harm. The Impaired and Empowered are the most active segments in terms of smartphone usage and the most likely to have taken steps to protect themselves – the main difference between them being that the Empowered are slightly more likely to feel safer as a result of their actions.

Those who self-classify as Self-Assured are less likely to have experienced data harm, though in fact are less likely to take protective actions than the Impaired and Empowered.

	UNAWARE 8% (n=492)	INDIFFERENT 19% (n=1212)	HELPLESS 17% (n=1115)	IMPAIRED 24% (n=1581)	SELF-ASSURED 17% (n=1115)	EMPOWERED 15% (n=985)
Mobile activity types in past 6 months	5.1	5.9	6.7	7.2	6.4	7.0
Smart devices owned	2.5	2.6	2.8	2.9	3.0	3.0
Experienced data harm	71%	86%	87%	86%	61%	84%
Willing to manage own data	49%	50%	50%	65%	73%	67%
Taken protective actions	74%	89%	89%	92%	63%	89%
Feel “a lot safer” due to actions taken	22%	24%	19%	22%	32%	29%
Age	38% 16-24	33% 16-24	34% 16-24	32% 16-24	39% 16-24	31% 16-24
	33% 25-34	39% 25-34	36% 25-34	38% 25-34	31% 25-34	36% 25-34
	16% 35-44	18% 35-44	18% 35-44	17% 35-44	17% 35-44	19% 35-44
	13% 45+	10% 45+	12% 45+	12% 45+	12% 45+	14% 45+
Gender	56% male	52% male	45% male	49% male	49% male	52% male
	41% female	45% female	52% female	49% female	44% female	46% female
Income	Low 49%	Low 34%	Low 33%	Low 31%	Low 40%	Low 31%
	Medium 31%	Medium 36%	Medium 37%	Medium 34%	Medium 30%	Medium 34%
	High 20%	High 30%	High 31%	High 35%	High 30%	High 35%

Base: All respondents self-identifying with each segment statement, bases indicated in table. For full statements see page 36



