

Digital Business

## The Business Value of Trust

Consumer trust has become the new battleground for digital success. To win, organizations need to master the fundamentals of data ethics, manage the “give-to-get” ratio and solve the customer trust equation, our recent research reveals.



Center For  
The Future of Work

# Executive Summary

When we interact with digital leaders such as Google, Netflix, Facebook, Amazon, Alibaba and others, it feels as if they already know us. It may be a book recommendation, a reminder to leave for the airport on time or any number of now familiar curated experiences that spark “a-ha” moments in our minds. At the heart of these experiences is our personal data, or Code Halo,<sup>™</sup> generated by our online behaviors and actions. The amalgam of this data — our “virtual selves” — is becoming increasingly valuable to companies, many of which are now scrambling to provide the highly personalized experiences to which we have flocked in recent years.

There is, however, a dark side to this business–technology shift that raises important technological, social and ethical considerations: What exactly is appropriate use of data? Is it appropriate for a health insurance provider to monitor clients’ fitness band data and use it to adjust their insurance premiums? Is it OK for a pay-per-view movie provider to charge higher fees to someone living in a wealthy neighborhood than to customers living in a less affluent area? Is it proper for a taxi service to charge a higher price for a passenger who’s headed to the airport because she tweeted that she was in a rush? There’s an infinite number of commercial questions — far too many to be answered individually; instead, we must frame them as ethics questions about how companies use consumers’ personal data and the extent to which their data-handling practices earn the ultimate prize: consumer trust.

We recently surveyed thousands of consumers in the Asia-Pacific region and Middle East to learn more about their perceptions of the business value of trust (see Methodology, page 16). We believe our findings are relevant not only to companies operating in those geographies but also for any organization concerned with maintaining trust in the digital business world. Our study revealed that one of the biggest threats to companies today comes not from the competition but from the ability to win and keep

consumer trust. In an age when personal data is the key to honing a competitive edge, data ethics is at the heart of business success, as customers will increasingly choose to work with Vendor A over Vendor B, if they trust Vendor A more.

As the digital economy rapidly expands, we will undoubtedly hear of more businesses suffering financial and reputational damage due to failures and abuses of security, privacy and trust. Conversely, companies that learn consumer trust will be better suited to weather the inevitable – and yes, they are inevitable – data and policy breaches.

Companies that earn consumer trust  
will be better suited to weather the inevitable  
– and yes, they are inevitable – data and policy  
breaches.

In our study, we explore the ethical battlefield of consumer trust and private data usage across a range of industries. We illuminate the factors that determine how consumers think about trust, the economic value associated with it and the inner-workings of the “give-to-get” ratio that every organization must understand and heed. We also offer recommendations on how businesses can succeed in this new battle for dominance in a trust-driven, digital-first world.

## Key findings: trust is the new currency

Our study reveals what happens when trust is breached and explores the factors that influence customer trust. In particular, businesses should note the following key findings.

- I Don't just keep my data; keep my trust.** The propensity for consumers to expose much of their personal lives, and thus data, online has provided an abundance of publicly available personal information that could be exploited if ethics are compromised by companies; 65% of respondents don't know how or where their personal data is stored.
- I "Return on trust" is the digital economy imperative.** Half of respondents are willing to pay a premium for products and services from companies they trust most. However, the reverse is equally true: Roughly 57% will stop doing business with a company that has broken their trust.
- I Breaking trust can break a brand.** On average, only 43% of respondents have a high level of trust in institutions across industries. Worse, nearly 40% plan to switch to the competition or digital startup due to trust issues. We observed significant differences across industries, with automotive companies and retailers at the bottom of the trust list.
- I Established companies have a 6% "legacy tax" on trust.** Approximately 47% of respondents plan to switch to a digital startup due to perceived trust concerns over how their personal data is being used, compared with 41% who said they would rely more heavily on established, pre-digital enterprises.
- I Privacy and security form the basis of trust.** Nearly all respondents are concerned about privacy (91%), theft (76%), misuse of personal data (75%) and even physical safety (72%). In the great compromise between privacy/security and delivering personalized products and services, respondents greatly value the ethical compasses of the companies with which they do business.
- I Data can be yours as long as you ask clearly and keep your word.** Transparency is the top factor (67%) affecting a company's trustworthiness. In fact, 45% of respondents are willing to share personal data if a company asks upfront and makes clear how the data will be used.
- I Show consumers a return on the value of their trust.** About 66% of respondents view personal data as valuable and are willing to share it with companies in exchange for some form of value. This positive "give-to-get" ratio is at the core of the economics of trust.

