The trust factor in the cognitive era

How CSPs can capitalize on personal data while preserving privacy

IBM Institute for Business Value

IBM communications industry solutions

More than ever, communications service providers need to rely on the latest solutions related to cognitive computing, analytics, cloud, mobility, network optimization, digital transformation and global integration. IBM has an extensive global network of telecom solution labs, research labs and innovation centers to support its industry offerings. With more than 22,000 subject matter experts working in the communications industry, we work with more than 200 major communications service providers across the globe. IBM continues to invest significantly in key acquisitions to add expertise and capabilities that enable clients in this industry. For more about IBM communications solutions, visit **ibm.com**/communications.

Three fundamentals: transparency, value exchange, security

Digital trust has become a key factor in the depth of relationship between consumers and their providers. Recent well-publicized data hacks and security breaches have humbled even mighty companies, leaving their reputations in question and their balance sheets damaged. Communication service providers (CSPs) have the luxury of being among the most trusted organizations for personal data security by consumers. But a single security lapse can seriously erode that trust. For CSPs to maintain their privileged position and capitalize on the trust consumers place in them, they must understand customer mindsets and focus on three specific fundamentals: transparency, value exchange and security.

Executive summary

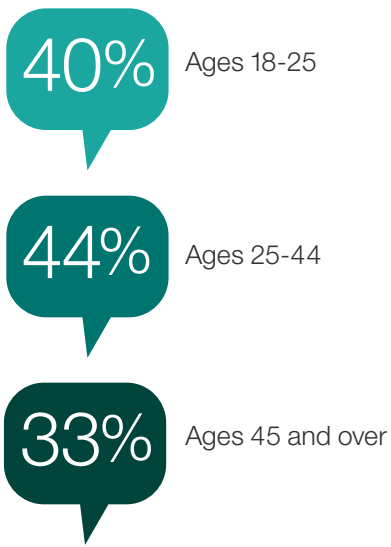
Personal data is the new currency of the digital economy. Generating insight from personal data can bring tremendous benefits to both individuals and organizations – but at ever-increasing risk. As more data is collected and transacted, the likelihood of a breach escalates. Cyberattacks are increasingly common, filling consumers with unease about the privacy and security of their personal information.

Trust in the organizations that collect and maintain personal data is decreasing, particularly in mature markets. Consumers are caught in the middle between organizations that need (or want) their data for mutual benefit and malicious forces that want to steal it. Customers say they want more personalized experiences from their providers, and CSPs, in return for loyalty and wallet share, are striving to provide high levels of personalization and intimacy. But for this to work, enormous amounts of personal information must be gathered, analyzed and secured. This is where trust can become a game changer.

IBM Institute for Business Value research highlights the strong trust position CSPs occupy among consumers. Four key insights provide guidance on the development of strategies to capitalize on this trust:

- In emerging markets, CSPs are the most trusted organizations by consumers for handling personal data. In mature markets, CSPs are second only to banks/credit card companies.
- Digital natives are more comfortable with CSPs handling personal data than individuals over 45.
- Among the four tiers of trust (high, moderate, neutral and low), CSPs in the top two levels enjoy significant advantages in monetization and growth.
- To optimize the trust equation, CSPs need to manage the yin and the yang of three primary customer mindsets (consistently trustful, increasingly suspicious and trustful-but-worried) and three trust imperatives (transparency, value exchange and security).

Consumers who said they were comfortable sharing personal data with their CSPs



But CSPs' strong brand equity is at stake if they fail to keep personal and corporate data secure. The potential damage to brand image could be more of an issue than any financial damage. Customers feel violated and deceived when their personal data is compromised. Once such trust is lost, it is nearly impossible to regain. When such brands fall out of public favor, their value also decreases significantly to potential ecosystem partners.

To increase trust levels, as well as the resulting potential revenue opportunities, CSPs need to understand the various levels of trust consumers place in organizations, as well as the contributing factors that define trust: transparency, value exchange and security. This knowledge will allow CSPs to develop initiatives and services that promote increased trust, identify partners that can help them deliver these services, and adopt the technologies necessary to establish transparent, private and secure environments.

To identify the factors that influence digital trust, as well as develop insights that can help CSPs capitalize on it, the IBM Institute for Business Value surveyed nearly 21,000 consumers in 42 countries, representing 73 percent of global population and 90 percent of global GDP.

Personal data: the new currency of the digital economy

The volume of personal data collected by organizations is considerable and growing. In addition to official records, demographic data and information voluntarily provided, people also, often unknowingly, leave digital footprints – browsing history, location data, social media activities, online purchases and more. Increasingly, data collected from smart devices and the IoT are becoming part of this footprint. For example, navigation apps can show where a person has traveled. Connected cars reveal driving habits. Smart utilities can record the activities of a person at home.