MEF
MOBILE ECOSYSTEM FORUM

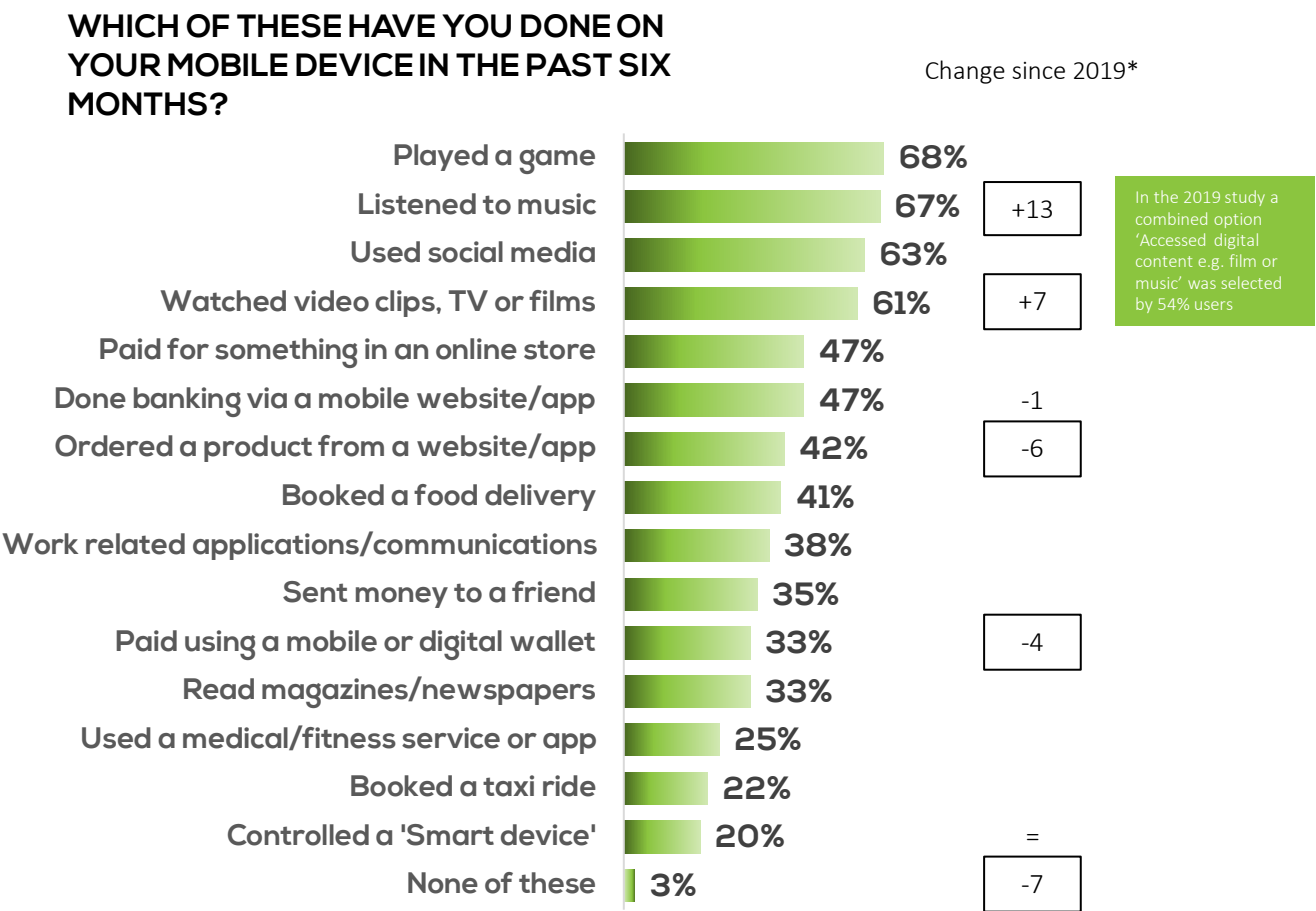
SMARTPHONE BEHAVIOUR AND CONNECTED DEVICES



ACCESING ENTERTAINMENT VIA SMARTPHONE IS INCREASINGLY MAINSTREAM

Well over half of users have accessed digital entertainment on their smartphones in the past 6 months, with games and music ranking most highly. This is followed by more functional activities such as purchasing items and using banking services.

There is a notable increase in the proportion who claim to use music and video services since the 2019 study. Entertainment services are consistently accessed via smartphone in all markets, while there is more differentiation observed for the other types of service (see pages [51-52](#) for differences by market and demographics).



