Personal data in the cloud:

A global survey of consumer attitudes

FUJITSU

shaping tomorrow with you

Foreword Cloud computing is a game-changing development for the ICT industry and has major implications for us all. For some, cloud computing evokes fear of change and of loss of control. For others, it is an opportunity for new services that make life easier. Fujitsu's vision of a human-centric intelligent society relies on the kind of scale and ubiquity that the cloud paradigm is able to deliver – both to individuals and to society as a whole.

Cloud computing describes a move to on-demand, scalable and subscription-based consumption of technology services, supplied from external sources and accessed over the Internet. The promise of the cloud is that information technology systems will become information systems. The Cloud allows us to focus on the outcomes we seek, be they business or personal. The days of a system or a piece of data being rigidly anchored to a physical point are numbered; systems may lose their moorings and become stateless and fluid. And we will need to revisit our assumptions about how we consume information. Our strategy is not just to see the cloud as a new way of delivering technology, but as a new approach to the way that businesses and organizations function, how they interact and even define themselves. We think that the next few years will see a period of profound change for enterprise computing and its role in the organization.

As a global company, we, Fujitsu, focus on the enterprise customer, but when we commissioned this report, we wanted to go further. Because sitting at the heart of the changes that the cloud brings is the relationship between an individual and their own information. We wanted to gain an understanding of how ordinary people around the world – our customers' customers – feel about their personal data. How they value it and who they trust with it. This is what we want to share with you in this report.

The research has shown, as one might expect, that individuals have genuine concerns and fears about privacy and are wary of some organizations and governments when it comes to data protection. It has also revealed that while consumers are concerned about their data, they do little to actively protect it. When we analyze the findings, we discover that deeper trends are at work. We find that privacy is linked to value, and both are linked to what is personal. The more personal the data, the more valuable its potential uses, and the more vulnerable it is. But the current perception is that giving up data only has a negative impact on the individual, because the individual cannot see the value.

This report argues that an evolution is taking place. To most people, these are new issues and they are unfamiliar and uneasy with them. As people become more aware and comfortable, so their behavior will change and they will start to take control and seek advantage. Data will start to take on a shape which we, as individuals, can observe and touch - even manipulate. We could draw an analogy with the evolution in banking from small, local, closed banks to today's globally integrated economy. Organizations have to change their tactics from thinking about standards to focusing on benefits to their customers, consumers and citizens.

This research is a starting point for a journey. Over the coming months, we will be widening the net: interviewing more people across a range of countries, further examining the topics we have developed in this report and bringing to you the regional implications of this insight. We believe this will inform the development of our vision and lead to a wider benefit for our customers.

Masaharu Sato
President, Fujitsu Research Institute

Introduction
Data with borders

Imagine your journey to work. At every point you generate data. Your mobile phone tracks where you are, alerting you to travel delays. Your local coffee shop knows you're coming and has your regular order ready as you walk in the door, and, at precisely the same moment, your phone company accesses your bank details and pays. As you sip your coffee, you pick up an email from your doctor reminding you that you're supposed to be cutting down your caffeine and another from your children's school confirming that they've arrived. This world, which is not so very far removed from the one we already live in, might sound appealing to parents, worried about the safety of their children, but invasive to people who don't want their doctor nagging them. One person might welcome automatic payments, while another wants to be able to authorize them. We're all different: our age, gender and the country we live in all have an impact on where we draw our personal boundaries.

When we read about cloud computing in the media, we tend to get one of two messages: that governments and corporations are gathering unprecedented volumes of data about us and exploiting it for their own ends, and that – as consumers – we should be concerned about the risks posed by our data being passed around without our permission and outside our control. Most of the debate has been around global standards and other regulations governing data privacy.

But there has been very little research about what we – as consumers – actually think. Much is inferred, but very little is proved. Which is why we believe that the research we've completed, surveying around 3,000 people in six different countries and interviewing many more, is so important.

Our analysis, summarized in this report, highlights three important conclusions:

- Consumers are more excited and intrigued by the opportunities stemming from cloud computing than has been thought. They are, indeed, concerned about data privacy, but weigh the risks involved in sharing data against the benefits.
- Although they expect governments to police the use of data, consumers don't really trust either the public or private sectors to protect it properly. Their sense of what is "personal" data is complex. Instead of systems in which other organizations look after their data, people want the tools to be able to control who has access to it. However, many of us are currently not acting on these concerns.
- No single, one-size-fits-all approach to data privacy will work. The boundary people want to draw around their data varies with age, gender and country. There is also wide variation in how people weigh up the potential benefits of sharing data, in specific applications, against the risks. Some people are comfortable with the idea that their data could be stored anywhere in the world. Others are not: their boundary is also their national border.

The implications are far-reaching. Most importantly, our research suggests that, if the full economic and social potential of cloud computing is to be realized, governments and business need to:

- Start with their citizens and customers: what will they gain?
- Think globally, but act locally when it comes to data privacy

90%

of US consumers want to be asked to give permission for their data to be shared, but only 77% of Japanese consumers do

88%

of people are worried about who has access to their data

72%

of German consumers expect the government to keep out of their personal data, but only 46% of US consumers expect this

36%

of Singapore consumers believe that the benefits of using personal data to create personalized shopping experiences outweigh the risks, but only 17% of UK consumers do

Weighing the benefits
consumers are prepared to trade off

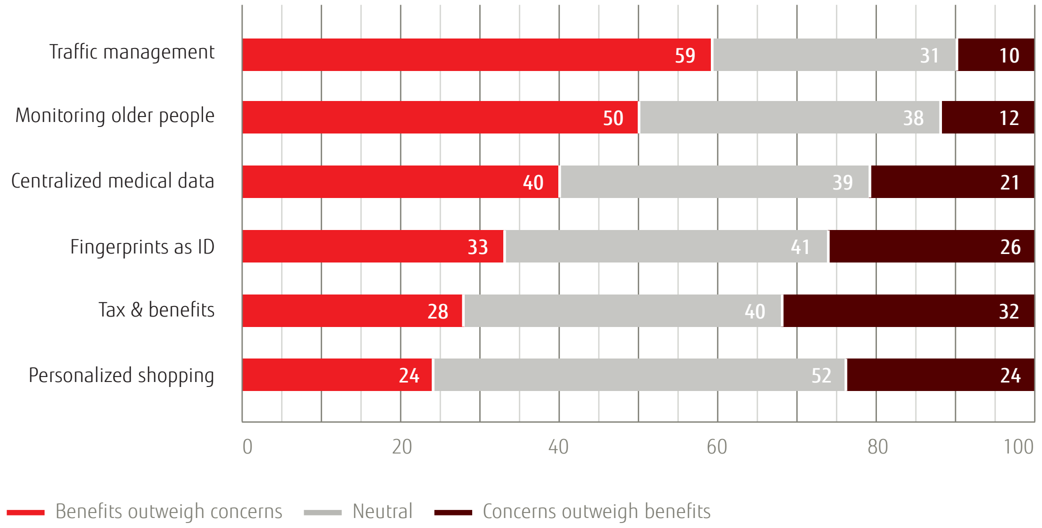
Our research suggests that people are more positive about the potential benefits of finding new ways to share data than most articles in the media would suggest. Fears about data privacy are substantial, but many of us are willing to offset them against what we think we will gain. However, our research also shows that people in different countries weigh these factors differently.