For CSPs and consumers, there is tremendous value in the ability to aggregate and analyze all this personal data and, most important, be able to create insights that enable its profitable use. (see Figure 1).

But personal data is vast, diverse, complex and continuously changing. Most data is unstructured and invisible, such as that hidden in videos and sensors. Traditional analytics cannot fully extract the value of this data. Cognitive computing technology is a key enabler to unlock the full value of unstructured data, which accounts for about 85 percent of all data generated (see sidebar on page 4).

Figure 1

Tremendous untapped value lies in the ability to aggregate and analyze personal data

Source: IBM Institute for Business Value 2017

Sidebar: Cognitive computing

Cognitive computing technology provides more detailed insights from personal data than traditional analytics solutions can deliver and creates increased value for both customers and organizations (see Figure 2). Cognitive systems can:

- Handle large volumes of both structured and unstructured data
- Learn actively from things, context, and the way people interact with them
- Adapt and evolve to be more useful and robust over time
- Relate insights in easily understandable ways, such as natural language/dialog, text and visual cues.

Figure 2

Cognitive solutions often provide insights beyond those of standard analytics

Source: IBM Institute for Business Value 2017

Monetizing personal data has become the new battleground, something the Internet giants clearly understand, as evidenced by top Internet companies in market value as of 2016, such as Apple, Google, Facebook, Amazon and Alibaba.[1] These companies maintain huge repositories of customer data, often generated by consumers when they visit their web sites. The importance of data is illustrated by the large sums paid to acquire organizations that maintain vast amounts of personal information, such as WhatsApp, bought by Facebook, and LinkedIn, purchased by Microsoft.[2] However, our study shows that CSPs have a trust advantage over these global over-the-top players (OTTs), which provides a tremendous opportunity to grow into new services and markets.

CSPs enjoy a strong consumer trust position

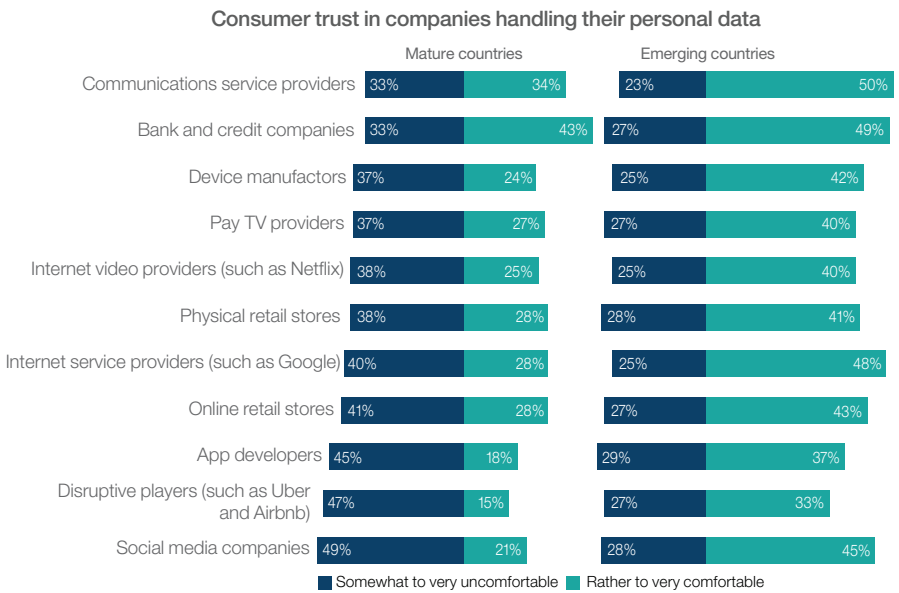
Consumers are increasingly concerned about data privacy. Media coverage fuels this worry with frequent reports about companies, institutions – and even governments – abusing personal data. The volume and severity of data breaches and abuse continue to increase. With more and larger breaches in the news, consumers have become worried about – and suspicious of – the organizations that collect, store and use their data. Fortunately, CSPs, globally, trail only bank and credit card companies in the degree of trust consumers place in them. (see Figure 3).

CSPs, while scoring high overall, tend to fare better in emerging countries, where they top even the bank and credit card companies. At the bottom in trust for mature economies are social media companies, while disruptive players, such new online transportation and lodging entities, are among the least trusted in emerging nations.

Of course, the notion of trust in organizations further varies across individual countries. For instance, in Greece and Italy, consumers rate CSPs significantly above banks, while in such countries as Egypt, Saudi Arabia, Indonesia, Philippines and Thailand, internet service providers (such as Google) and social media companies (such as Facebook) are first and second, above CSPs.

