KPMG

Crossing the line

Staying on the right side of consumer privacy

Privacy Advisory
Thought leadership

kpmg.com

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Table of contents

Foreword	4
Where do consumers draw the line?	6
Mass data collection risks alienation	8
Who do consumers trust?	10
Setting the scene	14
Beware the backlash: Consumers will want their cut	16
Where do regulators draw the line?	21
Crossing the line: a global view	22
Crossing the line: an industry view	24
How must businesses adapt to survive?	26
Keeping in line: Where next for privacy?	30
How KPMG can help	33
About the survey	34

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Foreword

Companies know more about their customers than ever before. In the last 24 hours, your organization probably amassed more information about customers than was conceivable a decade or two ago: the groceries they buy, where they're going on holiday, where they ate out last night or how they got to work this morning.

As consumers, we benefit from this closeness. The fitness apps that track our steps, the messaging apps we use to send pictures from the beach, or the telematics technology in our cars that lowers our insurance premiums.

When we use such technology — whether it's via a computer, a smartphone or a connected car — there is often an assumed understanding: We'll give you our information in exchange for the service or product that makes our lives easier, richer and sometimes cheaper.

This is the trade-off at the heart of the data economy. But there are limits to this trade-off. People are increasingly aware that organizations are collecting, using, retaining and disclosing their information, including buying and selling it. And they are growing uneasy: When does 'helpfully close' cross the line to become 'creepy and intrusive'?

KPMG International asked almost 7,000 members of the public in 24 countries a series of questions to understand in what circumstances they felt comfortable or uneasy about the use of their personal data — to discover where the so-called 'creepy line' lay.

This report is a guide for organizations, to help them tread this line and not cross it.

Unsurprisingly, people draw the line in dramatically different places: One person's 'creepy' is another person's 'cool'. Gender, age, wealth, nationality and education all bend and twist its course … often in surprising ways.

Over half of the survey respondents are willing to share their gender, education or ethnicity online, for example, whereas less than 20 percent are willing to share their income, location, medical records or address.

Asian countries such as India and Malaysia appear to be more receptive than Scandinavian countries to the idea of personalized advertisements. And Japanese consumers seem to have a much lower level of trust in organizations handling personal data than consumers in India, but at the same time are the least likely to take precautions to protect their personal data.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Society has barely begun to address the moral and legal questions of what is private and what is public in this era of big data. This is not a philosophical debate that companies should ignore. Falling foul of regulations or misjudging consumer attitudes not only risks significant financial penalty in key markets such as the European Union (EU) and United States — it also threatens a loss of trust and mass switch-offs from consumers who feel their privacy is being violated. Share prices, earnings and even the survival of some companies will likely rest on a more intelligent and sophisticated approach.

Very few companies are asking themselves whether they are handling customer information in a morally and legally sound way. It is time they did.

Mark Thompson
Global Privacy Lead
KPMG International

Greg Bell
Global Cyber Security Co-leader
KPMG International

Akhilesh Tuteja
Global Cyber Security Co-leader
KPMG International

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Where do consumers draw the line?

When does cool become creepy? When does convenient turn into intrusive? Understanding consumers' sensitivities around the use of their personal data is central to establishing and maintaining trust between consumer and company.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Global insights from the survey:

Over half of respondents said they were happy to share personal data on gender, education and ethnicity online

<20%

Less than 20 percent were happy to disclose information on their online search history, income, location, address or medical records.

55%

55 percent of people said they had decided against buying something online due to privacy concerns.

Respondents in most countries say control over privacy is more important than convenience.

Social media, gaming and entertainment companies are perceived to ask for an unnecessary amount of personal information.

In all markets but one, at least 75 percent of respondents said they were uneasy with their online shopping data being sold to third parties.

>2/3

Over two-thirds of people are not comfortable with smartphone and tablet apps using their personal data.

Half of survey respondents already delete their internet browser cookies or manage their social media privacy settings.

Almost one-third use incognito or 'do not track' modes when browsing the web.

25 percent use encryption to protect their personal data.

50%

Only around half of people would accept free or cheaper products in exchange for less privacy.

Income does not seem to have a big impact on whether people would accept less privacy.

Education levels do not seem to affect people's views on privacy and what they think is creepy or acceptable.

Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Mass data collection risks alienation

Many organizations have not yet recognized the separate levels of intrusion that individuals will tolerate in different areas of their lives. Consumers often compartmentalize their relationships with companies according to when and where they interact with them. When companies intrude into a more private area of life than consumers feel comfortable with, the risk is that people will get irritated and ultimately disengage with a brand.

Distinct sensitivities to privacy

Companies might like to harvest personal data from consumers at all times, but consumers are uncomfortable with this. People have fundamentally different expectations of the privacy they enjoy at home, at work or in public, and they are reluctant to hand over control of their privacy to third parties.

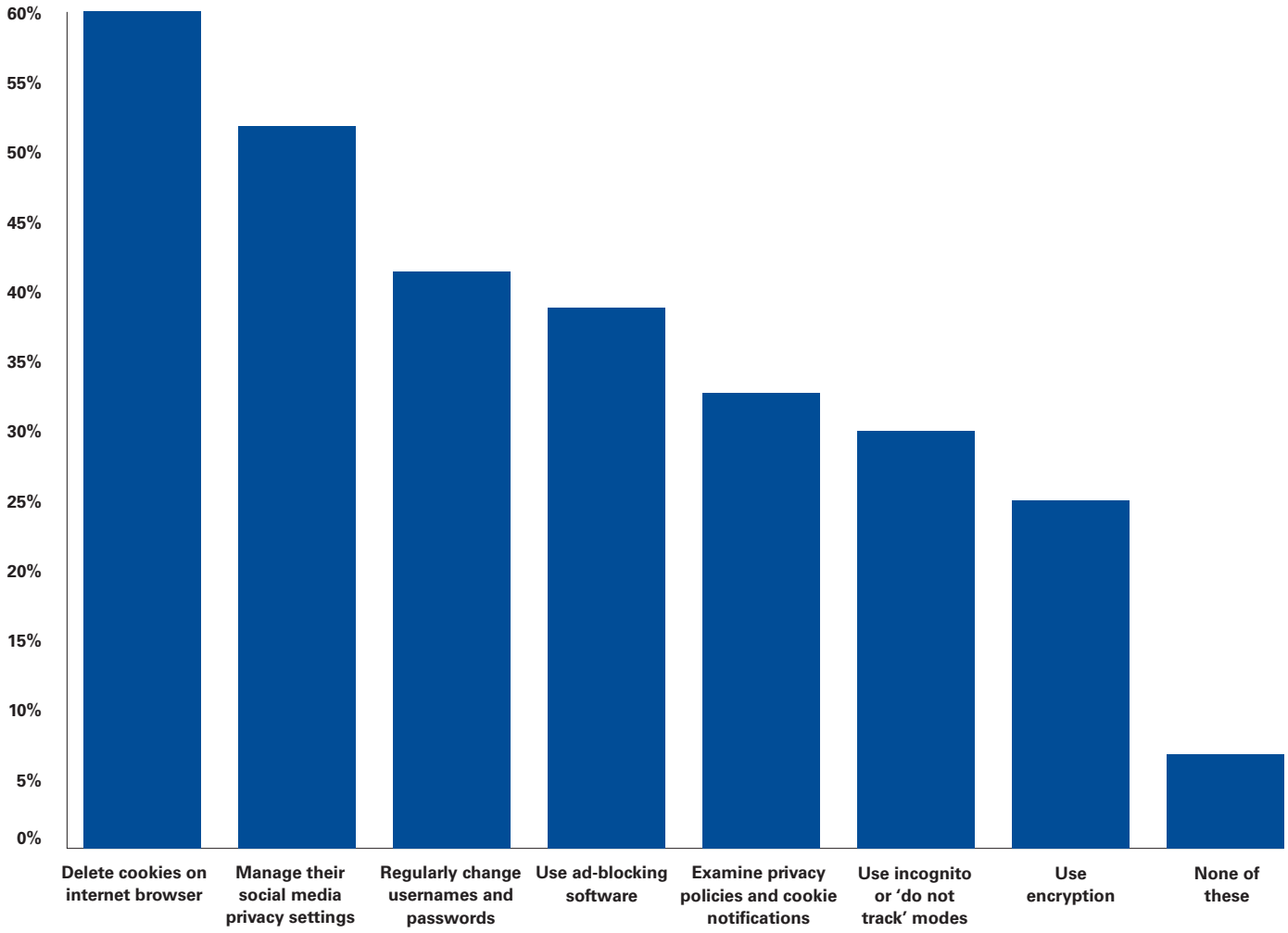
Further, less than 10 percent of consumers globally feel they have full control over the way organizations handle and use their personal information. In Spain, 55 percent said they had no control at all and even in Malaysia, the most relaxed country with regards to control over their personal data, only 31 percent said they had sufficient or full control over the way their personal data was handled and used.