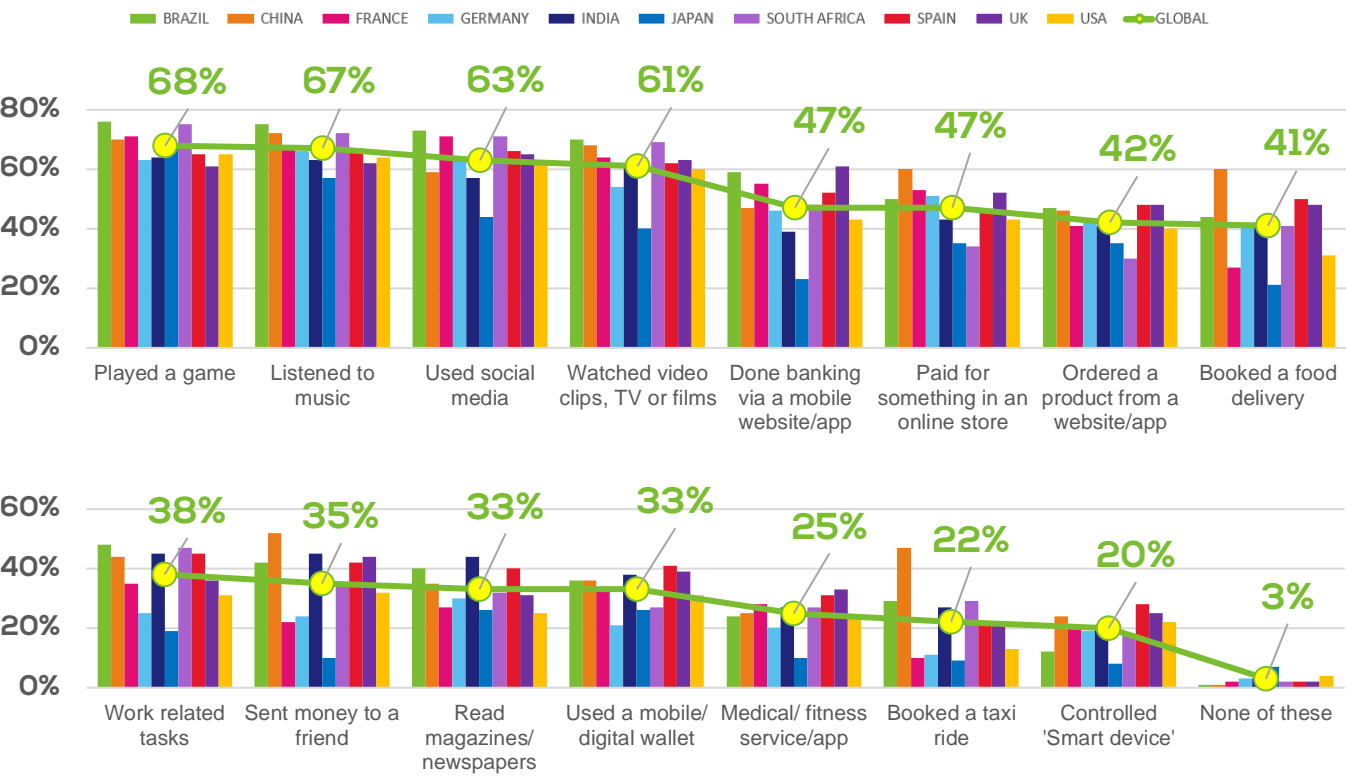
Base: All respondents, n=6,500 *Not all options were available for selection in the previous study

ENTERTAINMENT SERVICES RE COMMONLY USED IN ALL MARKETS

Entertainment services such as gaming, music and video are the most used in all markets, with Brazil and South Africa reporting the highest levels. Functional activities such as banking and payments tend to be less widespread, and there is more differentiation between markets.

China stands out for its relatively high usage of payments, food and taxi ride ordering. As observed in past studies, Japanese users are the least likely to use several of the listed services.