## Data: the foundation of trust

The technologies that pervade our existence are transforming how we as consumers live, work and play. It's no wonder, then, that almost half of respondents consider themselves "always connected" (see Figure 1, next page), and 77% view social media platforms as critical to maintaining social relationships. Such rampant connectivity has given rise to an age of personal data sharing (and over-sharing) and increased consumer expectations for mass personalization, with more than half of respondents (58%) saying they demand personalized products and services from companies.

Such contextually relevant experiences are impossible without data, and markets recognize this vital connection; in fact, data is among the intangible assets constituting as much as 84% of the market value of

companies listed on the S&P 500 index.<sup>1</sup> However, before data is an asset, it is a liability; according to Gartner, by 2018, half of business ethics violations will occur through improper use of big data analytics.<sup>2</sup> As Nobel Prize winning economist Ronald Coase has said, "If you torture data long enough, it will confess to anything you'd like."<sup>3</sup>

While consumers generally voice a desire for privacy, they are also very open with the information they share about their lives, often through smartphones and social media, which seem to have become permanent fixtures in many of our lives. Despite the security concerns, consumers continue to store precious documents in the cloud and rely on the likes of Netflix, Amazon and Google for recommendations and information.

Companies are now increasingly reliant on decisions driven by algorithms and machine learning to find the next business opportunity with consumers. However, the gradual reduction of human oversight over many automated processes poses pressing issues of responsibility and respect for human feelings. Moreover, while data scientists have been given a god-like power to draw new inferences from data, many of them fail to consider the ethical implications in their everyday actions, as there are no data ethics guidelines in existence at most companies. Concern continues to grow — and is perhaps approaching a tipping point — as 65% of respondents express high levels of concern about how and where their personal data is stored.

There are many ways to represent the hidden mechanisms of trust, but we've found the following equation to be useful for turning this nebulous concept into something more quantifiable and actionable:

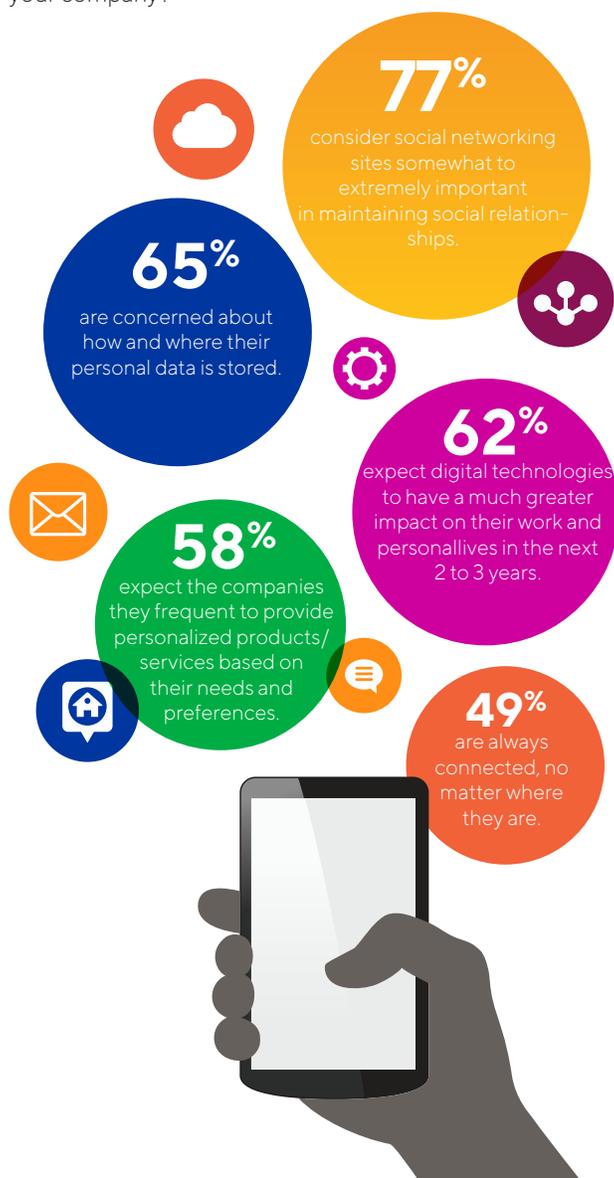
$$\text{Trust} = \frac{R * C * I}{SO}$$

In this equation, R stands for reliability, C for credibility, I for intimacy and SO for self-orientation. The first three elements correlate directly with trust, and have a multiplier effect. Conversely, self-orientation — which manifests itself as selfishness and narcissism — undermines trust. What was true in grammar school is true in the digital economy: Overt selfishness erodes trust.<sup>4</sup>