Indiscriminate personal data collection therefore risks alienating consumers. And the more uncomfortable individuals feel, the more likely they are to act to protect their personal data online. Globally, half of survey respondents already delete their internet browser cookies or manage their social media privacy settings. Almost one-third (30 percent) use incognito or 'do not track' modes and 25 percent use encryption **(Figure 1)**.

Around a fifth of respondents are extremely concerned over the way organizations handle and use their personal data.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Figure 1 : Precautions consumers usually take to protect their personal information



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

Public versus private spheres

People are instinctively wary about handing over information that relates to their home life. Energy and water companies in the United States, for example, have already experienced resistance to installing smart meters in residential buildings[1]. The survey reveals that 43 percent of people are uneasy about smart meters in their homes if the information obtained could be used by utility companies to infer how many people live there and what they are doing at certain times of day.

1. The Opt-Out Challenge by Jeff Evans, April 2012, http://bv.com/docs/articles/the-opt-out-challenge.pdf

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Who do consumers trust?

Most trusted

41% Banking

39% Health providers

36% Law enforcement

33% Local government

23% Utilities

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Least trusted

21%
Technology

17%
Supermarkets

14%
Gaming

14%
Retailers

13%
Social media

Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

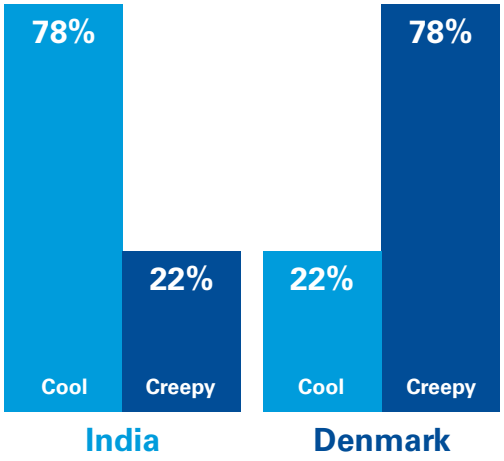
© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

The overarching message from the survey is that the stance on privacy varies according to the data and usage in question, as well as the attitude and location of the consumer. Take the 78 percent who would find personalized electronic billboards 'creepy', for example, compared to the 46 percent who would be prepared to have their TV viewing monitored in return for a cheaper TV. Or the 49 percent who are happy for government agencies to collect personal data to help combat terrorism, compared to the 18 percent who are OK with online retailers selling their personal data to third parties.

Similarly, there are huge regional differences in attitudes. **78 percent in India** think it is 'cool' for taxi companies to use geo-location data to offer people a ride, for example, compared to only **22 percent in Denmark (Figure 2)**. Similarly, personal billboard advertising is considered cool by **60 percent in China**, but creepy by **88 percent in Japan (Figure 3)**.

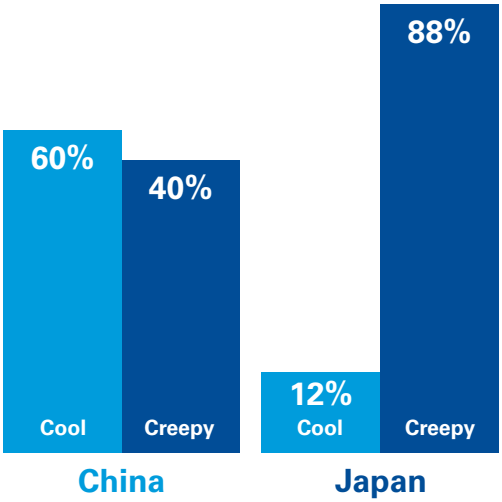
This presents the possibility of a dual economy for personal information. Some consumers are happy (or have no choice) to hand over their personal data, while the more cautious can implement strategies — or potentially pay — to keep it private. This is an unwelcome prospect for advertisers and companies alike, as they rely on personal data about their customers to develop and market their products effectively. This makes it all the more important that organizations learn to use consumers' data appropriately, to ensure consumers continue to provide their information freely.

Figure 2: Taxi companies using geo-location



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

Figure 3: Personal billboard advertising



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Insights for executives: a risk to trust

Mark Thompson
Global Privacy Lead
KPMG International

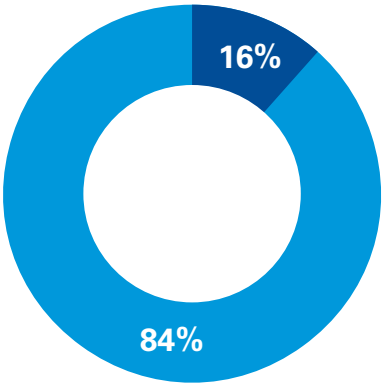
Companies must act with greater discretion when collecting personal data from areas consumers regard as more sensitive if they wish to retain their trust. While some may still count the exchange of personal data for services as a price worth paying, others will work harder to hold on to their personal data.

Without companies making a compelling case for collecting people's data, consumers who can could increasingly choose to withhold it. This could herald a privacy class divide in personal information processing. People who care about their privacy are likely to invest in a variety of protection methods to secure it. Indeed, as the survey shows, many people are already taking advanced steps to protect their privacy online.

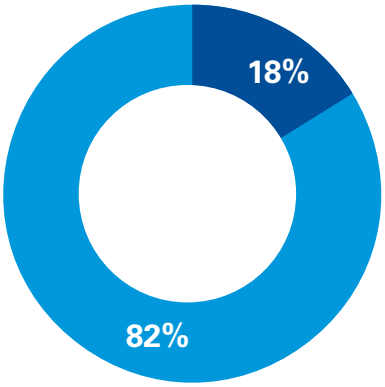
© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Setting the scene

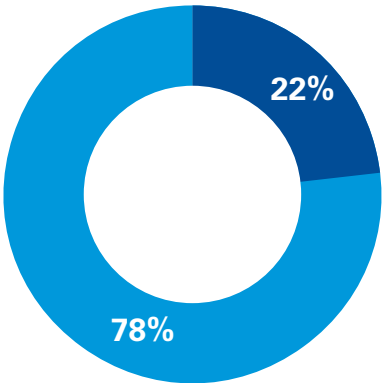
Understanding what consumers consider 'creepy' versus 'cool'



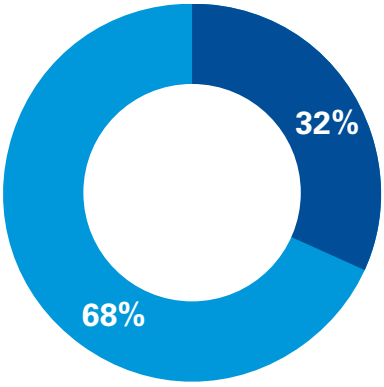
Smartphone and tablet apps used for navigation, chat and news that can access your contacts, photos and browsing history



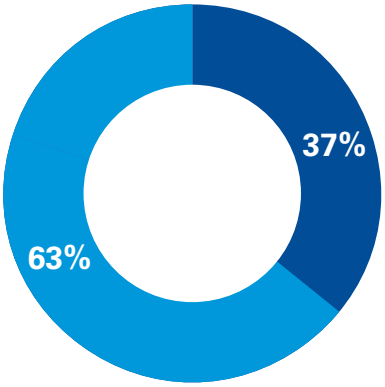
Online retailers that offer savings, speed, convenience, product range and delivery — but sell your data to third parties



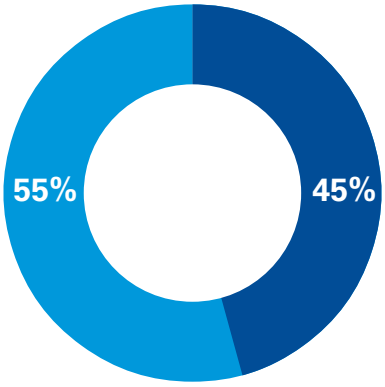
An electronic billboard that greets you by name, asks if you enjoyed breakfast and shows an advertisement for your favorite cereal



You email a friend about a planned Paris visit; online the next day, you notice advertisements for hotels, restaurants and excursions in Paris



A taxi company that buys your geo-location data so it can automatically offer you a cab ride when you get off the train

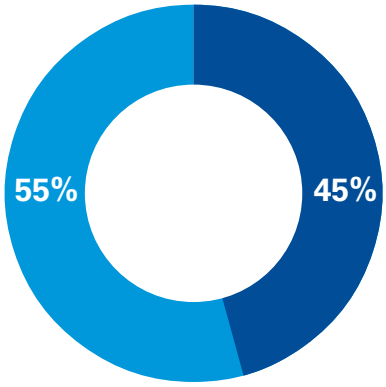


A free fitness-tracking device that monitors your well-being and produces a monthly report for you and your employer