WHICH OF THESE HAVE YOU DONE ON YOUR MOBILE DEVICE IN THE PAST SIX MONTHS? MARKET VIEW

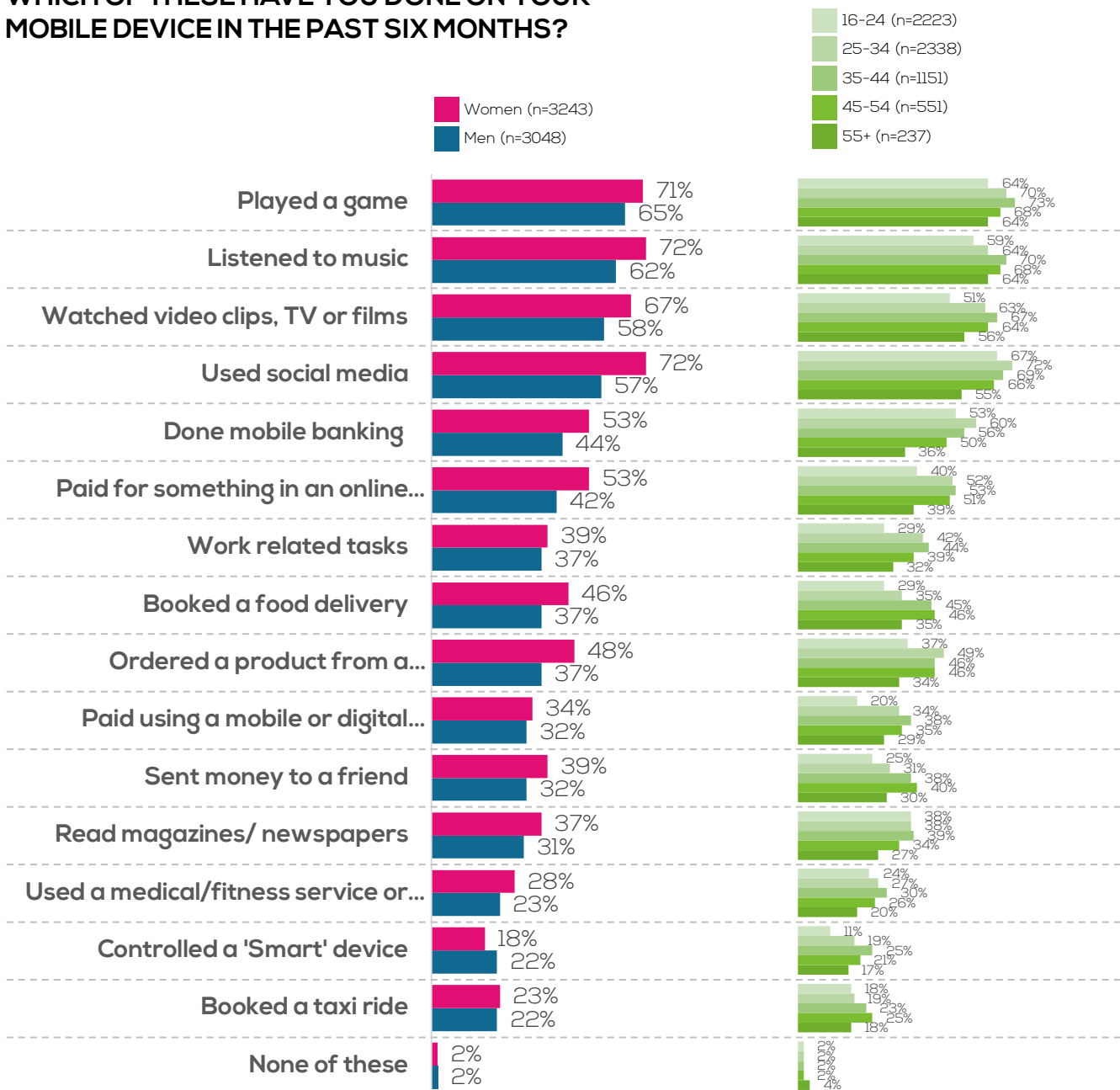


Base: n=650 per market, total 6,500

WOMEN ENGAGE IN MORE SMARTPHONE ACTIVITIES

Women are more likely than men to engage in most activities, with the difference most marked for social media. While age profile varies by activity, the youngest (16-24) and oldest (55+) cohorts tend to engage with fewer activities.

WHICH OF THESE HAVE YOU DONE ON YOUR MOBILE DEVICE IN THE PAST SIX MONTHS?