We asked people to consider six examples of how wider data sharing might be used in the future. We also asked them to rate the extent to which the benefits they could see in each scenario outweighed the concerns raised.

Intelligent traffic systems topped the list: few could raise any argument against the idea that data on car movements could be aggregated and distributed to help people avoid congested areas. “You could turn off lights at intersections where there is no traffic,” suggested a US-based interviewee. “If you listen to a traffic report in Chicago, everything’s changed by the time you get there.”

> “The transport system is at bursting point now, the roads are just coping, the hospitals are just coping, we’re just holding on really. You go down to the doctor with a cough and there are 40 people waiting.”
> UK consumer

Benefits of and concerns over future scenarios (in %)



Traffic management: Our highways are monitored by an intelligent traffic system. If this system senses traffic congestion or an accident, it will alert you to take a different road

Monitoring older people: You are elderly; there are sensors in your house detecting if you are moving around, and if not, sending messages to your children or an emergency line

Centralized medical data: All your medical data will be stored electronically and can be accessed from anywhere in the world and at any time by all medical professionals

Fingerprints as ID: You can use your fingerprints to access your financial information and make purchases in shops

Tax & benefits: Governments will monitor how much you earn, thus removing the need to fill in tax forms and eradicating tax evasion; in addition, state benefits will be paid to you accurately and automatically

Personalized shopping: When you walk into a shop, you will see personalized adverts and recommendations (e.g. special promotions with your clothing size) being played as you enter

Remote monitoring of older people in their homes to check their safety and wellbeing also met with broad approval, partly because it was seen as a way to help them stay in their own homes for longer.

Giving access to centralized medical data, ensuring that patients get the correct treatment quickly and potentially saving lives, was more contentious, but still approved of on balance. “I’ve been in hospital many times,” commented a consumer in Chicago, “but none of it is connected. If I get a new doctor, they won’t know what operation I had or when I had it, so it would be good to have that information available instantly. Some of my previous doctors are dead: I don’t even know what has happened to their records.” This person was not alone: although there were concerns about the loss and misuse of such data, 40% of people surveyed thought that the benefits of centralized medical records were more important than the issues, compared to 21% who thought the opposite.

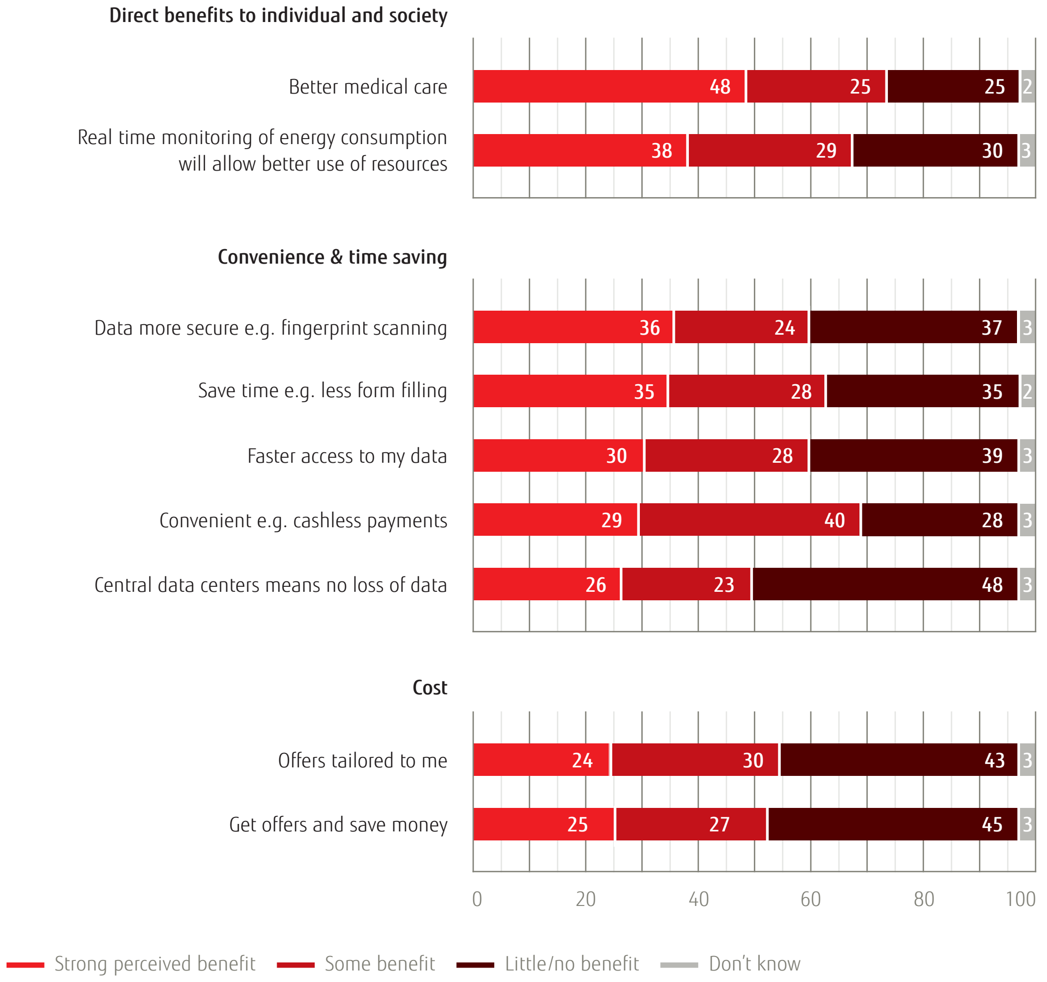
The other three scenarios were less attractive, with the negative consequences almost equal to, and sometimes outweighing, the perceived benefits. Biometric IDs – the commonplace use of fingerprints to access financial data and make purchases in shops – clearly smacked of “Big-Brotherness”, even in countries such as Singapore, where some forms of biometric information are already in use. While respondents could see some gains in terms of efficiency and security, there were concerns that the system would require a large, central database of information which would potentially be open to abuse and other risks. As we’ve already noted, the prime beneficiary of allowing governments to monitor how much people earn was thought to be governments themselves. Similarly, a personalized experience while shopping (adverts reacting to your presence) was widely seen as a thinly-disguised way for Big Business to make more money.