Figure 3

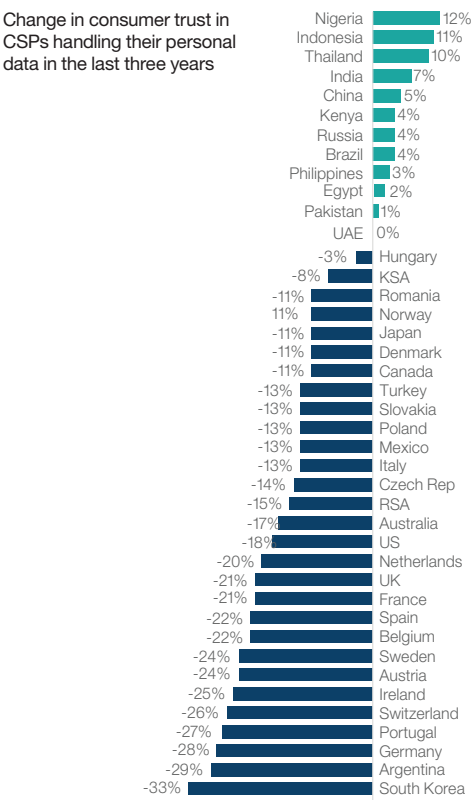
CSPs are among those companies that consumers trust most to handle their personal data



Source: IBM Institute for Business Value 2017

Figure 4

Consumers' trust in CSPs has decreased in all mature countries surveyed; however, trust has increased in many emerging countries



Source: IBM Institute for Business Value 2017

Trust varies by age as well. Globally, 40 percent of consumers in the 18-25 age group in our survey indicated they feel comfortable sharing personal data with their CSPs. For the 26-45 group, the number grows to 44 percent. However, only 33 percent of those over 45 said they trust their providers.

Over the past three years, trust has declined across the board for all organizations that handle personal data. If there is a bright side to this for CSPs, it is that their decline in trust is less than all other surveyed industries: 12 percent average decline across all 42 countries surveyed. And in many emerging countries – representing more than 4 billion people – trust in CSPs even increased (see Figure 4). The primary concern of consumers (60 percent in our survey) is that CSPs might sell their personal data to third parties without their consent. Forty-five percent were concerned their data might not be secure, and 35 percent were concerned about how much their providers knew about them.

Capitalizing on personal data and preserving privacy

Assessing the relative levels of trust consumers have in their CSPs enables a four-tier categorization of trust (see Figure 5). The CSPs in Level 1, interestingly, are primarily from emerging markets and have been leading expansion into areas such as payments and higher value-added services. Additionally, relative trust in banks is lower in those markets than in mature markets.

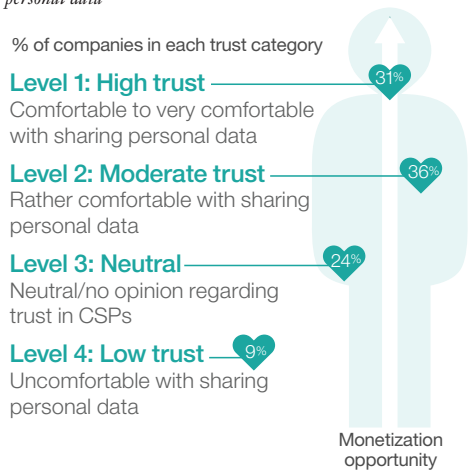
Personal data services seem to generate growth among the high-trust band of companies, which account for 31 percent of the operators in the 42 countries we surveyed (see Figure 5). In this band, a number of CSPs have been able to launch successful mobile money and mobile commerce services. For many, these services are key differentiators. Examples include CSPs such as Telkomsel (with TCASH), XL Axiata (XL Tunai), MTN (Mobile Money), Etisalat (GTEasysavers) and Vodafone India (MPesa).[3] Other CSPs find lifestyle apps enhance trust. Examples in this category include Globe (G-Apps) and Smart (Smart Life).[4]

CSPs are at the heart of their customers' digital universe, which also includes social media, IoT and activities in adjacent industries. Three principal growth opportunities exist for CSPs to use their competencies and assets related to personal data:

- *As a digital services provider* – Offering customer-defined and experiences-led services to their customers, thinking digital first, and driving almost all interactions online and across devices, with the customer at the center. This allows real-time personalized and contextual actions that are both agile and data-intelligent.[5] Continued focus in improvement in customer experience and Net Promoter Score (NPS) should further enhance the trust position.
- *As a data provider* – Earning revenue by providing anonymous personal information to third parties. Belgian Telco Proximus, for example, has launched a new big data service, called MyAnalytics, to provide anonymized user location data to third parties, such as local authorities, enterprises and event organizers.[6]