The future will soon belong to companies that build their products and services around the trust equation, and place it at the core of their brand. Such is the case at Swedish car maker Volvo,<sup>5</sup> which collects reliable data on vehicle capabilities and the services the company provides, and uses that insight to ensure passenger safety. Because it realizes the power of the trust equation, the company has set a goal that by 2020 no one should be harmed or killed in a Volvo.

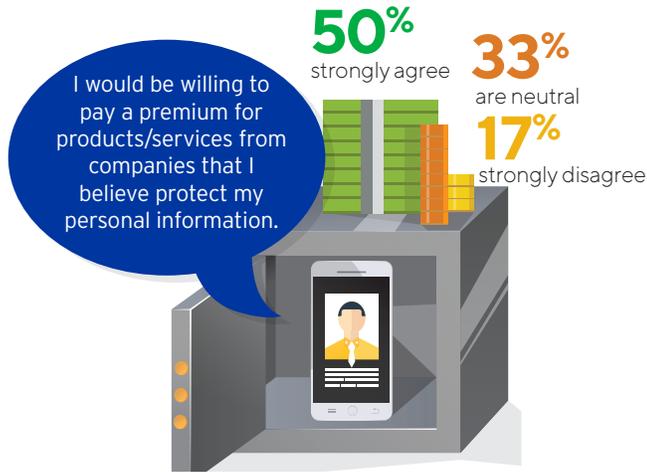
## Data is the foundation of trust

What are the benefits of enhanced digital capabilities for your company?



Response base: 2,404 consumers; multiple responses permitted  
Source: Cognizant Center for the Future of Work  
Figure 1

## Trust motivates spending, loyalty



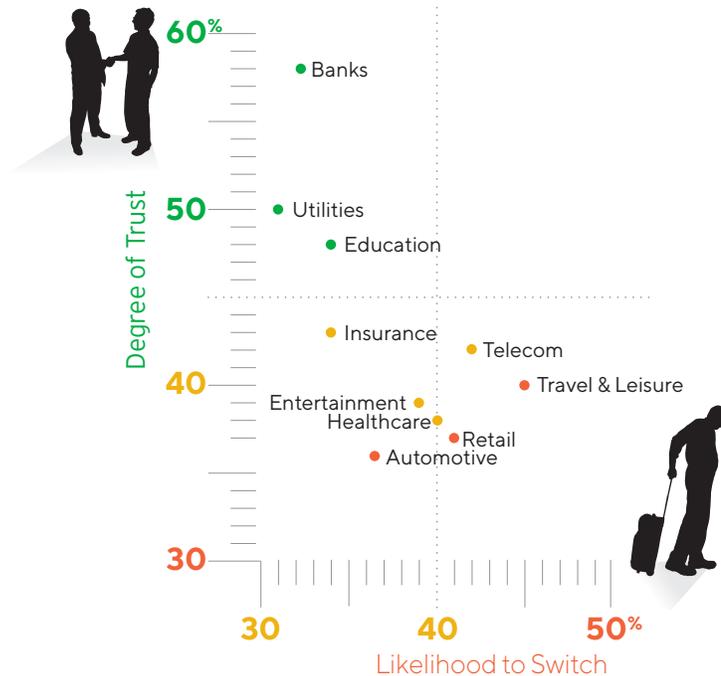
Response base: 2,404 consumers  
 Source: Cognizant Center for the Future of Work  
 Figure 2

## Trust is money, and all industries are losing it

Trust has been elevated to a C-suite issue, not an afterthought, because consumer trust converts into bottom-line benefits; in our study, half of respondents say they are willing to pay a premium for products and services from companies they trust (see Figure 2). On the flipside, the misuse or mismanagement of personal information has potentially irreversible downsides. We are living in a time in which technological advances are outpacing the rate of legal and cultural constructs, causing significant consumer confusion, even fear, when it comes to trust.