These attitudes became even more apparent when we asked about the type of uses to which data could be put in broad terms. Better medical care and more efficient use of energy were acceptable reasons for allowing organizations to access personal data, as were convenience and time saving, but to a lesser extent. By comparison, getting offers from companies tailored to our needs was not regarded as particularly attractive.

Our research indicates that the more a person sees a direct value to them as an individual from making their data accessible to others, the more likely they are to share it. Personal benefits matter most, but people also welcome applications which have wider benefits to society as a whole. Some commercial applications – such as when Amazon or Netflix make recommendations to us based on our past purchases and other people’s preferences – are recognized to be useful to both sides. But often, among those we spoke to, the value for corporations and governments was seen as inimical to the value for individuals. Indeed, the more an organization is likely to gain, the more people suspect that they will lose.

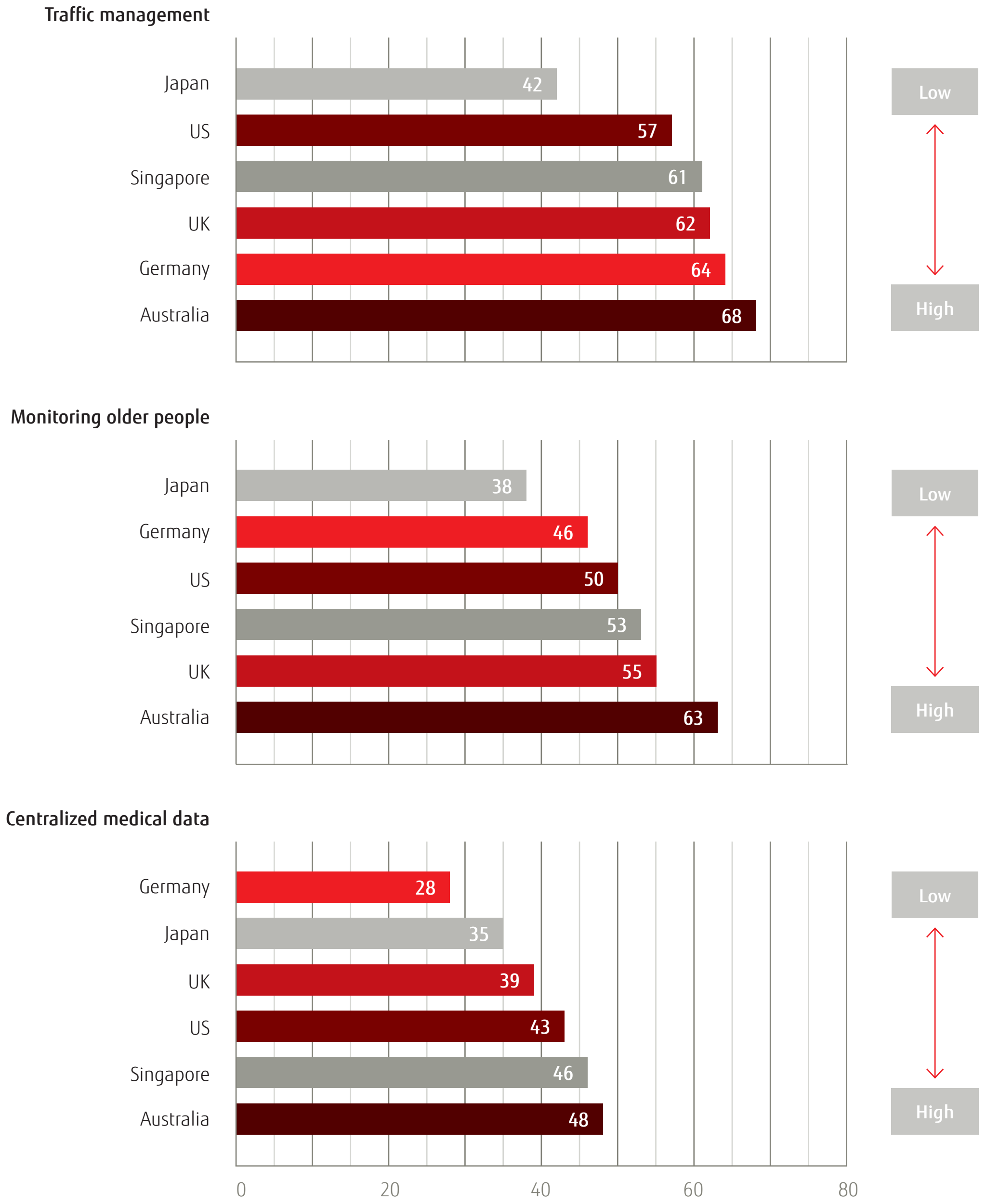
These differences vary from country to country. Australian consumers were the most positive about all the scenarios except having a personalized shopping experience (something that consumers in the US and Singapore were more comfortable with). German and Japanese consumers were generally more conservative, especially where their data would be used by business and governments.

Perceived benefits from allowing organizations electronic access to your information (in %)