Figure 5

Highly trusted CSPs enjoy significant advantages in monetizing personal data



Source: IBM Institute for Business Value 2017

- *As a digital services enabler* – Curating a trusted ecosystem for IoT and third-party applications/services, allowing them to develop personal data-based apps and services. Axiata's WSO2 API-based platform, for instance, provides a simple and cost-effective way to quickly integrate customers, partners, internal and external systems, and services in a connected, secure, adaptive and collaborative business ecosystem.[7] Leveraging a high consumer trust position within local market ecosystems can enable CSPs to improve margins, as partners also value trust.

Pursuing these personal data opportunities is not without risk, however. Data breaches/hacks and legal liabilities/regulatory environments are among the challenges that most frequently make the news. Across the United States and the United Kingdom, for example, telcos have been fined because they failed to prevent cyberattacks or used cookies to track the websites that were visited by their customers.[8]

Uncertain business models, time-to-market/agility, unclear ROI investments and vague partnership concepts are just a few of the numerous factors CSPs must address if they are to take advantage of their personal data opportunities. The biggest risk of all, however, is losing consumer trust. Privacy issues, arising from the extensive use of personal data, also could undermine the trust individuals place in CSPs.

Trust: the battleground for competitive advantage

Gaining – and keeping – digital trust is the prerequisite for any organization that wants to capitalize on personal data to create value. Trust in a company gives customers the feeling their data is in safe and secure hands and increases willingness to share information, even if just minimal value is offered in return. Further, trust motivates spending and loyalty and enables the CSP to offer more relevant revenue-generating services and applications.

Understanding the yin and yang of customer mindsets and trust imperatives is the key to increasing trust and subsequent improvement in monetization opportunity (see Figure 6).

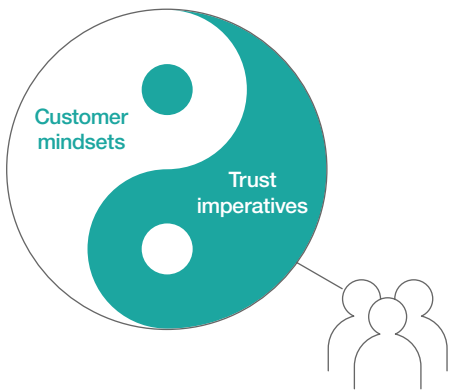
The differing customer mindsets about trust

Consumers, according to their answers in our survey, can be segmented into three distinct trust mindsets according to their perceptions and actions about data sharing. These mindsets reflect how willing consumers are to share data and whether they take defensive actions to avoid giving away personal information:

- *Consistently trustful* – This group is worried, but not alarmed. They understand the seriousness of data breaches, but do not believe the situation is as bad as media coverage implies. This group tends to be a bit lax in protecting against abuse of personal data.
- *Increasingly suspicious* – This segment is very suspicious about how CSPs handle personal data and are not certain the data can (or will) be kept secure. Increasing media attention to data hacks and cyberattacks – as well as the potential of big data and Deep Packet Inspection (DPI) to enable CSPs to know so much about customers– result in even less trust. This group goes to significant length to protect access to data, such as deleting or blocking cookies and using different web browsers.

Figure 6

CSPs need to manage the yin and yang of customer mindsets and trust imperatives



Source: IBM Institute for Business Value 2017

"The mobile industry has a privacy 'obligation.' Mobile operators must keep the protection of subscriber privacy at the forefront of their thinking."

Former Director General of GSMA

- *Trustful-but-worried* – This group is the most positive about how they can benefit from sharing data. They have a high trust in CSPs, and this trust continues to grow. They say they benefit from data sharing by getting better services, products or experiences. However, they worry about how CSPs handle their data and are concerned that CSPs will sell their data to third parties. As a result, they try to control access to their personal data as much as possible.

Each of these segments takes a different view about the relative importance of the three pillars upon which digital trust is built: transparency, value exchange and security. CSPs must evaluate how the different mindsets value these trust attributes and respond accordingly.