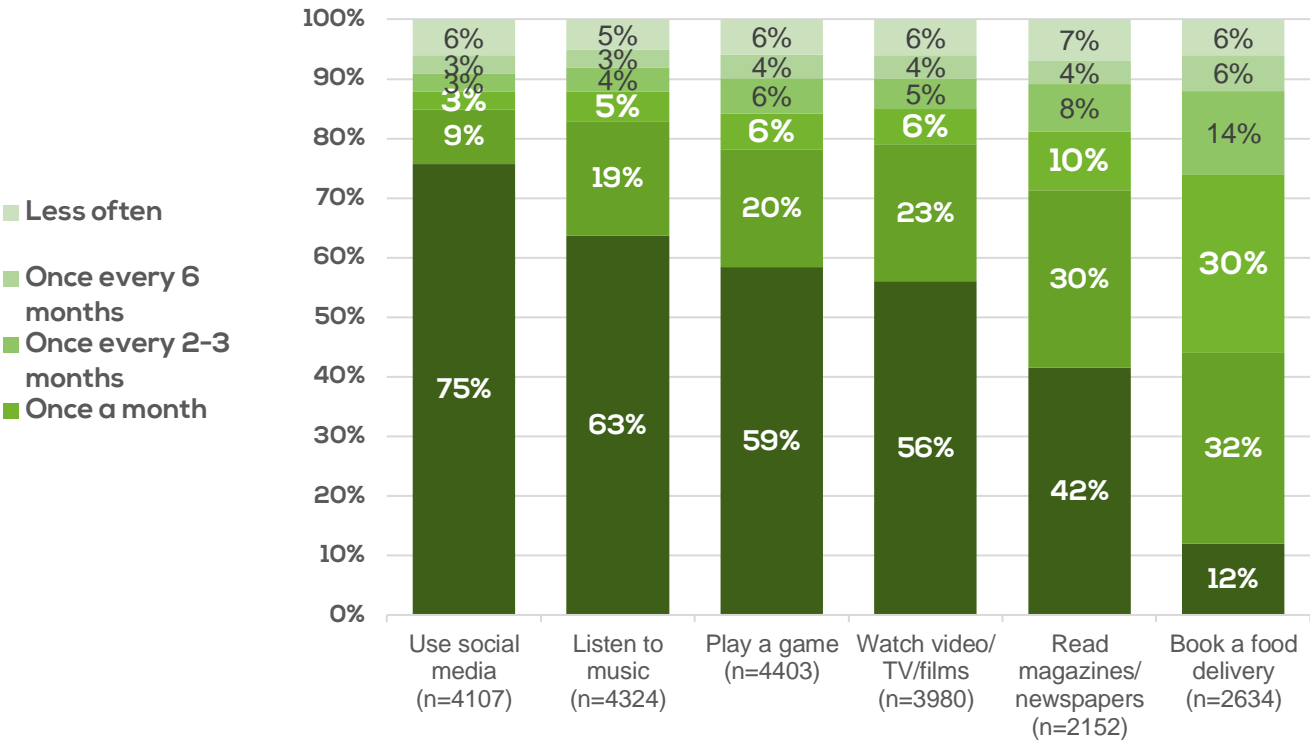


Bases indicated in legend

THREE QUARTERS ENGAGE WITH SOCIAL MEDIA EVERY DAY

Social media is the most frequently accessed service, with three quarters of its users engaging at least once a day. Listening to music is the second most regular activity, followed by playing games and watching videos.

HOW OFTEN DO YOU DO EACH OF THE FOLLOWING ON YOUR MOBILE DEVICE? (PAST 6 MONTH USERS)



Base: All respondents who used each service in the past 6 months, bases indicated in chart

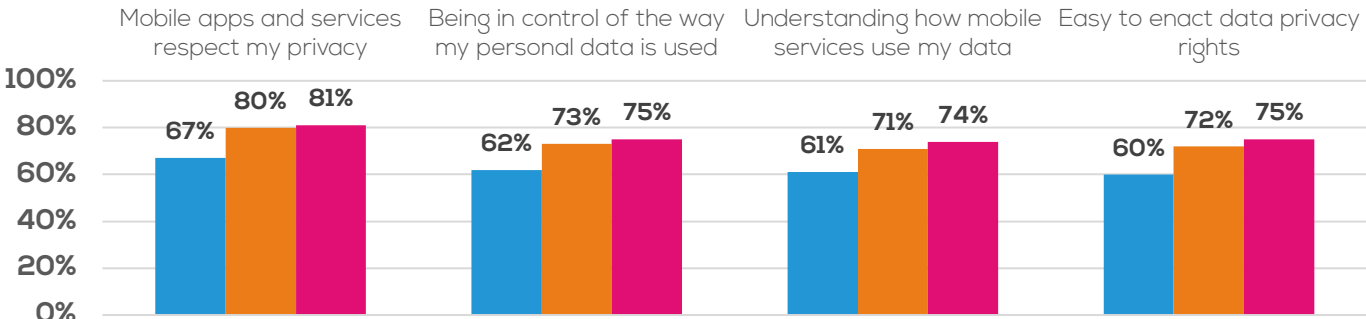
PRIVACY EXPECTATIONS HIGHER FOR FREQUENT SOCIAL MEDIA USERS

Do frequent users of social media have different perceptions when it comes to privacy?