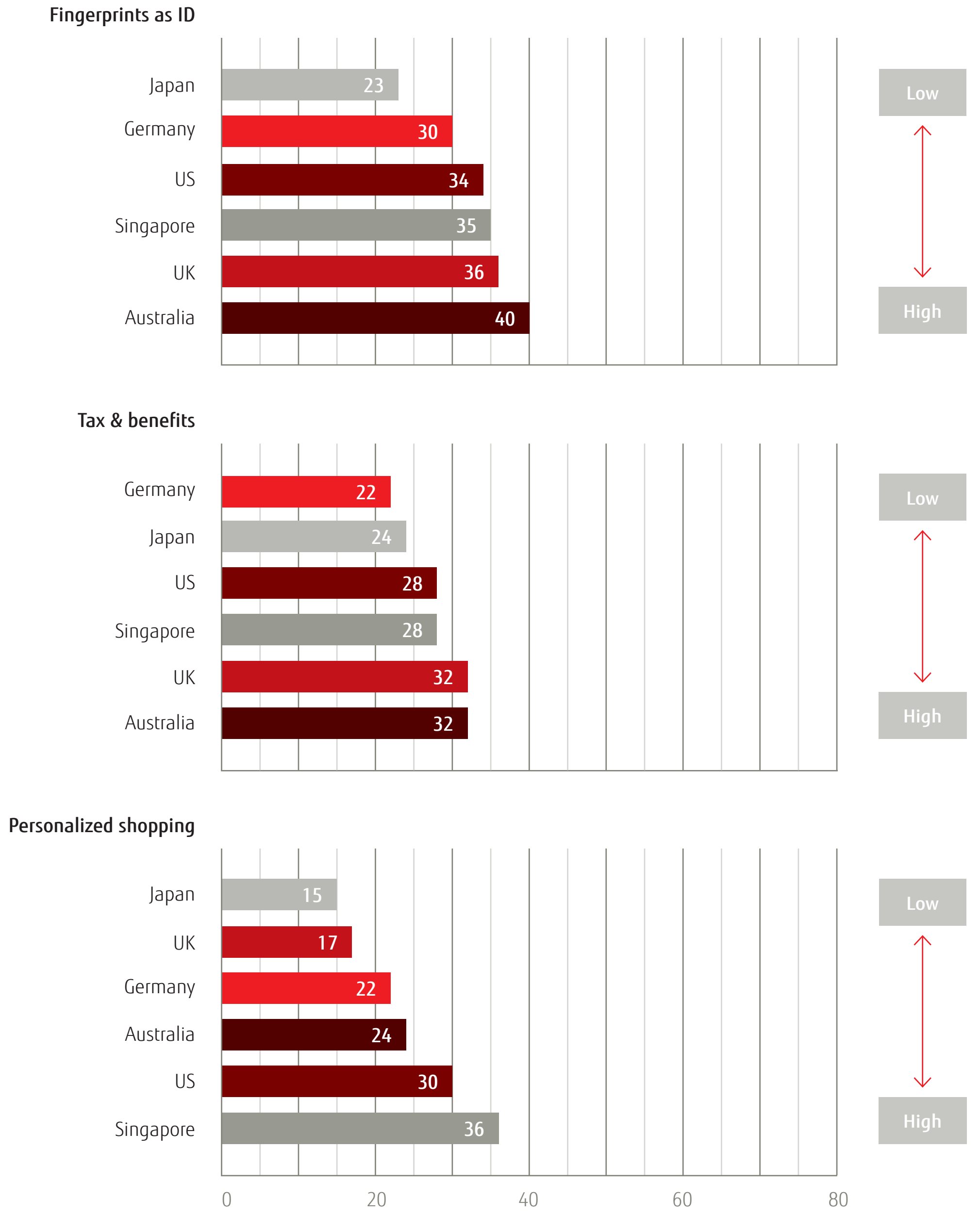


All this suggests that organizations – both private and public sector – need to think differently about the applications they develop based on cloud computing. Instead of looking at what’s in it for them (better data on consumer trends, more targeted promotions, etc.), they should consider how consumers will gain and how the perception of those benefits will vary depending on demographics and regional preferences. The most successful products and services, those with the potential to transform how we will live and work, will add value to both sides.

Consumers for whom benefits outweigh concerns for each scenario by country (in %)



Consumers for whom benefits outweigh concerns for each scenario by country (in %)



Deposit-box data

The risk of consumer inertia

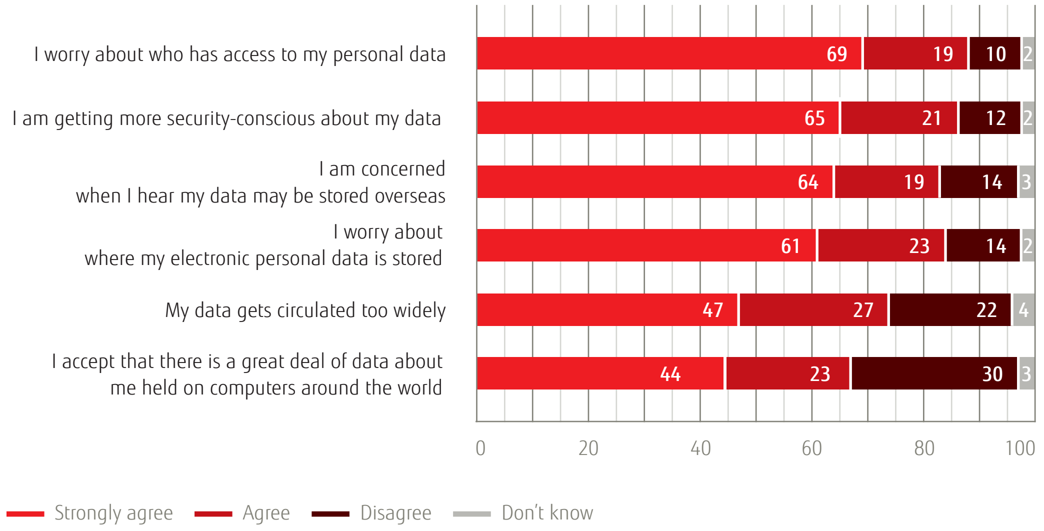
The recent financial crisis has shown consumers the perils of a financial system in which unimaginably vast quantities of money flow, apparently effortlessly, through the world's banks and investment companies. From their perspective, invisible transactions, made by unscrupulous bankers on the back of incomprehensible financial products, cost some people their money and everyone their sense of security. Our research suggests that people feel similarly powerless where their data is concerned, about where it goes and who uses it. Although most think that governments have a role to play in protecting their data, they're not convinced that regulation is the answer.

88% of those interviewed said they worry about who has access to their personal data, and 84% worry about where their data is stored. "Control is an illusion," said one Singapore consumer.

Current fears and concerns (in %)

Concerns about access to data

When prompted, 88% say they are worried about who has access to data and 84% worry about where their data is stored



"Every time new technology comes out, people become more reliant on it. Sometimes it moves too fast, and common sense and safety don't follow as closely. Are we safer than we were 1,000 years ago?"
US consumer

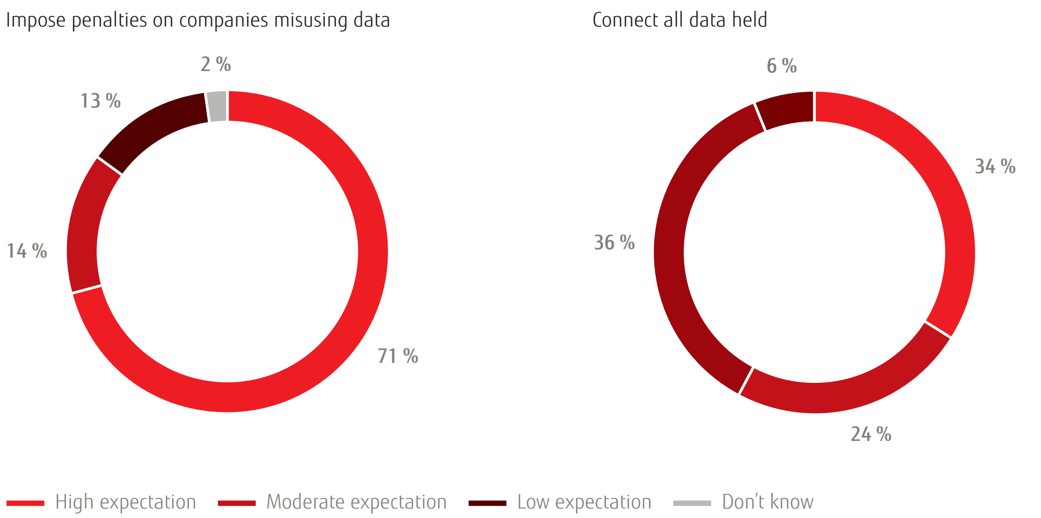
If anything, these figures underestimate the extent of people's fears. Few of those we questioned appreciated the potential mobility of data, i.e. the possibility that, when they buy something online, their data may be sent from retailer to manufacturer to delivery agent, or that their data may be held in other countries. China, Russia and India were considered insecure locations by three quarters of those surveyed. People want to keep their data close to home, both literally and metaphorically. Switzerland was seen as the safest place to store data, but even then, 41% of respondents were very concerned about their information being stored there.