The three imperatives of trust

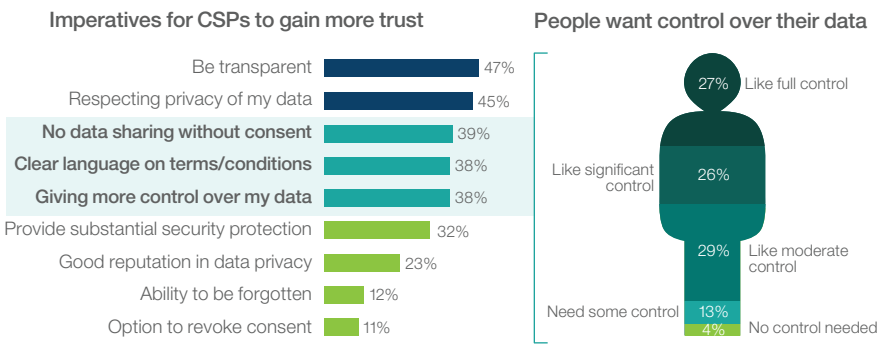
Transparency

Most of the respondents to our survey have only limited knowledge about what types of personal data are collected and how it is used. Further, 64 percent of respondents indicated that finding out what data is collected and used is at least moderately difficult.

With such difficulty, it should come as no surprise that respondents cited transparency as the top driver in building trust (see Figure 7). Customers want to know how their data is used and by whom.

Figure 7

Transparency and privacy are the two primary drivers to build trust. People also want more control over their data.



Source: IBM Institute for Business Value 2017

Case study – Telefónica's personal data bank[9]

Telefónica has announced that it will create a personal data bank for each of its 350 million customers to store, manage and sell their own data. The operator wants to give customers back control of the data they generate on its networks. A simple traffic-light tool will expose how third-party Internet applications and services propose to use data, while customers will be able to choose to cash-in personal data by selling it to third parties.

In our survey, 38 percent of respondents reported they regularly experienced instances in which their data was used for something for which they did not agree or which they did not authorize. Twenty-two percent indicated this happened often or very frequently. Only 12 percent said they had never experienced such an event.

Consumers in our survey said it is important that providers tell them what personal data is collected and how it is stored and used. However, there were some differences among the three customer mindsets, with 45 percent of the increasingly suspicious, but only 29 percent of the consistently trustful, saying this is extremely important to them. In addition, the sense of having no control over their data is one of consumers' growing concerns. Fifty-three percent of overall respondents say they would like significant-to-full control over the data they share, possibly using a browser or an app. They want control over whom they share data with, how they share it, as well as what they get in return.

Consumers clearly want the ability to opt-in for location access; otherwise, they are likely to see it as a violation of their privacy. Some CSPs have already taken steps toward creating personal data banks to give customers more control over their data (see case study).

Transparency recommendations

Give your customers control over their personal data – Offer them tools, in the form of a browser or app, to let them understand what happens with their personal data – the data you collect and the data collected by your partners – and to give them effective control over the management and use of their personal data. This enables them to actively participate in the ecosystem.

Be clear to your customer about your opt-in, opt-out policy – If you use the opt-in approach (preferred by most consumers), then allow customers to change their minds at any time and revoke access to their data. If you use the opt-out approach, make that clear to your customers and provide them with information about how to opt-out. In either case, make it easy for customers to decide and change.

Be open about your data policies – Make privacy policies part of your organization's brand image. Build transparency into the design of services and products.