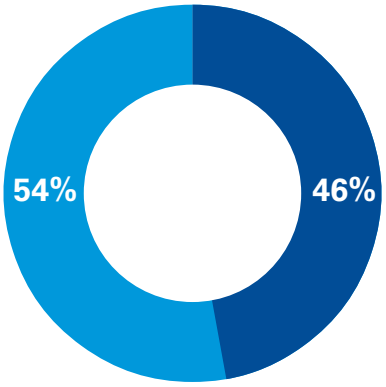
Creepy

Cool

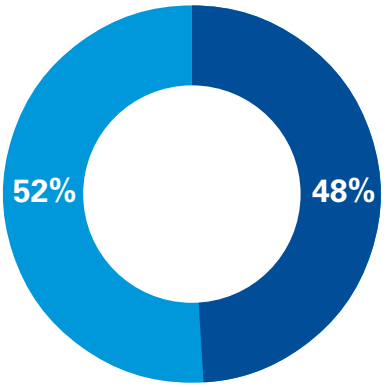
© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated



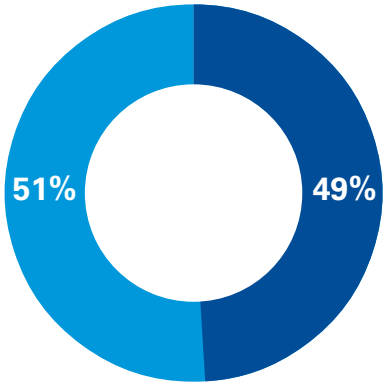
A telematics device that reduces your insurance costs, but gives your insurer the right to inform the police if you drive dangerously



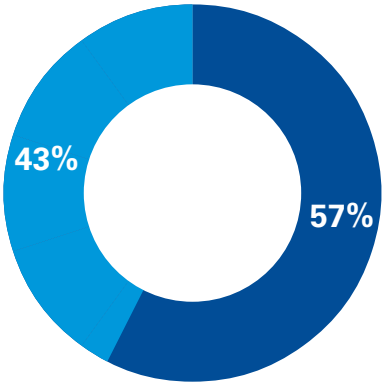
A new television that comes with a discount if you allow your viewing habits to be monitored



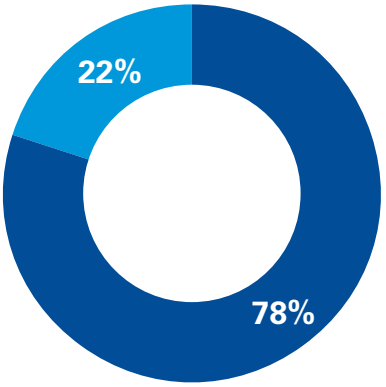
A free tablet PC if you let a tech company track when, why and how you use it



Allowing your emails, text messages and browsing history to be collected to help law enforcement agencies prevent terrorism



Smart energy meters that allow your provider to deduce how many people live in your home, when you eat and sleep, and the appliances you use



A telematics device that enables emergency services to track your vehicle

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Beware the backlash: Consumers will want their cut

Every day, consumers agree to give organizations their personal data in return for free communication, instant knowledge, unlimited entertainment and unparalleled convenience. As long as the consumer feels they are receiving a fair deal, the agreement holds.

But what would happen if a significant section of consumers, say those who find use of their personal data creepy, began to feel they were being shortchanged? Or became more aware of the extent to which their personal data was being used? The growing adoption of anonymous browsing, ad blocking and cookie deletion are early indicators that this is an increasingly important issue for many people.

The survey revealed that 60 percent of consumers globally already delete cookies on their internet browser and 52 percent manage their social media privacy settings.

When looking at figures by country, India was the most likely overall to manage social media privacy settings and regularly change usernames and passwords to protect personal information.

Respondents from Japan, in contrast, were least likely to take precautions to protect personal information.

As awareness around privacy issues grows, businesses risk a backlash when consumers realize the kind of money being made through the trading of their personal data.

The business models of big search engines and social media platforms are based on the sale of consumer data. The Organisation for Economic Co-operation and Development (OECD) estimates that the personal data relating to a single European consumer is worth just under US$5 a year to Facebook. An American is worth closer to US$10[2]. In 2014, a start-up data broker called Datacoup offered people exclusive rights to their own personal data for US$8 a month[3], foreshadowing an ethically debatable situation where individuals have to buy back their own personal data from third-party organizations.

Individuals may generate personal data through the monitoring of their online actions, their purchases and their communications. Data harvesters would say that once they have shared that personal data, it no longer belongs to them.

The UK's National Health Service, for example, has already investigated monetizing its personal data stores. Proponents say that the cost of upgrading to a digital health service would pay for itself in efficiency savings, as well as allowing companies paid access to anonymized health data.

2. OECD (2013), 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value', OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en
3. How much is your personal data worth? | News | The Guardian, by Billy Ehrenberg, 22 April 2014. https://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Data brokers: knowing me, knowing you

They probably know more about you than your significant other, mother or father — possibly even yourself.

Data brokers collect and sell information about billions of people around the world. They might know your email address and phone number, your internet searches from months ago, purchasing patterns … even your sexuality.

One leading data broker says it has information on 700 million consumers worldwide and over 3,000 'propensities' for nearly every US consumer.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Revenue sharing

A more equitable model for sharing the revenue from personal data would be for consumers to enter a formal revenue sharing arrangement with the companies that sell on their personal data. Another option would be for businesses to price their products based on the personal data the consumer surrenders. This already happens to an extent with the telematics box that reduces a driver's vehicle insurance premiums in return for monitoring their driving habits. In fact, globally, 45 percent of respondents said insurers could monitor their driving in return for cheaper premiums, even with the threat of being reported to the police. And in **Brazil**, **China** and **Russia**, the majority of respondents (64 percent) were happy for their driving to be monitored in this way **(Figure 4)**.

It's not too far-fetched to imagine that the next step might be a similar arrangement enabling people to reduce their health insurance premiums in return for wearing a fitness-monitoring device.

According to the survey, if respondents were offered the latest fitness-tracking device by their employers to monitor their levels of fitness and provide them with a monthly report on how to maintain a healthy lifestyle, 76 percent in Brazil and 85 percent in India would accept the offer. Northern European respondents, however, were less likely to find this acceptable.

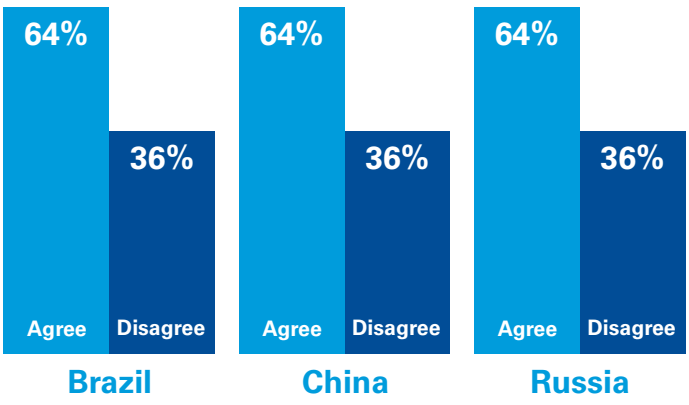
This dual pricing model could extend into other connected devices. A TV that tracks what a consumer is watching might cost US$100. The same TV without data monitoring might cost US$500. The 'internet of things' — a universe of connected devices estimated to grow to over 20 billion 'things' by 2020 — makes this a particularly pertinent consideration for consumer goods manufacturers[4].

The question of consumers' willingness to share personal data is central to the digital future. The survey shows that in the vast majority of countries, between 60 percent and 87 percent of people say control over their privacy is more important than convenience, and 55 percent said they had decided against buying something online due to privacy concerns. Respondents in **Malaysia** (74 percent), **Finland** (72 percent) and **Singapore** (70 percent) were most likely to worry about what would happen to their personal data when buying something online **(Figure 5)**.

However, it may be too late for consumers to claw back control of their personal data even if they wanted to. An individual's personal information is already spread so widely that it would be virtually impossible to regain full control, and given the accelerating rate of connectivity, only a fraction of the personal data that could potentially be shared has so far been shared.

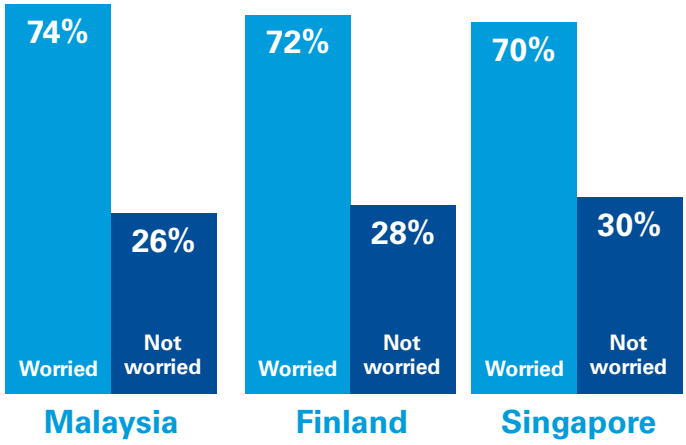
In the longer term, it is likely that businesses will be compelled to set clearer boundaries for personal data sharing and to openly acknowledge the value of people's data. Until then, it is likely to be a question of managing and minimizing the impending backlash.