Ever increasing dependence on technology compounds people's fears, to a point where they see themselves caught between a rock and a hard place, forced into giving up their data while often reluctant to do so.

The assumption remains that governments have some responsibility here: 80% of respondents expect governments to play a role in policing the use of data. But this belief is undermined by lack of trust in both the competence and motives of governments. While most people recognized that national or, indeed, international institutions may be required to police the use of data, some questioned the ability of governments to do this, citing previous failures in security and new IT systems. Even greater was the fear that governments will act in their own interests, not their citizens'. While 85% expect governments to impose penalties on companies that break data privacy laws, only 52% seriously expect them to respect the privacy of people's personal data and only 34% want governments to take an active role in connecting data held about people in different places.

Role of governments

Over 80 % expect governments to legislate and regulate, imposing penalties on companies that don't use data responsibly

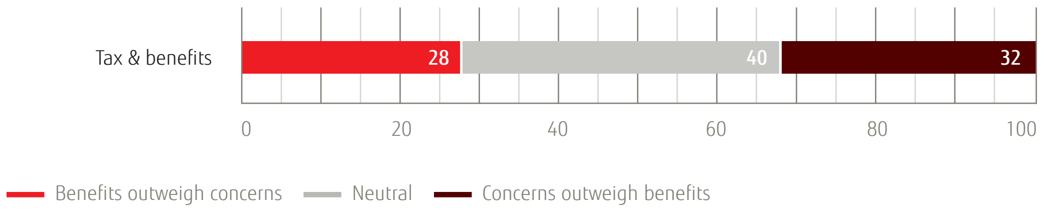

Impose penalties on companies misusing data

Connect all data held

"There needs to be some major deterrents for abuse: some major fines, some heads should roll."
US consumer

This reinforces what we learned from the six scenarios we'd asked people to consider. Questioned whether they'd like to see governments monitoring how much they earn and automatically taking taxes or paying benefits triggered very mixed responses. 32% of people felt the concerns outweighed the advantages, against 28% who thought the benefits more than offset the drawbacks. In other words, respondents felt governments should prevent abuse, rather than be active players in the information economy.

Trade-off of benefits and concerns (in %)

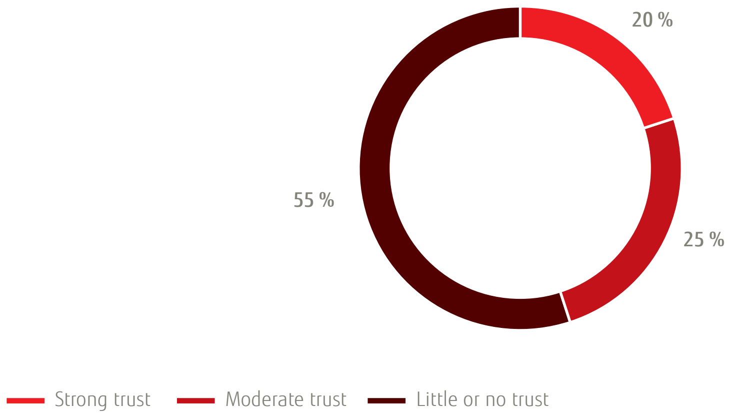


As with the perceived benefits of sharing data, attitudes to the role of government also varied around the world. German and Japanese consumers were most concerned with the notion that governments could be active agents, connecting individuals' data, but were also eager for governments to take responsibility for creating and maintaining robust data protection laws and imposing penalties on companies that break them. US consumers were generally less positive about government involvement, especially when it came to keeping people's data safe.

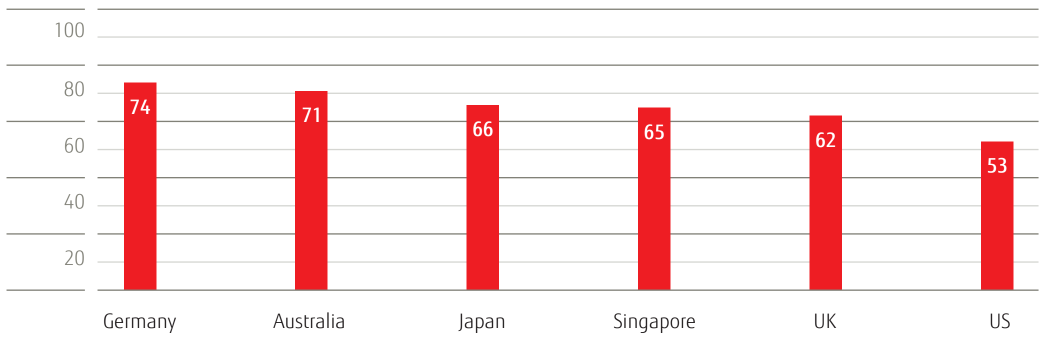
"Governments end up with too much information."
Singapore consumer

Trust of consumers in governments to look after their data (in %)

Only 20% of consumers have real confidence in governments to look after their data

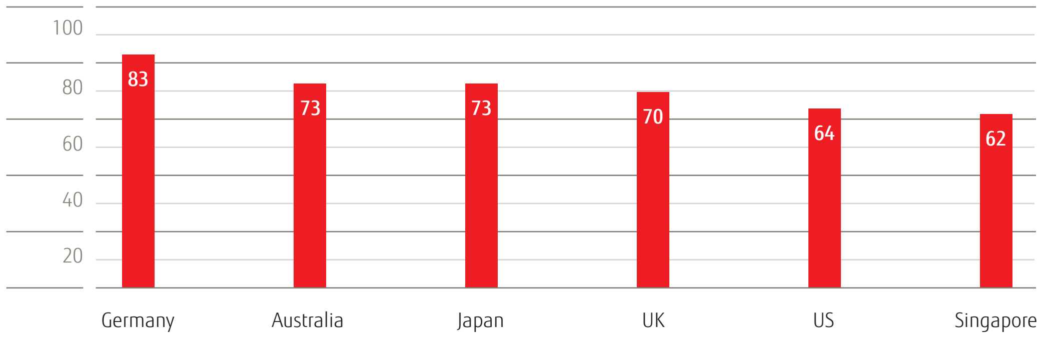


Roles and responsibilities (in % with strong expectation)
Role of government – regional view
Keep data safe and not lose it



Feelings where private companies are concerned are even more ambivalent. Consumers, especially women and older people, expect them to behave responsibly, using secure IT systems and providing guarantees that they won't pass data on to others. Expectations were highest in Germany, but significantly lower among US and Singapore consumers.