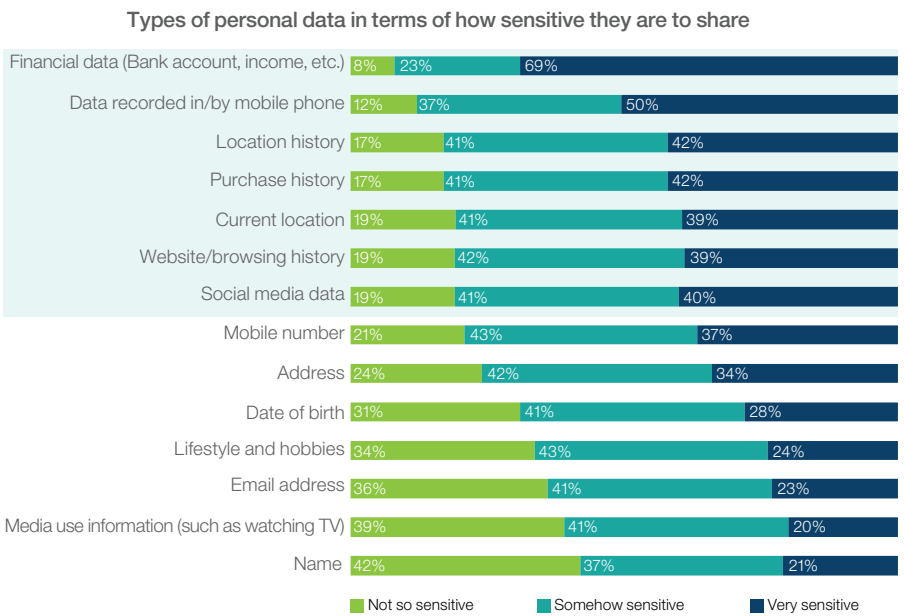
Value exchange

Offering a fair value in exchange for personal information, and making the exchange transparent, is a key element in building trust. A mutually beneficial arrangement allows businesses to gain data they (or third parties) can use to better understand, service and/or target consumers. In return, the customer should receive something of value, such as superior service or a financial reward. However, consumers say they are often not adequately rewarded for use of their personal data. According to a European study by French CSP Orange, 67 percent of consumers believe the organization benefits most from gathering information about customers. Just 6 percent think that the consumer is the "winner," while 16 percent believe benefits are equal.[10]

Consumers value personal data based on the type of data and how it is used. Data held by commercial organizations and institutions (such as banks and healthcare organizations), as well as digital footprints, are considered most sensitive (see Figure 8). Consumers require more return value to share these types of information.

Figure 8

Data held by commercial organizations ot generated by digital footprints is considered most sensitive; consumers require more value to share this information.



Source: IBM Institute for Business Value 2017

To facilitate willingness to share personal information, individuals must understand how they benefit from it. Examples are:

- *Improved service or experience* – Consumers generally feel the enhancement itself is a fair trade for their data
- *Free or discounted products/services* – Many people desire apps or content in exchange for personal information
- *Recommendations for products, apps, content and services* – Recommendations based on their data and analytics are usually appreciated
- *Targeted offers or advertising* – Many consumers do not see this as a value exchange and would rather avoid advertising messages
- *Part of the value from selling to third parties* – In general, consumers will expect more value in return for personal data sold to third parties
- *Compensation in other forms* – Many consumers just want a reward in the form of a discount, cash back or a coupon.

Most consumers want to have a lower-priced product or service in return for their data. However, our survey revealed that a number of customers, particularly those aged 45 and above, prefer to pay for products/services, rather than allow use of personal data (see Figure 9). This is certainly true for the consumers with the suspicious mindset; their preference is not to share any personal data.

Value exchange recommendations

Use cognitive analytics to understand what customers value – Invest in cognitive analytics to develop real-time contextual insights by tapping into behavior patterns, trends and sentiments from both structured and unstructured data.

Case study – BMW's driver assistant[11]

BMW has started a project exploring the use of cognitive technologies in vehicles to better personalize the driving experience and create more more intuitive support systems. The conversational and machine learning capabilities of cognitive systems offer opportunities for vehicles to learn about personal preferences, needs, and driving habits of their drivers over time, making the safest and most comfortable driving experience possible.

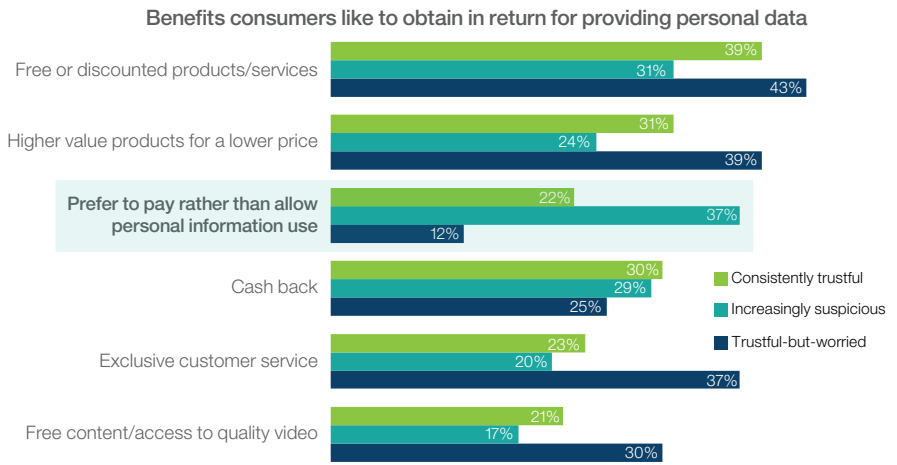
The driver can interact in natural language, for instance asking for the best route if he needs to make a couple of stops on his way home from the office. The solution will also include data from the Weather Company, as well as real-time, contextual updates about route, traffic and vehicle status.

Deploy a trusted API-based ecosystem platform to bring in value-added services from partners – Enable third parties to access core CSP capabilities to develop personal data-based apps and services, that give customers real value for the data they share.

Clarify to customers the benefits they receive in exchange for sharing personal data – Shift from a one-way data-collection mindset to a two-way transaction or "fair-value" exchange approach. Share personal insights with the customer. Stop using data from customer groups that see no or negative value from these CSP practices.