Figure 4: Agree to their driving being monitored



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

Figure 5: Privacy concerns during online shopping



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

4. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, 10 November 2015, http://www.gartner.com/newsroom/id/3165317

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Insights for executives: red light for data sellers

Greg Bell
Global Cyber Security Co-leader
KPMG International

A price difference at the point of purchase would at least be an open acknowledgement of personal data collection. Currently, consumers have to choose whether to use a service based on a long and complicated set of terms and conditions that almost nobody reads.

A simple, regulated traffic light system is another potential solution. A website that sells on all personal data would come up as red; one that sells some details — amber; and a site deemed green would leave the consumer in complete control. Consumers could make an informed decision about whether they were getting a fair exchange for their personal data.

Early indications are that greater transparency and control leads to more open sharing on the part of consumers. In an experiment in Trento, Italy, hundreds of families used an open sharing system. Their information was stored in a secure way and they could control who accessed it. Because the families had confidence in the system, they ended up sharing a lot more information[5].

5. 'With Big Data Comes Big Responsibility', Harvard Business Review, by Harvard Business Review Staff, November 2014. https://hbr.org/2014/11/with-big-data-comes-big-responsibility

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

So if consumers value their privacy, why do they give it away?

Bruce Lyons
Professor of Economics
University of East Anglia
United Kingdom

People say they are uncomfortable about sharing personal data, but then give it away. We post more and more about our lives on social media, yet fret about losing privacy, says Bruce Lyons, Professor of Economics at the University of East Anglia.

Behavioral economics offers some possible answers as to why people veer from rational decisions and standard economic theory when it comes to personal data:

Status quo bias: People tend to stick with what they have. Companies can exploit that inertia through their default option settings. Online, that default option is often 'share'.

Framing bias: The benefits of sharing are communicated up-front, while the negatives, such as loss of privacy, are hidden away. Consumers are more likely to accept, despite feeling uncomfortable.

Overconfidence: We trust ourselves not to share anything we might later regret. Much of the evidence from Facebook and Twitter tells a different story.

Present bias: We crave the immediate satisfaction of social media 'likes' and shares, but fail to weigh up the longer-term consequences of sharing information.

Organizations are well aware of the behavioral strategies they can use to influence consumers, but so, too, are regulators, says Professor Lyons. The Financial Conduct Authority in the UK, for example, is already monitoring behavioral bias to make sure consumers are not exploited, while in December 2012, the Department of Finance and Deregulation in Australia published a paper on using behavioral strategies to improve regulation.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Where do regulators draw the line?

Organizations can no longer afford to treat privacy as an afterthought. Cyber security and the battle against hackers has long dominated the chief information officer's (CIO) agenda. But cyber security is not the same as privacy.

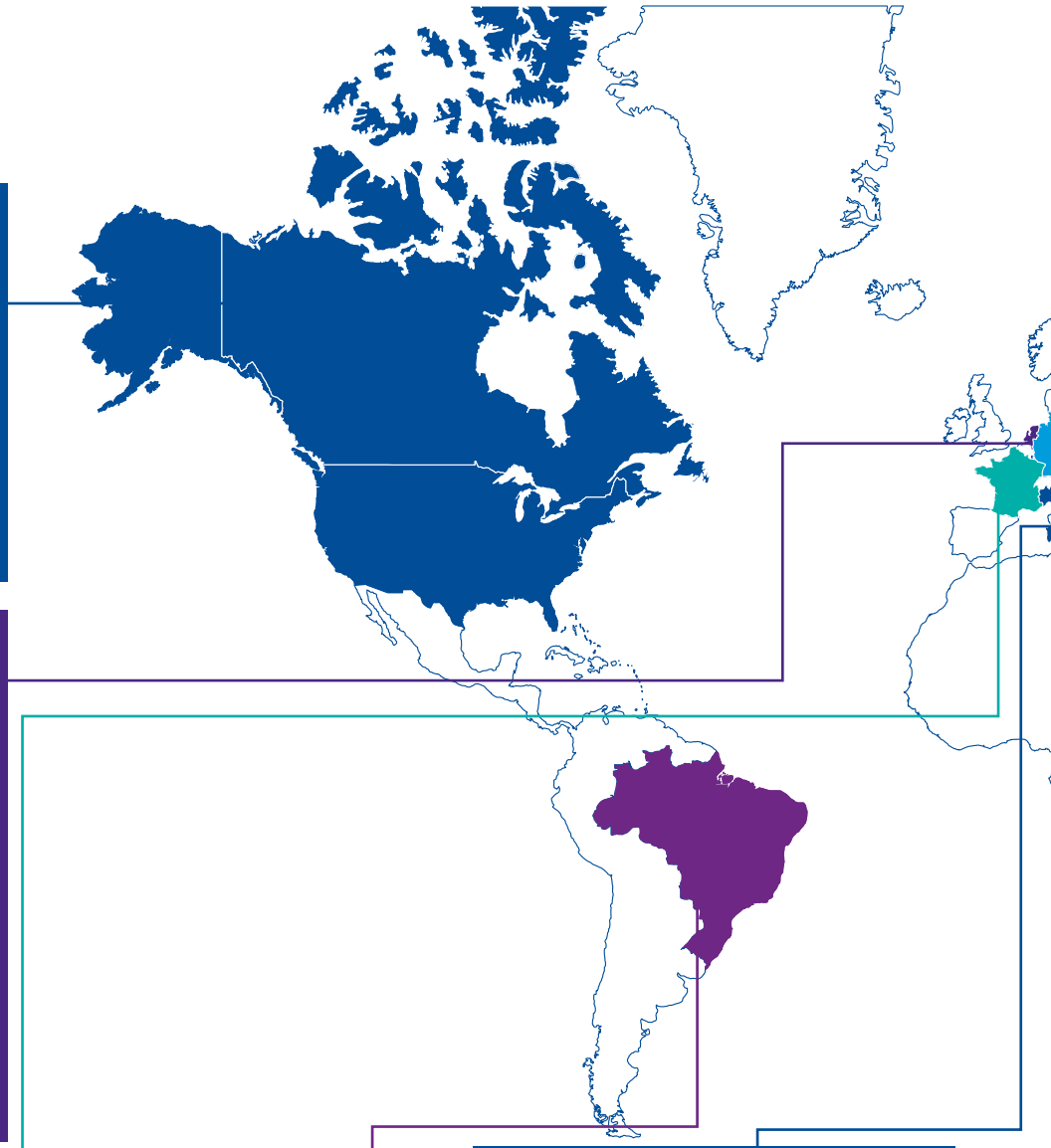
The EU's new rulebook, the General Data Protection Regulation (GDPR), marks a fundamental shift towards the view that privacy must be at the forefront of organizations' minds when dealing with consumer data. Due to come into force in May 2018, it could see organizations hit with fines of up to 4 percent of global worldwide turnover for non-compliance.

Although the GDPR is perhaps the most comprehensive attempt to define a coherent regulatory framework for privacy, governments around the globe are sharpening their focus on the issue and introducing legislation to offer greater protection to consumers — and harsher penalties for violations.

The stricter approach being adopted globally catapults privacy towards the top of organizations' risk radars. In this rapidly changing environment, organizations need to consider a new attitude towards privacy — and they need to do it quickly to minimize the risks to their balance sheet and their reputation.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Crossing the line: a global view



United States and Canada

The USA and Canada were the most concerned about hackers stealing their personal data. *"With almost daily data breaches occurring in North America, it is not surprising that people are concerned about hackers. Increasing litigation and class actions, plus the increase in penalties through legislation like the GDPR, will require US-headquartered firms to really consider their approaches to privacy."* — **Doron Rotman, KPMG in the US**

Netherlands

Dutch respondents are amongst the people that are the least concerned about how organizations handle and use their personal data. Russia is the only country where people have less extreme concern. *"Perhaps the Dutch down-to-earth mentality plays a role here. On the other side, the Netherlands is running ahead of GDPR regulation with the data breach notification law and fine capabilities for the privacy body as of January 1st, 2016. The raise in fines already resulted in urgency at Dutch organizations to report on data breaches and manage privacy comprehensively."* — **Koos Wolters, KPMG in the Netherlands**

France

France is one of the countries least likely to be in favor of government agencies collecting personal data, even to help combat terrorism. *"Given the history of tragic events in France, French people value the privacy laws that were first enacted almost 40 years ago; this shows governments need to take into account citizens' privacy expectations when trying to address some of the most difficult challenges we face in modern society."* — **Vincent Maret, KPMG in France**

Brazil

A draft bill for the protection of personal data was released in January 2015. It includes measures around obtaining consent, processing and transferring personal data, reporting data breaches and allowing people to access their personal data. The draft bill contains penalties for violations, including fines and suspension or prohibition from processing personal information for up to 10 years. — **Leandro Augusto Antonio, KPMG in Brazil**