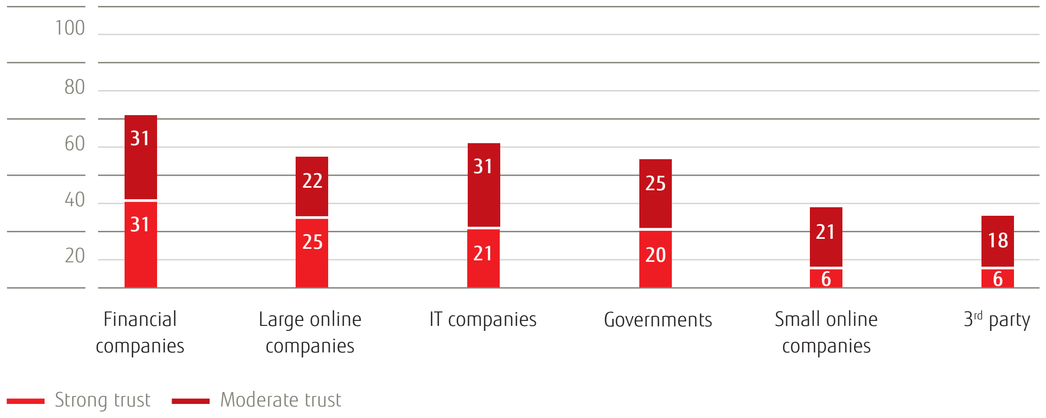
Roles and responsibilities (in % with strong expectation)
Role of companies – regional view
Use data in responsible way



But overall confidence is not high. "I won't like it if companies have too much of our information," commented one of the people we spoke to in Singapore. Despite the failure of the banking system, banks remain – grudgingly perhaps – the best in a set of bad options. Yet, even here, only a third of respondents said they really trusted their banks to protect and respect the privacy of their data. Bigger companies were generally considered more trustworthy than smaller ones; third parties, which process information behind the scenes, were the least trusted of all.

"History tells us that, when new technology appears, some people will profit from it. The question is who will profit from access to our data?"
US consumer

Trust of consumers in organizations to look after their data (in %)



The only people consumers trust to look after their data is themselves, but – and here's the crux of the problem – they don't believe they can do so effectively. "I cannot control who buys my data," commented a German interviewee. "Real, all-embracing security is impossible." Faced with the sense that this new society is beyond their control, people are virtually paralyzed, unable to take even the most basic steps to protect themselves. 94% of people questioned want companies to ask explicitly for permission to collect and hold their data, yet fewer than 50% always or regularly read the terms and conditions governing online transactions. "You haven't got any control over things. If you want the service, and that's the way the company holds and uses your information, what are you supposed to do about it?"

"Private companies say they'll protect your data, but we can't be sure they'll keep their promise."
Non-internet user

That so many people we surveyed were keen to see data privacy laws tightened also suggests that they feel there is no legal recourse when problems occur, a point brought out in interviews, even with regular internet users: "If someone breaches their terms and conditions, how are we going to seek justice from them?" said one.

"These clauses are here to protect companies, not you."
UK consumer

Regulation is, at best, only part of the solution. Consumers are just as concerned about the government's agenda as they are about that of private companies. Moreover, the significant variance in regional attitudes suggests that a single set of global rules governing data privacy will not answer all consumers' concerns. Governments and business need to take this into account and establish what it is that their citizens and customers are looking for, rather than assuming that one approach to data privacy will suit everyone.

Our research suggests that some consumers want the equivalent of the tangibility and security of a deposit box in a Swiss bank for their data. Other people, particularly the elderly and those less familiar with the internet, may simply throw away the key. Arguing that the risks of allowing access to their data are far greater than the likely benefits, they will opt out entirely. Most people, according to our research – will keep their key, opening their deposit box only when they choose to do so.

Drawing our own borders
How data defines who we are

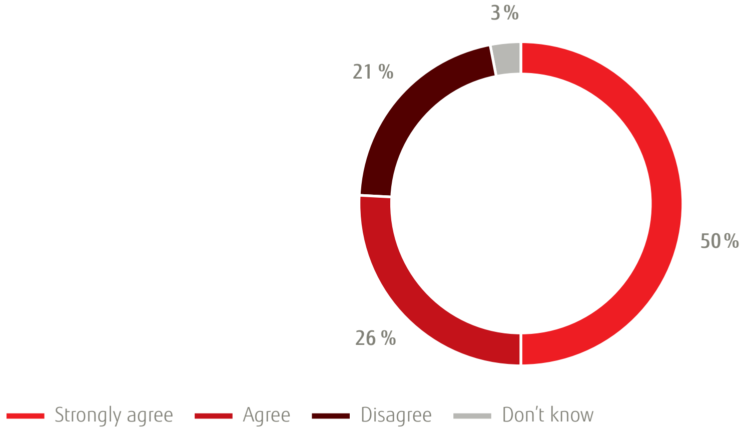
Unwilling to trust governments and corporations with their data, consumers want control, the ability to decide who gets their data and where it's stored. How they decide and the extent to which they are willing to share their data is, our research indicates, a very important and fundamental personal decision.

Our data defines us. "I don't want everyone to know everything about me," was how a German consumer put it. "I want to remain an individual." By giving away our data, we fear we're giving away a part of our identity and becoming part of a world in which everyone is the same. Our data, and who has access to it, also defines our relationships. We may have public personae on Facebook, LinkedIn and the like, but these are not necessarily our private selves. The people closest to us know most about us: if everyone knows everything, then no one is special. Many of the benefits of cloud computing stem from linking isolated pockets of data together and turning them into something new, so that the whole is greater than the sum of the parts. But will we, too, be subsumed into a society that no longer sees us as individuals? If we've given everything away, what's left behind?

"Social contact is lost. There will be no need to go out because everything will be done from home."
German consumer

Another theme that emerges from our research is that greater data availability may ironically make people more socially isolated. Elderly people who are monitored remotely will receive fewer visits from relatives; people who send in results of self-administered medical tests for analysis may not have the opportunity to speak to a doctor. "We'll rely more on systems than on people," said one interviewee. "It's the Age of the Robotic," said another.