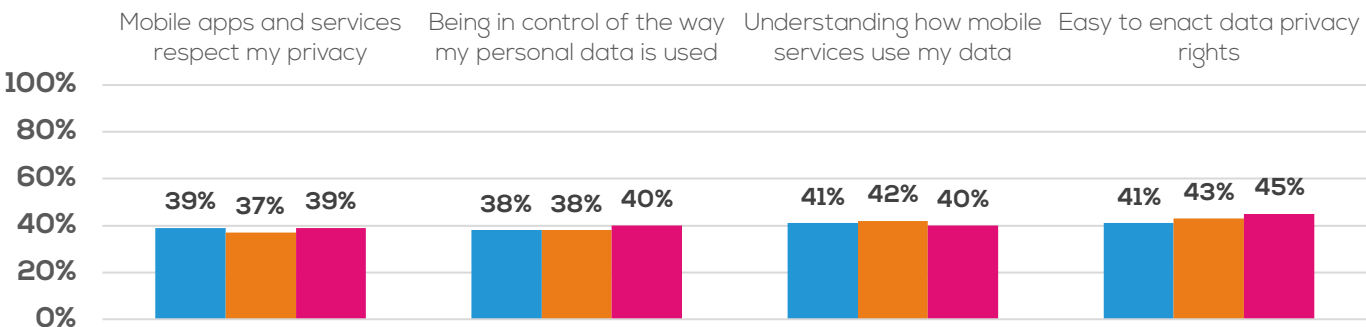
Data suggests that frequent users of services - including social media but also other services such as digital news - are more likely to state that privacy is very important. However, they are no more likely than average to believe that mobile services are delivering on privacy.



RATE EACH ASPECT AS VERY OR EXTREMELY IMPORTANT



SLIGHTLY OR STRONGLY AGREE THAT NEEDS ARE MET



Base: All respondents / Those accessing social media on mobile at least daily / Those accessing newspapers/magazines on mobile at least daily / Those accessing food delivery services at least daily; bases indicated in legend.

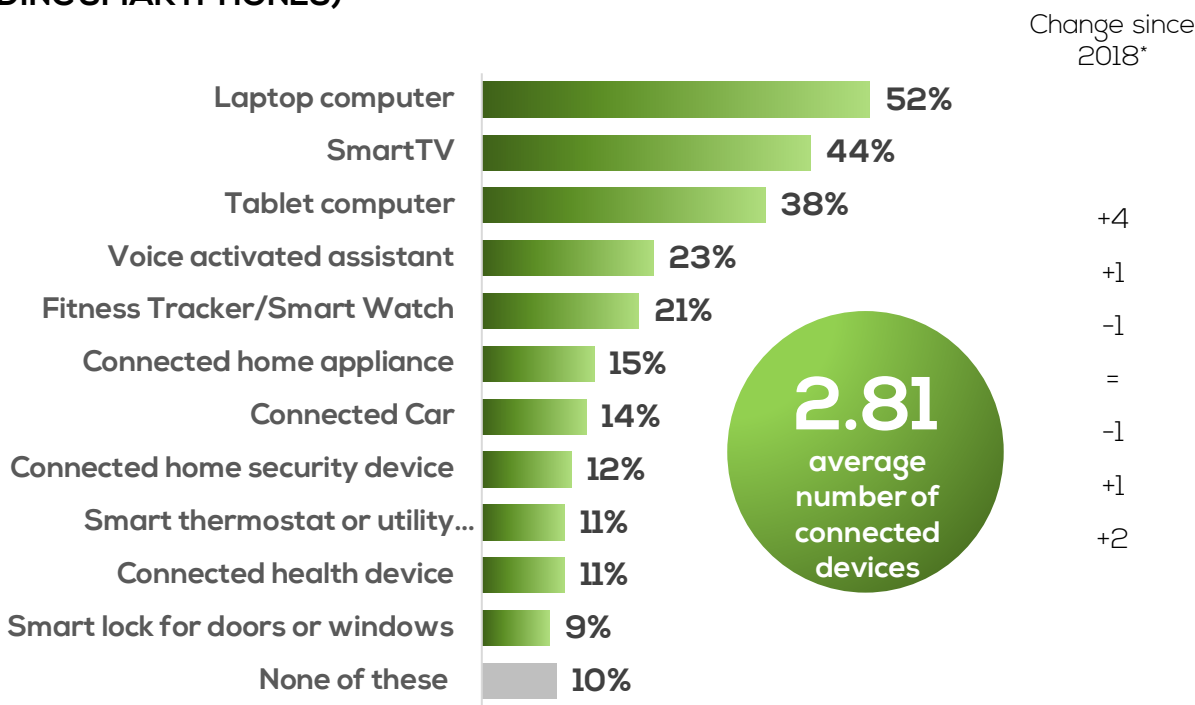
Importance question: To what extent do you agree with the following statements? Scale from 'Not at all important' to 'Extremely important'