Figure 9

Consumers with suspicious mindsets prefer not to share any personal data



Source: IBM Institute for Business Value 2017

Security

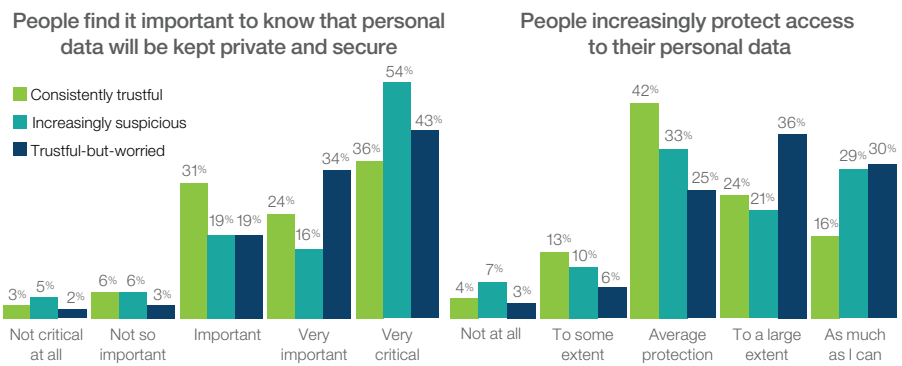
Cyberattacks are becoming increasingly common and often make headlines. Consider, for example, just a few from 2016: data stolen from a billion customers, Caller ID apps exposing 3 billion names and numbers from users, stolen customers records even put up for sale and more.[12]

Consumers are increasingly concerned about the protection of their data, and it is vital to CSPs for them to know how security is guaranteed. This is particularly true for both older customers and those of the suspicious mindset in our survey, with 50 and 54 percent of them, respectively, indicating knowledge of data security is very critical (see Figure 10).

Most consumers surveyed said they believe many organizations misuse their personal data on the Internet, and many have taken protection measures themselves, blocking cookies, using different browsers, opting out where possible and using advanced online tools.

Figure 10

More suspicious customers need to know that CSPs keep their personal data private and secure; they also protect access to their data



Source: IBM Institute for Business Value 2017

Sidebar – IoT security

As the IoT market size increases, hackers have an expanded surface area, and protecting customer data is more urgent than ever before. The IoT devices could be used to harvest huge amount of personal information. However, at the same time, hackers have the potential to completely disturb society by abusing personal data stored on connected devices. Securing multiple points of vulnerability, whether a smart watch, a healthcare device or a smart TV in an individual's home, is fundamental for the success of the IoT. Security is a cooperative initiative in the IoT ecosystem, in which the CSP can play a central role.

Blockchain technology enhances security[13]

The Internet was originally built on trust, but all the data breaches and cyberattacks have made that a thing of the past. With the ever-expanding IoT, it is more important than ever to secure personal data handling and privacy. It is key to move from a "security-through-obscurity" (closed source) approach to one that is based on transparency.

Blockchain offers a potential solution by enabling private and secure personal data handling. The blockchain is a decentralized public ledger of transactions that no one person or company owns or controls. In addition, the technology can secure a company's network by placing the identities of all authorized users in the blockchain ledger, which continuously verifies them. As a result, it is better able to withstand malicious intrusions and provide users control of all their information and transactions. The technology also allows for ecosystem simplification.

CSPs are already exploring applications of blockchain technology. Orange Digital Venture – for example – invested in U.S.-based start-up Chain, which is developing blockchain solutions for the financial industry and other transactional services, such as mobile money.[14] Du, in United Arab Emirates, announced a pilot program to facilitate the secure transmission of electronic health records using blockchain technology.[15]

Although CSPs are among the most trusted companies with personal data, they have not escaped unscathed. A number of companies in the United States and Europe experienced data compromises of one sort or another. CSPs remain accountable for any lapses in protecting the personal information they maintain about their customers. Potential penalties include the loss of customers, fines, litigation cost, drops in share price and damage to reputation.

Security recommendations

Radically transform practices for security in the Cloud - Continue to invest in cloud-secure technology, to provide optimal security protection for customers and to improve defenses against threats

Access the potential of blockchain technology – Use blockchain technology to deliver a single authoritative entity for trust. It can, for example, add new mobile payment capabilities to enable autonomous transactions within IoT platforms, and to help solve issues of identity.

Use cognitive technology to identify security threats – Deploy cognitive security systems to analyze vast amounts of structured and unstructured data to provide insights into emerging threats, as well as recommendations on how to stop them

Educate your customers about securing their personal data – It is not sufficient to present them the terms and conditions of using data, it is important to educate them in security best practices about their personal data.