People are becoming socially isolated as all communication will be done with computers and not people (in %)



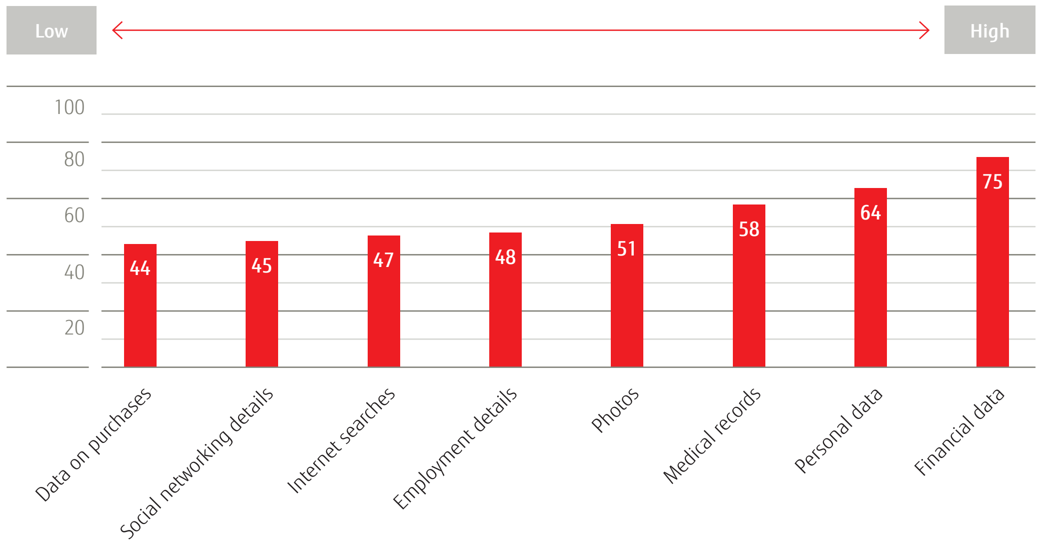
"Our generation is not phobic about new technology; if we feel it's ruining conversation, we'll switch it off. We're worried that the next generation won't be able to, because they're always thinking about something else."
UK consumer

Underlying this are issues relating to how we distinguish between the data we regard as personal and that which we don't. Not surprisingly, the people we spoke to are broadly more concerned about the widespread availability of and access to their financial, personal and medical data than they are about the details they put on social networking sites or information about their past purchases. So, we're not worried about where Amazon might choose to store information about our purchase data because we don't regard it as particularly personal, but many of us feel uncomfortable with the idea that our medical records may be stored overseas. Some data is global, but we want certain information to be held locally.

However, go beyond this and the responses are less intuitive. Why is it, for example, that financial data is seen to be more important than our medical records? Why are we, at least in relative terms, less concerned about our employment details being seen or accessed by others?

Level of concern about data privacy

% of respondents who said they were very concerned that the data should be kept private



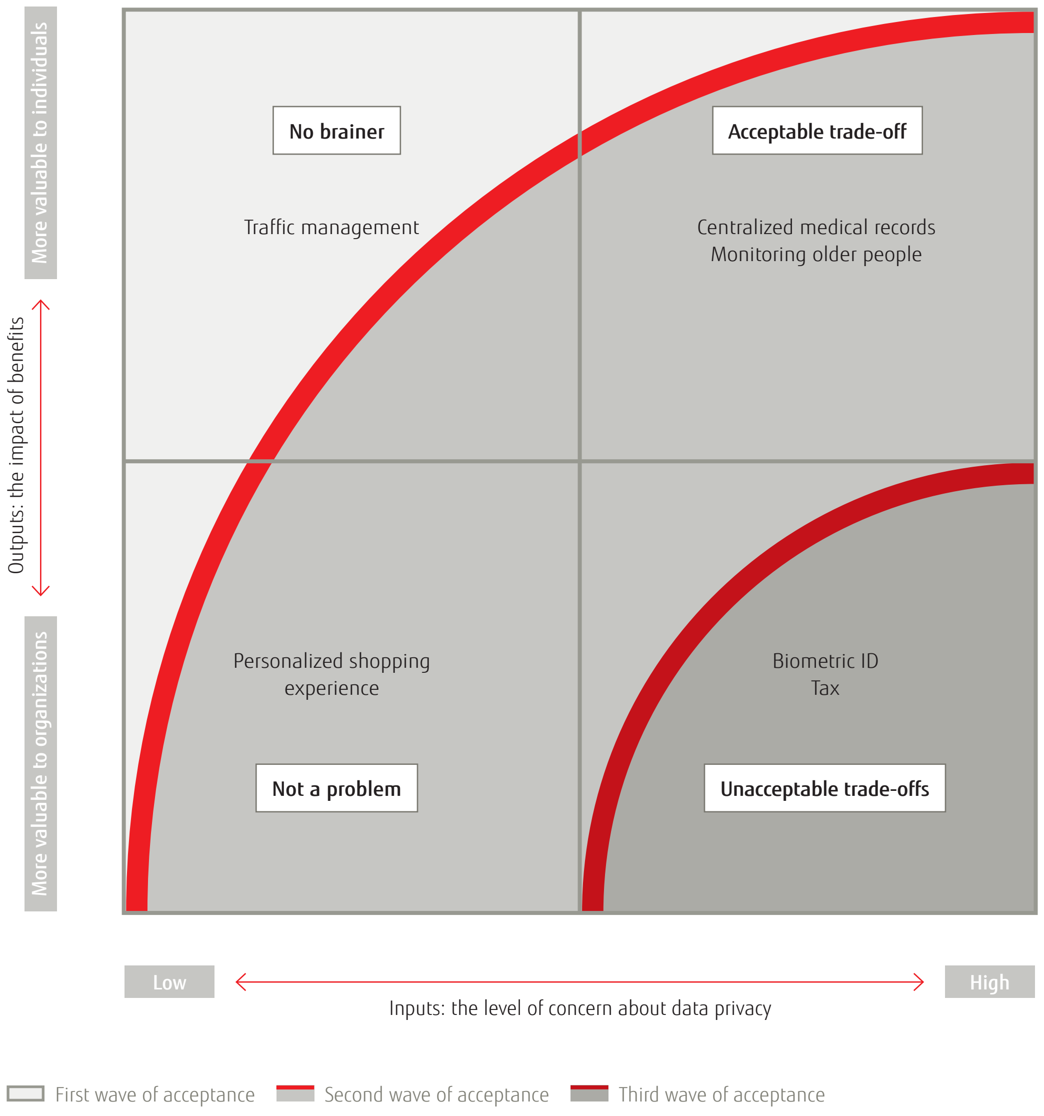
If we map, as is shown on the next page, the benefits of our six future scenarios against the level of concern people have over the data likely to be used in each, it becomes clear that the latter is not seen in isolation. We have, in effect, no single definition of what is personal and valuable, but a dynamic one that changes depending on who we are, where we live, and on the extent to which we think organizations – companies and governments – will exploit that information for their own ends.