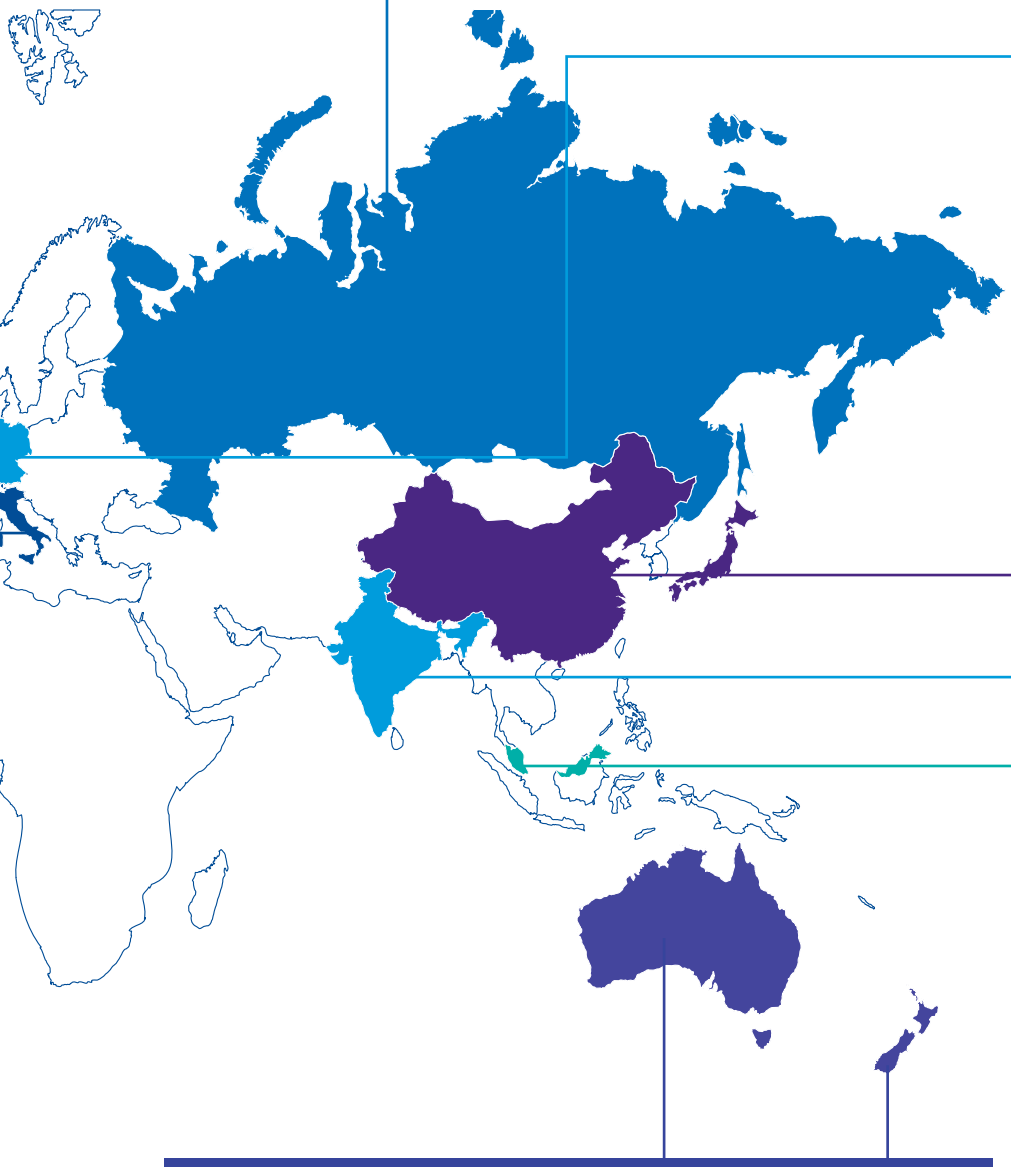
Italy

Italy is one of the countries most likely to be in favor of government agencies collecting personal data. *"It is coherent with a sort of dangerous low perception of privacy risk that Italians have; looking to this data we can notice that Italy is one of the European countries that uses more social media and is the country least likely to worry about what would happen to their personal data when buying something online. There is still a long way to go in terms of privacy awareness but, looking to the high relevance of digital media in Italian society, it is the only choice."* — **Luca Boselli, KPMG in Italy**

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Russia

Only 11% of Russian respondents were extremely concerned about the way companies handle and use their personal data. *"This fact represents that Russian people do not fully realize the consequences of personal data leakage. Terms of privacy are currently emerging in Russia and the average Russian citizens are less conscious of technical aspects and their legal rights in this field. Along with that, it is not common in Russia to cover privacy incidents in mass media, leading to low awareness."* — **Ilya Shalenkov, KPMG in Russia**



Germany

German respondents are among the least likely to accept a free fitness-tracking device from their employer. *"This is not surprising, given Germany's traditional reticence over sharing personal information. It presents a real challenge for German businesses as they move into a more digital economy. German businesses risk getting left behind unless they can strike the right balance."* — **Michael Falk, KPMG in Germany**

China

"Although 60% of the respondents think personalized billboard advertising is cool, 39% are extremely concerned about the way companies handle and use their personal data! For organizations operating in China, using digital innovation to bring customers closer is well accepted but the tension between new and exciting products and trust poses a real challenge." — **Henry Shek, KPMG in China**

Japan

Japanese were the least willing overall to share information with organizations online, but also the least likely to take precautions to protect their personal data. *"This creates an interesting dilemma for Japanese companies who operate online. It also provides an opportunity for organizations to succeed if they get the balance right."* — **Atsushi Taguchi, KPMG in Japan**

India

"India has the highest level of trust in organizations handling personal data. As the digital economy evolves, this trust provides a real opportunity to create value in the Indian market. However, as awareness of privacy issues grows, I would expect the trust and expectations of Indian consumers to be transformed." — **Mayuran Palanisamy, KPMG in India**

Malaysia

"Asian businesses are committing to major investments in the tech revolution, with an explosion of new start-ups and huge investments in digital and analytics initiatives. Ensuring customers' privacy concerns are adequately addressed will be vital for success." — **Dani Michaux, KPMG in Malaysia**

Australia

Of non-European countries, Australians are least likely to read a privacy policy when entering a website. *"This raises an interesting challenge for Australian organizations. If customers are generally not reading the information they are given, how can organizations ensure they are being transparent with their customers? It will require organizations to think about new innovative and accessible ways to provide this transparency."* — **Jacinta Munro, KPMG in Australia**

New Zealand

New Zealanders are the most likely to use ad-blocking software to protect personal data. *"New Zealanders take privacy seriously. Organizations need to reflect this in all their dealings with customers and clients."* — **Souella Cumming, KPMG in New Zealand**

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Crossing the line: an industry view

Life sciences

"Traditional pharmaceutical business models are no longer viable. The life sciences industry has experienced unprecedented change via merger-and-acquisition activity; the shift to personalized medicine; focus on value-based outcomes for patients; advancements in and interconnectivity across medical technologies; and greater collaboration with business and IT partners. Information is the key ingredient in driving and sustaining these new business models; we must identify, protect and govern information in order to capitalize on recent advancements." **Chris Stirling, Global Chair, Life Sciences**

Technology

"With the internet of things, everything from our shoes, to TVs that monitor us when they are turned off, to our photocopiers is likely to be connected to the internet. The costs of getting privacy wrong could result in real and meaningful damage to organizations, and require expensive and lengthy remediation work." **Gary Matuszak, Global Head of Technology, Media and Telecommunications, KPMG International**

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Consumer markets

"Consumer goods and retail companies are targeting customers with increasingly more relevant and timely messages. Given the vast amount of detailed personal and behavioral data that these companies can track on their customers or online shoppers, they are at a particularly high risk of crossing the 'creepy' line. Consumer goods and retail companies need to pay careful attention to both the positive and negative effects of their marketing campaigns to know exactly where and when to draw the line." **Willy Kruh, Global Chair, Consumer Markets, KPMG International**

Financial services

"Financial institutions have a tradition of protecting assets and information and continue to invest heavily as a priority. The challenge they face is to ensure the areas where they are investing will deliver the protection their customers expect, and investing in the right capability to manage the business and risk profile in a sustainable way. Those who are able to conquer these two challenges will have competitive advantage to potentially become trusted custodians of customer data for additional online identity and privacy services." **Jeremy Anderson, Global Head of Financial Services, KPMG International and Partner, KPMG in the UK**

Energy and resources

"Energy companies are now entering the home, with new technology such as smart meters revealing new insights into customers at a level never seen before. Creating value from this is key, but it is critical that these innovative activities do not impact the organization's core business activities." **Alejandro Rivas-Vásquez, UK Head of Cyber Security, Energy, KPMG in the UK**

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

How must businesses adapt to survive?