Performance question: To what extent do you agree with the following statements? Scale from 'Disagree strongly' to 'Agree strongly'

CONNECTED DEVICES ARE THE NORM

On average, smartphone users around the world have 2.81 connected devices within their household (excluding their smartphone). This rises to well over 3 devices in China and Spain, driven by strong adoption of tablets and other device types (see page [56](#) for detail by market).

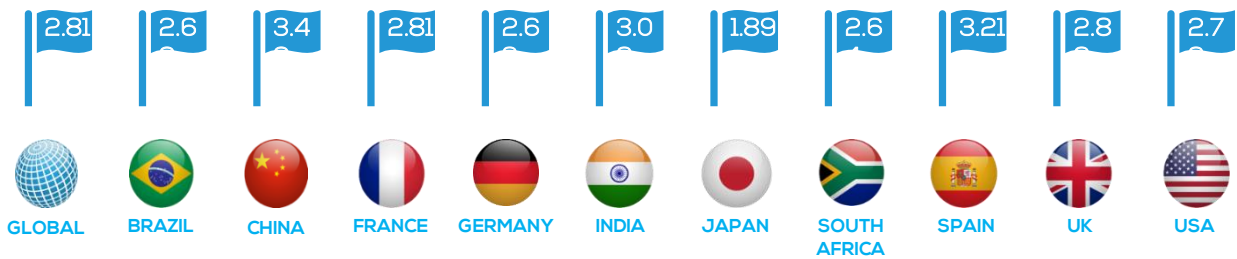
WHICH OF THE FOLLOWING SMART DEVICES, CONNECTED TO THE INTERNET, DO YOU USE, WEAR OR HAVE IN YOUR HOUSEHOLD? (EXCLUDING SMARTPHONES)



Base: All respondents, n=6,500

*Not all options were available for selection in previous study. Indicative comparisons only – 2018 study included 2 different markets (out of 10)