The bad news is that no industry we studied is perceived as highly trustworthy by respondents. On average, only 43% have a great level of trust in institutions across industries, and nearly 40% plan to switch to a competitor or a digital startup due to trust issues (see Figure 3).

## Loss of trust is loss of business



Respondents were asked about their level of trust in each type of organization to manage their personal information responsibly.

They were then asked about their likelihood to switch providers if they ever felt their personal information had been mishandled.

(Figure shows respondents who gave an 8+ rating on a scale from 1 to 10)

- Lower Risk
- Moderate Risk
- Higher Risk

Response base: 2,404 consumers  
 Source: Cognizant Center for the Future of Work  
 Figure 3

Here's an industry round-up of consumer trust levels:

**I Relatively high trust in banks and utilities is marred by a propensity to switch in the event of an unforeseen incident.** Although respondents revealed moderate trust in banks (58%) and utilities (50%), one third are still likely to switch their banks (32%) and utility providers (31%) if trust is compromised.

**I Automotive companies and retailers are at the highest risk of losing brand value.** Of all industries, automotive companies (36%) and retailers (37%) rank the lowest in trust, and 41% of respondents would switch retailers if there were a breach in trust. Recent events reinforce these findings:

- I The Volkswagen emissions scandal demonstrates how quickly a company can lose trust. Volkswagen's stock lost 20% of its value (about US\$28 billion<sup>6</sup>), and the company plans to reduce its investments by US\$1.14 billion a year to offset the financial damage.<sup>7</sup>
- I After Target Corp. experienced a data breach affecting 70 million customer records, the company's profits fell 34.3%, and as of January 31, 2015, the company has incurred US\$252 million in cumulative data breach-related expenses. Target's latest annual report surprisingly reveals no mention of "consumer trust" in its report filing.<sup>8</sup>

**I Telecom operators are next in line to lose out over ethical concerns.** While 42% of respondents trust their telecom operators, an equal percentage say they would switch to a new provider. Talk Talk, a telecom operator in the UK, revealed that 157,000 of its customers' personal details were breached. Since October 2015, the company's share price has fallen 27%, and it saw a 4.4% decline in market share of new customers in its home services segment.<sup>9</sup>

Another example is Telstra, a leading telecom provider in Australia, which suffered trust issues after a data breach of 15,000 customers.<sup>10</sup>

## Broken trust breaks business, brand and loyalty

Consumers may forgive companies for their mistakes but not for dishonesty. Inappropriate use of data is a recipe for disaster, with 57% of respondents saying they would completely stop doing business with a company that has used their personal data unethically (see Figure 4). Additionally, about 37% of respondents would take legal action against the company. We already see this playing out in the courts. Two Hong Kong companies faced lawsuits when customers accused them of abusing their personal data for direct marketing purposes.<sup>11</sup>

### Lost consumer trust is a path to self-destruction



Response base: 2,404 consumers; multiple responses permitted  
Source: Cognizant Center for the Future of Work  
Figure 4

Brand loyalty is the result of trust cultivated over many years, but it can be destroyed in a day, especially when evidence of poor ethical judgment can go viral with the tap of a screen. For instance, Kmart Australia was lambasted on social media recently when customers complained that the company provided limited information and little guidance following an online security breach.<sup>12</sup> Another example is inBloom, a data management company that collects student data to provide teachers with insights.<sup>13</sup> When parents raised privacy concerns, the company remained silent – and then shut down less than a year after its launch.

The impact of broken trust can be pernicious; Forbes Insights noted that 46% of organizations surveyed had suffered damage to their reputations and brand value following a data breach.<sup>14</sup>

## Trust is gained by walking the talk

Respondents’ lack of confidence – and ultimately trust – in companies’ ability to provide privacy and security signals a tremendous opportunity for business leaders to make bold decisions about data transparency. Open and transparent communication is the top factor (67%) for bolstering consumer trust, followed by product and service quality (61%), fair pricing (60%) and well-communicated data usage policies (59%) (see Figure 5).