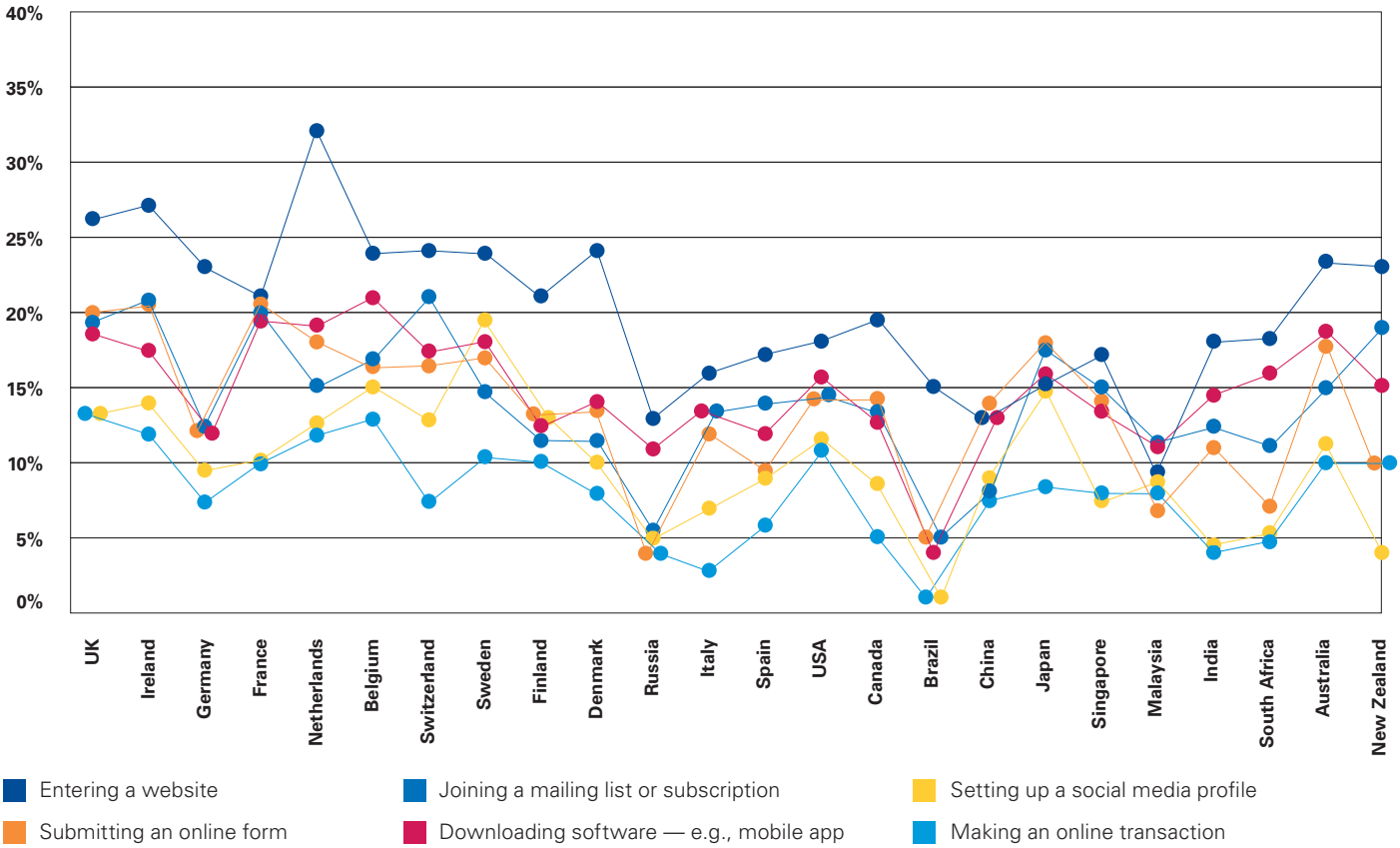
One of the first issues to tackle should be mind-set. What may have been accepted, or at least tolerated, in the past, should be reviewed in light of stricter global approaches to privacy legislation.

Gaining customer consent by mystifying them with long-winded legal statements and 20-page policy disclaimers is not a sustainable strategy. As the survey shows, for example, 57 percent of people globally fail to read, or only skim, privacy policies on entering websites. At a regional level, **Europeans** appear to be less likely to read privacy policies than consumers in the **North America** and **Asia Pacific** regions **(Figure 6)**.

Instead, transparency should be the guiding principle regarding privacy. Organizations need to ensure they fully understand what they want to do with customer data, and where and how they are storing it, and then explain it to customers in a clear and simple way.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Figure 6: How thoroughly consumers read privacy policies when doing various activities



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

Getting privacy right

Organizations may find it hard to be transparent about privacy because they are unaware about how they are affected by existing or future regulations, or because they:

— have no privacy policy

— are collecting personal data on an ad-hoc basis

— have no real idea where data resides.

Without knowing where the data is, it is impossible to manage it. As well as customer lists in sales and marketing, personal data will pass between IT, business development, HR and finance — stored on potentially hundreds of different systems that may not be compatible with one another.

It may sit on legacy data servers and get passed around to suppliers, payment providers, auditors, regulators and dozens of other third parties without a thought. There will likely be literally thousands of gaps to fill.

Data localization measures often included in the new wave of global privacy legislation also pose a considerable challenge for businesses. Data localization is when data is required to be stored and processed within national borders. Given the increasing reliance on cloud computing as a way to reduce costs, enhance flexibility and improve efficiency, regulations that require data to be localized could fragment the global market and actually disadvantage internet users.

Organizations need to start prioritizing the issue of privacy at board level, and investing appropriate resources into their privacy strategy, systems and processes. Those that don't could find themselves paying a heavy price.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Safe and secure

In contrast to the problem of privacy, getting senior management to focus on data security is often an easier task. In the survey, 32 percent of people on average said strong security systems were the most effective measure to gain trust, rising to 40 percent and over in some key markets, such as **France**, **Malaysia** and **Spain (Figure 7)**.

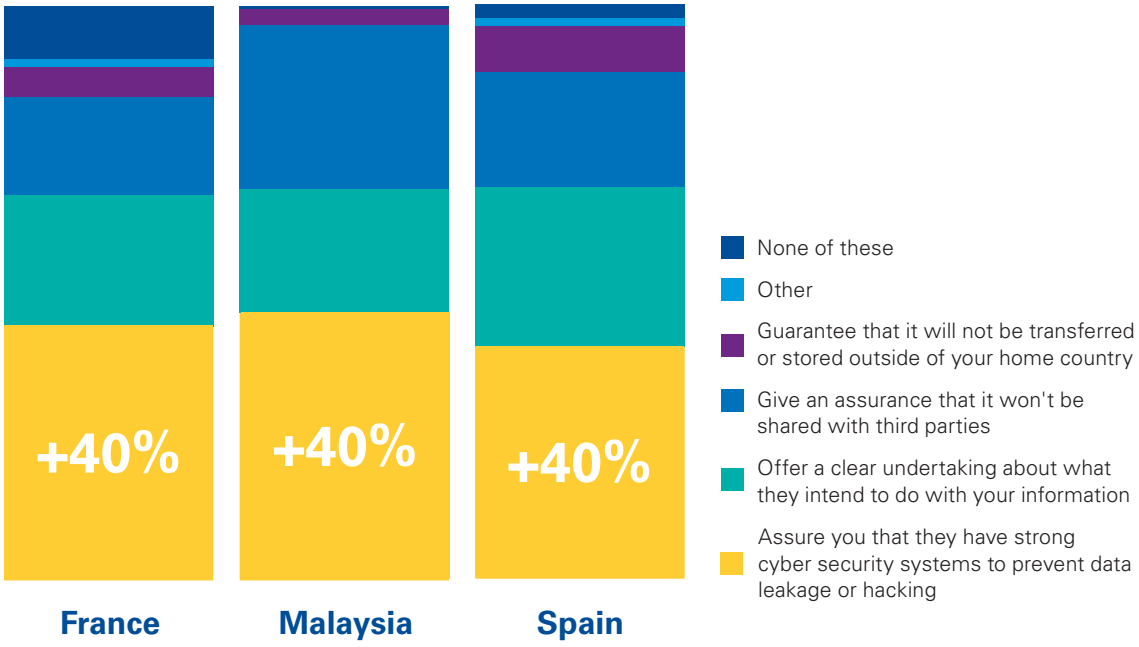
Security, particularly when it is breached, grabs the headlines and, therefore, the attention and resources that are still rarely directed towards privacy.

In reality, however, security is just one of the many factors that need to be considered in a comprehensive privacy framework. An organization's security might be strong, but does the organization properly notify individuals and gain their consent? Does it comply with rules around the transfer of personal data across borders? Is it ready for any forthcoming regulatory requirements? A rigorous privacy management framework has dozens of other elements to consider; security for privacy is just one element.