Are you ready as your customer's most trusted partner?

- Do you know where you sit as a trusted provider in your market relative to your competition and to other organizations, such as banks, OTTs?
- Do you understand and segment your customers in terms of the trust mindsets? Do you know the value of this trust and how to monetize?
- Are your strategies and initiatives to increase trust in line with the monetization opportunities in your market?
- Is your security strategy and performance rock solid to prevent trust erosion?

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for phone or tablet from your app store.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Global Business Services, develops fact-based strategic insights for senior business executives around critical public and private sector issues.

About the authors

Bob Fox is the Global Industry Leader, Telecommunications and Media & Entertainment (TME), IBM Global Business Services. He is responsible for managing IBM's consulting business, developing business consulting strategy, advancing global client relationships and providing industry thought leadership. Bob has spent 30 years advising CSPs around the world about business strategy. He can be contacted at robertfox@us.ibm.com.

Nick Gurney is the Communications Sector Leader for IBM Asia Pacific. He has 25 years of experience working with CSPs around the world, particularly on transformation initiatives. Nick is a member of the IBM Industry Academy, an Industry Eminence team composed of circa 150 executives from Sales, Services, Technology and Research around the world sponsored by IBM's Chairman. He can be contacted at nick@au1.ibm.com.

Mario Cavestany leads the TME industry for IBM Europe to support telecommunications, media and entertainment companies facing today's challenges to transform into digital services providers and to run more agile and leaner operations. Mario has 30 years of experience in the TME industry in Europe and Latin America and is a member of the IBM Industry Academy. He can be contacted at m_cavestany@es.ibm.com.

Rob van den Dam is the Global TME Industry Leader for the IBM Institute for Business Value. He leads strategic thought leadership in TME and is a contributor to the IBM global telecom strategy. He has 25 years' experience in this industry and has worked in a range of advisory and implementation roles for major TME organizations. Rob has published multiple articles in leading telecom magazines. He can be contacted at rob_vandendam@nl.ibm.com.

Notes and sources

1 "Market capitalization of the biggest internet companies worldwide as of May 2016 (in billion U.S. dollars)." Statistica: The Statistics Portal. 2016. https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/

2 IBM Institute for Business Value analysis, based on publicly available information

3 Fox, Bob, Nick Gurney and Rob van den Dam. "Outthinking disruption in communications: The 2020 CSP in the cognitive era." IBM Institute for Business Value. February 2016. http://www-935.ibm.com/services/us/gbs/thoughtleadership/2020csp/

4 ibid

5 Ibid

6 "Proximus starts selling customer data reports for €700 a time." European Communications. November 22, 2016. http://www.eurocomms.com/industry-news/11968-proximus-starts-selling-customer-data-reports-for-700-a-time

7 WSO2 website. http://wso2.com/about/news/wso2.telco-launches-open-source-api-platform-for-telecom-operators/

8 Riaz, Saleha. "Verizon hit with $1.35M fine for use of supercookies." Mobile World Live. March 8, 2016. https://www.mobileworldlive.com/featured-content/home-banner/verizon-fined-1-35m-for-use-of-supercookies/

9 "Telefónica to create personal data bank for customers, expose "unfair" apps." European Communications. November 9, 2016. http://www.eurocomms.com/features/analysis/11940-telefonica-to-create-personal-data-bank-for-customers-expose-unfair-apps

10 "The future of digital trust: A European study on the nature of consumer trust and personal data."Orange. February 2014. https://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf

11 Chang, Lulu. "IBM and BMW want to make Watson your own personal back-seat driver." December 15, 2016. Digital Trends. http://www.digitaltrends.com/cars/bmw-ibm-partnership/#ixzz4ZKYSM0l5

12 IBM Institute for Business Value analysis, based on publicly available information.

13 "Fast forward:Rethinking enterprises, ecosystems and economies with blockchains." IBM Institute for Business Value. June 2016. https://www-935.ibm.com/services/us/gbs/thoughtleadership/blockchain/

14 "Orange Digital Ventures invests in Chain, the leading provider of blockchain technology solutions. Orange. September 10, 2015. http://www.orange.com/en/Press-Room/press-releases-2017/press-releases-2015/Orange-Digital-Ventures-invests-in-Chain-the-leading-provider-of-blockchain-technology-solutions

15 Everington, John. "Du to use blockchaine for health records." The National. May 30, 2016. http://www.thenational.ae/business/technology/du-to-use-blockchain-for-health-records

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
September 2018

GBE03807USEN-01