This results in four categories of data use:

- No brainer: Intelligent traffic systems are potentially valuable, especially to people living in busy, urban environments, and they require little in the way of personal data. The first wave of cloud computing applications will be (indeed, already are) in this category.
- Not a problem: The applications in this category are seen to benefit organizations primarily; the gains for individuals lie in convenience. However, because the data required is non-invasive, such applications don't worry people especially. Consumers may not go out of their way to use them, but they are equally unlikely to resist them. Such applications are therefore likely to be in the second wave.
- Acceptable trade-offs: Centralized medical records and monitoring older people in their homes both require access to medical records. Although potentially invasive, people are comparatively comfortable with this approach because they and those nearest to them will benefit.
- Unacceptable trade-offs: These scenarios require people to give up data they regard as critical, largely (though not necessarily exclusively) for the benefit of governments and corporations. Resistance to such applications will be strongest here.

Map of data privacy trade-offs

Consumers are drawing borders around data-rich solutions



More valuable to individuals
Outputs: the impact of benefits
More valuable to organizations
No brainer
Traffic management
Acceptable trade-off
Centralized medical records
Monitoring older people
Personalized shopping experience
Not a problem
Biometric ID
Tax
Unacceptable trade-offs
Low
High
Inputs: the level of concern about data privacy
First wave of acceptance
Second wave of acceptance
Third wave of acceptance

91%

want a system which enables them to control how their data is used

People and organizations often want to get different – sometimes opposite – things from more readily available and accessible data. The types of products and services consumers push for (monitoring older people and centralized medical records) are not necessarily the ones in which organizations or governments see much value. Similarly, the uses the latter may be keen to exploit will meet – and already are meeting – resistance from people who simply don't see what's in it for them.

The key to squaring this circle – matching the needs of individuals to those of organizations – depends on choice, enabling consumers to choose the level of security they require, something that will vary according to:

- The circumstances of the individual (age, gender, familiarity with the internet, and so on)
- The type of data involved and the use to which it will be put
- The part of the world the individual comes from

"I like to decide, not others."
German consumer

Consumers are divided between those who feel in control (the younger and the more internet savvy) and those who don't (older, less regular internet users).

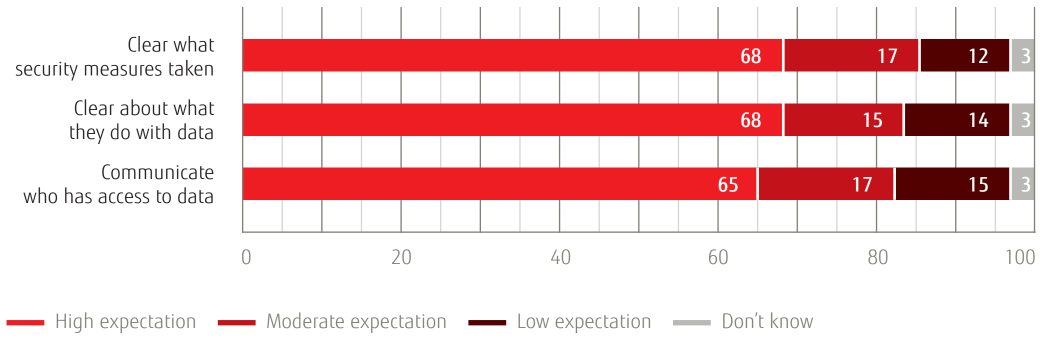
As noted previously, people are currently passive, or feel out of control when it comes to protecting their data. The fact that few people take advantage of the tools available to them – only a quarter choose passwords that are hard to crack and only 21% say they always read the terms and conditions when shopping online – could mean that there is no point in giving consumers and citizens further control. However, our research shows that there is almost universal agreement that people would like more clarity and simplicity in how they can control their data. 91% want a system which enables them to control how their data is used. 88% of people want simpler terms and conditions. Three quarters of people would like greater clarity about what an organization is doing to protect their privacy. If these needs are not met, we may risk the current passivity tipping into unwillingness to share data at all.

In releasing the social and economic potential of cloud computing and data sharing, the challenge for business and governments is to design a structure and provide the tools that put people in control, allowing them to see where their data may go and who has access to it, also giving them the power to accept or reject such options as they choose.

Our research shows that consumers are far more open to the concept of data sharing than they are often given credit for, but only where the benefits outweigh what they perceive to be the risks. Those trade-offs will vary from individual to individual and from country to country: some of us will choose to live in a virtually borderless world; others will want clear boundaries. The role of business and governments is to create the mechanisms that allow us, and not them, to make those choices.

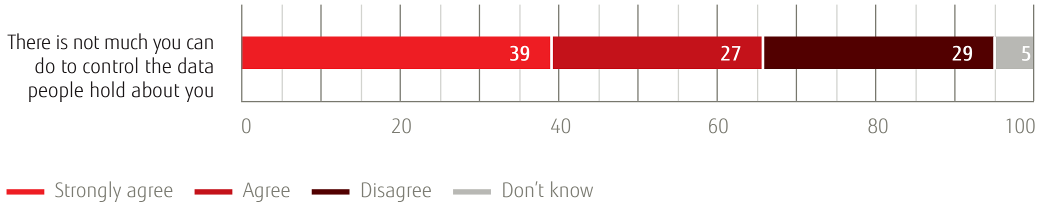
Consumers' expectations of organizations that gather data (in %)

As well as keeping their data safe, over 80% of consumers expect companies to communicate clearly about what they do with that data



Current fears and concerns (in %)

Concerns about access to data



This report was commissioned by Fujitsu Research Institute and produced by Fujitsu Global Business Group (part of Fujitsu Limited). It is based on data compiled as a result of a market research project undertaken by ORC International Limited on behalf of Fujitsu Global Business Group. All enquiries relating to this report should be addressed to Pernille Rudlin, Director of External Relations at Fujitsu Global Business Group (pernille.rudlin@uk.fujitsu.com).

The research was conducted from June to August 2010 using online bulletin boards, focus groups and quantitative research. Participants from Australia, Germany, Japan, Singapore, the UK and the USA were screened to ensure a broad sample in terms of age, gender and use of IT and technology. There were 500 respondents from each country for the quantitative research – 3,000 in total.

FUJITSU LIMITED
Shiodome City Center, 1-5-2 Higashi-Shimbashi
Minato-ku, Tokyo 105-7123, JAPAN
Tel. +81-3-6252-2220
www.fujitsu.com