Getting this right is a significant and global challenge, even for a large dedicated privacy team — a resource which very few corporates can call on.

Addressing this situation will take investment, time and expertise. A challenge that is compounded by a lack of qualified, experienced people in what is still a relatively new discipline.

Figure 7: Most effective measure to gain trust



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Achieving 'privacy readiness'

The survey showed that globally, on average, **56 percent** of people are either 'concerned' or 'extremely concerned' about the way companies handle and use their personal data.

China, India and **Singapore**, in particular, show a high level of concern about the handling and use of their personal data. The proportion of people who were 'extremely concerned' was highest in these markets, at 39 percent, 35 percent and 32 percent, respectively **(Figure 8)**.

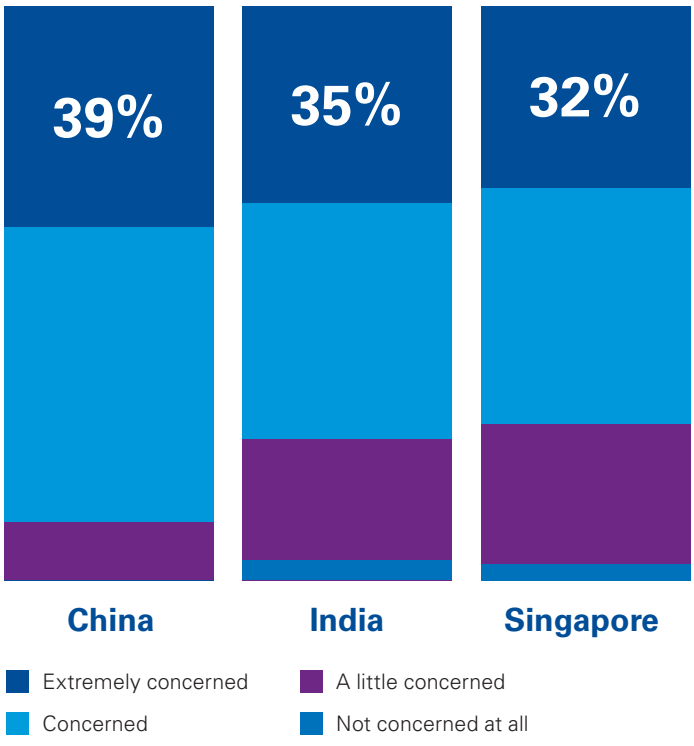
Developing a comprehensive framework to prioritize privacy is, therefore, essential. A global manufacturer with thousands of employees might focus on employee data first. For consumer-facing businesses, on the other hand, the priority should be to resolve any issues with their consumer data.

Done right, a comprehensive privacy framework should not be seen as a brake on sales and marketing, but a tool to help businesses better understand their customers, improve products and services and tailor them to customers' specific demands.

Whether it is opportunity or fear that focuses minds, organizations need to understand the scale and complexity of the problem and act quickly. Privacy needs to be embedded into everything companies do with personal data — from the moment they collect it, throughout its entire life cycle. It may seem like a mountain to climb, but with authorities around the world snapping at their heels, the sooner organizations start climbing, the better.

"The survey showed that globally, on average, **56 percent** of people are either 'concerned' or 'extremely concerned' about the way companies handle and use their personal data."

Figure 8: Level of trust in organizations handling personal data



Source: Crossing the line: Staying on the right side of consumer privacy, KPMG International 2016.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Keeping in line: Where next for privacy?

Personal data is the fuel of our future economy — a source of revenue and driver of prosperity. As the public becomes more aware of the threat to their privacy, new business models are emerging to deal with consumer concerns, presenting both opportunities and challenges to existing businesses.

Typically, the availability of personal data is the enabler for disruptive technologies. App-based ride-sharing services, for example, rely on users' GPS locations. As such, they replace the need for background process, such as manually entering your location, and reduce costs. But there is a natural tension between business models built on personal data and consumers' privacy.

With the survey suggesting that **84 percent** of people feel they have less than 'sufficient' control over the way organizations use their personal data, compared to only 10 percent who feel they are in full control, the time is ripe for new technology to help consumers regain control over their personal data[6].

People will often hand over their personal data when they see a clear benefit in doing so. Frequently, this takes the form of reduced or zero cost to the consumer. But there are clear positives for businesses, too. For example, in the financial services industry, innovators such as Kreditech[7] in Germany and Fair Isaac Corporation (FICO)[8] in the United States are overturning traditional credit analysis, using people's online and social media profiles to help quantify their credit risk. The traditional process behind lending criteria is becoming less important.

For consumers, using personal data is a move towards the sharing economy, where people can crowdsource loans, insurance or investments. In return, potential investors check their personal data — including social media — before lending.

"**84 percent** of people feel they have less than 'sufficient' control over the way organizations use their personal data."

6. 'Privacy and Cybersecurity: Key findings from Pew Research', Pew Research Center, by Mary Madden, 15 January 2015.
7. FT: 'Kreditech: A credit check by social media', Financial Times, by Jeevan Vasagar, 19 January 2016.
8. Forbes: 'Your social media posts may soon affect your credit score', Forbes.com, by Bill Hardekopf, 23 October 2015.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Commoditization of personal data

It is not hard to see a time in the not-too-distant future when personal data is packaged and traded on the stock market, with personal data from more wealthy consumers having more value. Businesses may start offering people products and services at different rates, depending on the level of personal data they are prepared to share.

Shift in awareness

Most people remain unaware of the level of personal data that companies hold about them and the effect this could have on their lives, but the tide may be turning.

Among the latest developments are apps to track the trackers. Designed by US academic teams, the idea is to show people exactly which companies are following them across the internet[9]. Knowledge of this sort may well enlighten large sections of the public as to just how their information is being used — and highlight any loss of privacy.

Data brokers for consumers

Another option is an 'identity attribute exchange', where a third party will manage an individual's personal data on their behalf. Private investment companies are looking into offering this service. The tools and regulations are not yet fully in place to make this a reality, but given the current rate of change, it could happen sooner rather than later.

Will people continue to tolerate business models that use their personal data, as long as they are happy with the service they receive in return? It is hard to imagine the major search engines or software companies losing their market dominance in the short term, but the growth of privacy-enabling services highlights people's basic desire to hold on to their personal data.

As the market develops, organizations must recognize that protecting customers' data is not just a box-ticking exercise to appease over-zealous regulators. Customer awareness and market expectations have already grown to such an extent that any perceived failure to take data protection and privacy seriously not only risks undermining customer confidence, but also undermining the fundamental financial stability of the business itself.

9. 'Privacy apps to help fight back against companies that track you', New Scientist, by Aviva Rutkin, 25 November 2015.

Insights for executives: Get me my broker!

Akhilesh Tuteja
Global Cyber Security Co-leader
KPMG International

Data doesn't disappear, but it is possible to hide it. So it's not hard to envision the emergence of companies marketing online brand obfuscation — a service that helps you mask your identity or 'rebrand' it. It's the next logical step from online personal brand managers, which already exist.

Companies might also see the development of personal brokers that market to consumers directly. A personal data broker would act as an intermediary between the individual and organizations looking to use their personal data. Imagine your car has broken down. You could get in touch with your data broker — who already knows your location, car model, and registration and bank details — to sort out recovery and repair. The data broker model offers consumers a single point of contact, with all the relevant information at their fingertips, to sort out the end-to-end process.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

Are you privacy ready?

As authorities around the globe sharpen their focus on privacy, few organizations are ready for what's about to hit them. Fines that were once measured in the tens of thousands for organizations caught mishandling, mis-collecting or misusing customer data could potentially rise to hundreds of millions or even billions.

With many industry insiders expecting regulators to flex their newfound muscles early in order to make a point, organizations need to move quickly to understand the creepy line, and act fast to ensure they don't stray onto the wrong side.

Seven steps to be privacy ready:

Step 1
Educate senior stakeholders so they understand what privacy means for your organization.

Step 2
Understand the level of privacy risk to which your organization is exposed.

Step 3
Understand the expectations of the individuals whose data you process and set a privacy strategy that aligns to this.

Step 4
Understand the organization's level of privacy maturity and set a clear strategy aligned to your desired target privacy maturity state and your consumer's 'creepy line'.

Step 5
Develop a robust plan to mitigate your privacy risks and deliver your target state.

Step 6
Execute your plan. Introduce sustainable structures to help manage your privacy risks, ensuring compliance but also providing a strong foundation to flexibly leverage personal data to create value for the organization, your customers and your employees.

Step 7
Monitor, maintain and repeat.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated

How KPMG can help

KPMG member firms' privacy professionals support clients around the globe in resolving complex privacy issues, from niche challenges specific to certain organizations to end-to-end privacy compliance programs in complex and highly regulated industries.

The KPMG privacy team has deep experience in helping clients to address the challenges posed by privacy risk, with a structured and flexible approach to meet the needs of diverse organizations. The global reach of KPMG member firms enables them to work effectively across multiple territories at a local level.