AVERAGE NUMBER OF SMART DEVICE TYPES EXCLUDING SMARTPHONES MARKET VIEW

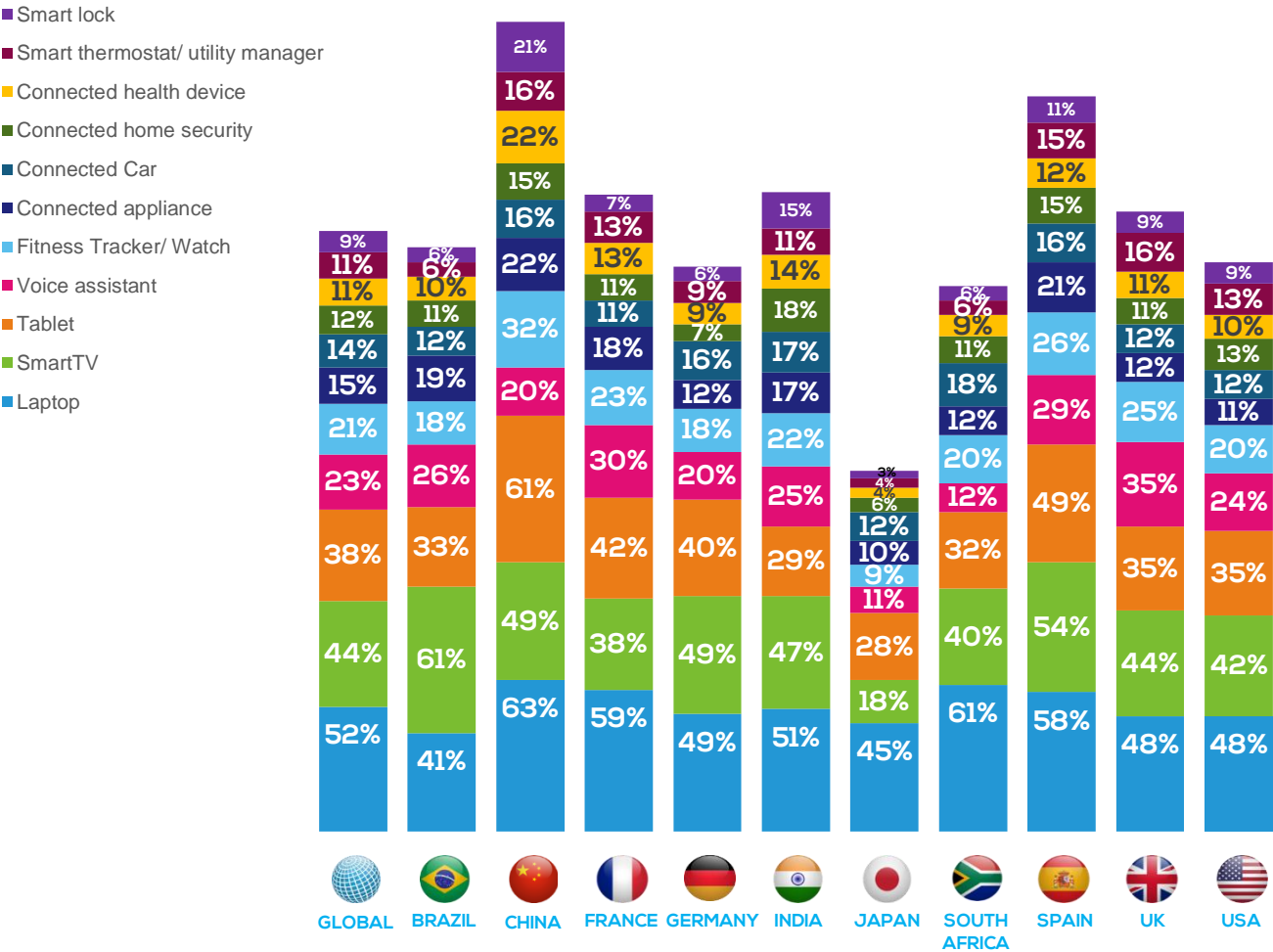


Base: n=650 per market, total 6,500

CHINA AND SPAIN MAKE HEADWAY IN SMART DEVICES

Above average adoption of smart devices in China is driven in particular by tablets but also by laptops, smart locks, fitness trackers/smart watches and connected health devices. Spain also observes more smart devices than average, in particular tablets and SmartTVs.

WHICH OF THE FOLLOWING SMART DEVICES, CONNECTED TO THE INTERNET, DO YOU USE, WEAR OR HAVE IN YOUR HOUSEHOLD? [EXCLUDING SMARTPHONE]*
MARKET VIEW



Base: n=650 per market, total 6,500 *Respondents could select as many devices as were applicable



ABOUT THE STUDY

MEF’s 7th Annual Smartphone Study was carried out in January 2021 . On behalf of MEF, On Device Research surveyed 6,500 smartphone users, 650 in each of 10 markets. Where appropriate year-on-year comparisons are made.



Acknowledgements

With thanks to the contributors of the study:

MEF: Dario Betti, Susan Finlayson – Sitch, and Dhoni Ibrahim

Assurant Strategic Advisor: **Michael Becker**

Consultants: **Barbara Langer**, Insight Angels

Full survey data sets are available for downloading



Visit:

MOBILEECOSYSTEMFORUM.COM



[MOBILEECOSYSTEMFORUM.COM](https://mobileecosystemforum.com)

© 2021 Mobile Ecosystem Forum Ltd.

All Rights Reserved.

Disclaimer

Mobile Ecosystem Forum Ltd. makes no representation, warranty or undertaking with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy, completeness or timeliness of the information provided.