Areas where KPMG member firms are frequently engaged include:

— **Assessment:** providing an independent assessment of privacy risk and how to reduce it

— **Design:** designing privacy compliance programs

— I**mplementation:** implementing robust privacy processes, policies and controls

— **Strategy:** developing pragmatic privacy strategies and gaining buy-in from senior management

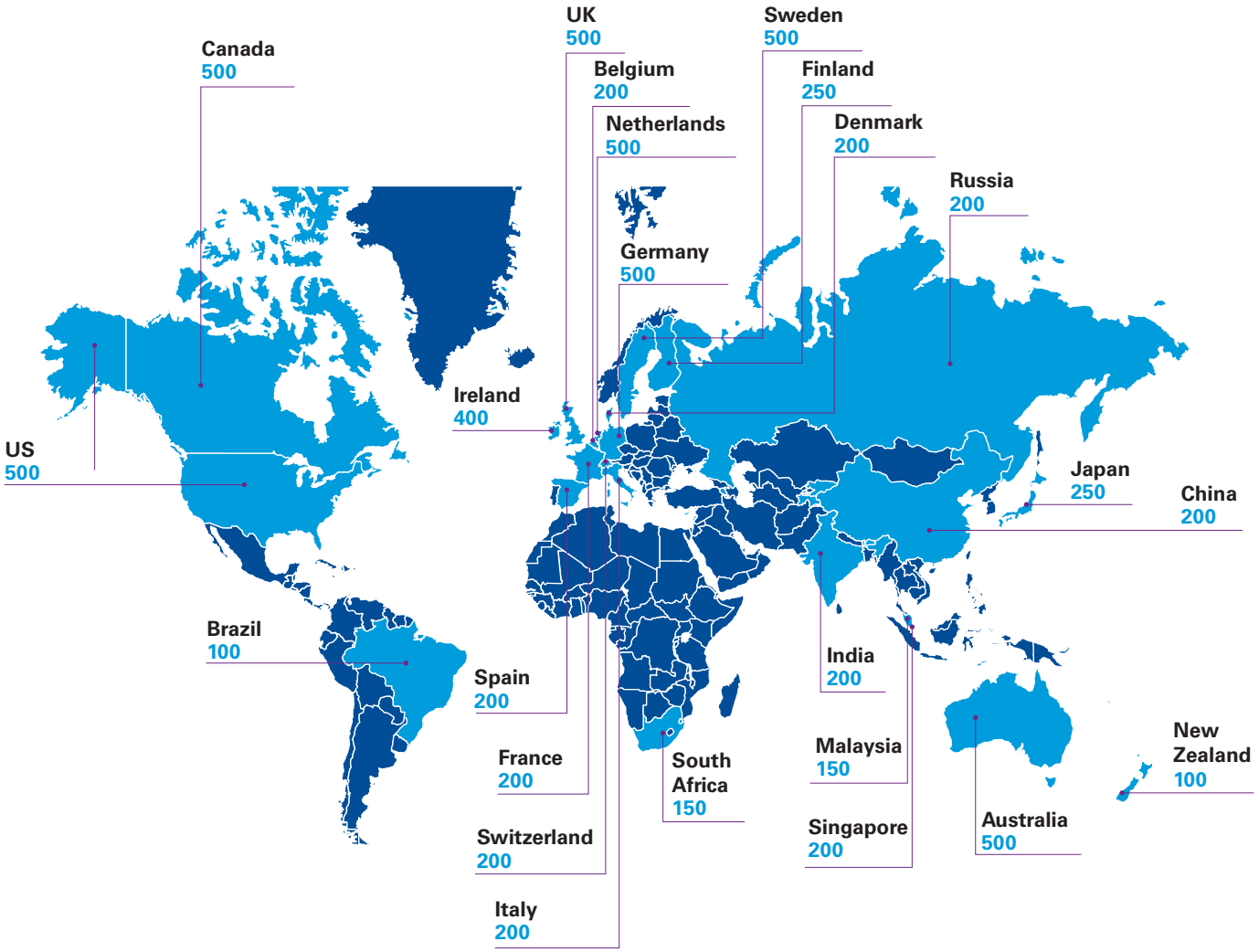
— **Operations**: providing ongoing support to help clients operate their privacy framework

— **Monitoring:** helping clients as they maintain and monitor the performance privacy regimes

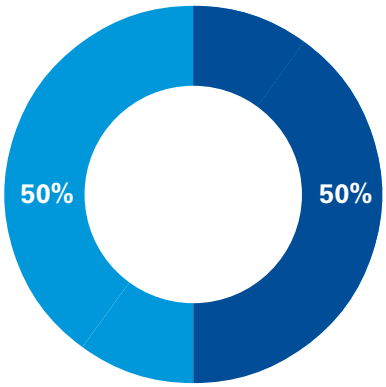
© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

About the survey

6,900 responses across 24 countries:

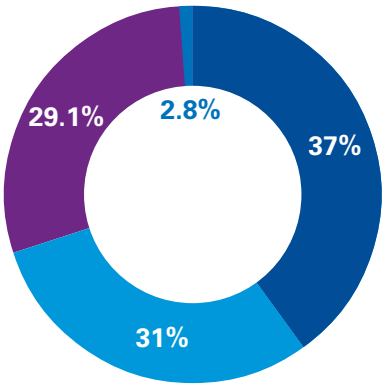


© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated



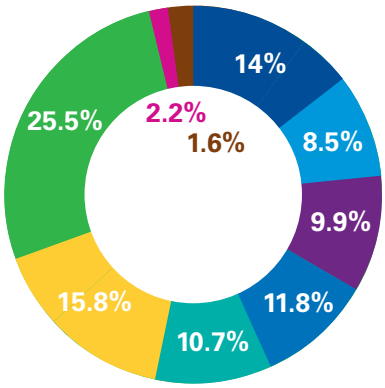
Please select your gender

Male	(3,451)
Female	(3,449)
Total	**(6,900)**



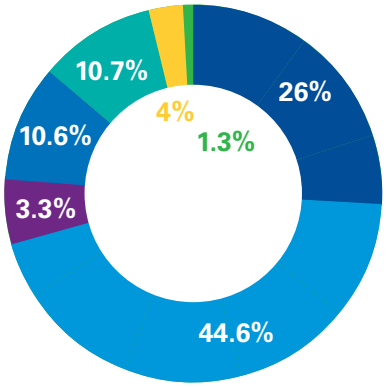
How old are you?

Millennials	(2,555)
Generation X	(2,142)
Baby Boomers	(2,009)
71+	(194)
Total	**(6,900)**



Which of these life stages best describes you?

Young adult pre-children	(965)
Young family — e.g., pre-school children	(585)
Middle family — e.g., children aged 5–9	(683)
Older family — e.g., children 10–16	(811)
Older dependents — e.g., children aged 16+ living at home	(738)
Empty-nester — children who have left home	(1,090)
Adult(s) without children	(1,762)
Other (please specify)	(155)
Prefer not to say	(111)
Total	**(6,900)**



Which of these best describes you?

Single (and never married)	(1,792)
Married	(3,077)
In a civil partnership	(230)
Living with a partner	(729)
Widowed, divorced or separated and living on own	(701)
In a relationship, not living together	(278)
Other	(93)
Total	**(6,900)**

Note: Totals might not add up to 100% due to rounding.

© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Contact us

Mark Thompson
Global Privacy Lead
KPMG International
E: mark.thompson@kpmg.co.uk

Greg Bell
Global Cyber Security Co-leader
KPMG International
E: rgregbell@kpmg.com

Akhilesh Tuteja
Global Cyber Security Co-leader
KPMG International
E: atuteja@kpmg.com

Doron Rotman
KPMG in the US
E: drotman@kpmg.com

Koos Wolters
KPMG in the Netherlands
E: wolters.koos@kpmg.nl

Vincent Maret
KPMG in France
E: vmaret@kpmg.fr

Leandro Augusto Antonio
KPMG in Brazil
E: lantonio@kpmg.com.br

Luca Boselli
KPMG in Italy
E: lboselli@kpmg.it

Jacinta Munro
KPMG in Australia
E: jacintamunro@kpmg.com.au

Souella Cumming
KPMG in New Zealand
E: smcumming@kpmg.co.nz

Ilya Shalenkov
KPMG in Russia
E: ishalenkov@kpmg.ru

Michael Falk
KPMG in Germany
E: mfalk@kpmg.com

Henry Shek
KPMG in China
E: henry.shek@kpmg.com

Atsushi Taguchi
KPMG in Japan
E: atsushi.taguchi@jp.kpmg.com

Mayuran Palanisamy
KPMG in India
E: mpalanisamy@kpmg.com

Dani Michaux
KPMG in Malaysia
E: danimichaux@kpmg.com.my

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store

©2017 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by Create | CRT063635
Publication name: Crossing the line: Staying on the right side of consumer privacy
Publication number: 134122-G
Publication date: January 2017