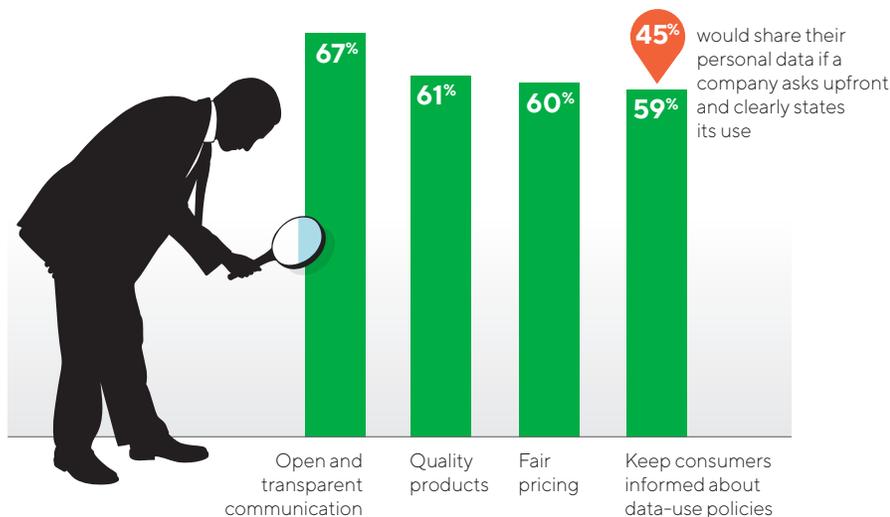
In fact, 45% of respondents said they are willing to share their personal information when companies ask upfront for permission to use their data and clearly state how it will be used. When companies share responsibility for and show an interest in minimizing risk, consumers become more willing to trust.

The collaborative consumption characterized by the sharing economy is built on transparency. New

players like Airfrov<sup>15</sup> (which connects shoppers and travelers for overseas items) and Fortune Mother Exchange<sup>16</sup> (which connects mothers across cities in India to provide kids with home-cooked meals) are redefining transparency. Google began reporting on transparency a few years ago; while it originally met with criticism, the idea has spread, with over 30 major companies now issuing transparency reports publicly, highlighting how user data is collected and used.<sup>17</sup>

## Transparency is the new competitive differentiator

Respondents were asked which factors were important or extremely important for determining their level of trust in a company.



Response base: 2,404 consumers; multiple responses permitted  
 Source: Cognizant Center for the Future of Work  
 Figure 5

Consumers trust businesses not on the basis of their physical assets or the products and services they offer but rather on the value and experience they deliver in the virtual and physical worlds.

## Digital startups increasingly winning the consumer trust battle

Customers today want faster delivery of services without compromising their personal data, and digital startups seem to be meeting these expectations, as they have built their entire business on personal data control (see Figure 6). Nearly half (47%) of respondents said they would switch to a digital startup because they trust their approach to data ethics.

For instance, the Blackphone 2 smartphone is built around the promise of keeping personal information private, elevating customer expectations from mobile manufacturers.<sup>18</sup> Another example is Alipay, China's third-party online payment company, which has become the largest online payment processor in the world in less than a decade.<sup>19</sup>

Increasingly, consumers trust businesses not on the basis of their physical assets or the products and services they offer but rather on the value and experience they deliver in the virtual and physical worlds. The center of gravity is shifting to agile businesses that can quickly innovate and embrace the power of digital platforms. These digital disruptors are creating new customer expectations every day, and in the process, they are redefining consumer trust.

Competitive pricing is another crucial factor, with 77% of respondents citing better price as a key driver for switching to the competition (see Figure 6). Although traditional businesses can compete in terms of price, they are struggling to match the energy and innovation of digital startups.

## Lack of privacy leads to mistrust

Despite their higher levels of trust for digital startups, nearly all survey respondents voiced general concern about their online data privacy (see Figure 7, next page); additionally, more than half do not believe what companies claim to be doing to protect their data privacy. The sense of having no control over their data (58%) is one of the main causes of respondents' growing concern, and as new digital technologies (3-D printers, health and lifestyle sensors, smart watches, etc.) go mainstream, more than 50% believe privacy-related issues will only get more complicated.

### Trust is a given for digital startups

What could lead you to switch to another competitor?

 **77%**  
Better price

 **57%**  
Better experience

 **56%**  
Promotions/  
discounts

What could lead you to switch to a new digital startup?

 **49%**  
More choices

 **49%**  
Faster delivery

 **47%**  
Trust the use of  
personal data

Response base: 2,404 consumers; multiple responses permitted  
Source: Cognizant Center for the Future of Work  
Figure 6

## If you're not paying for a product, you are the product



Response base: 2,404 consumers; multiple choices permitted  
 Source: Cognizant Center for the Future of Work  
 Figures 7 (above) and 8 (below)

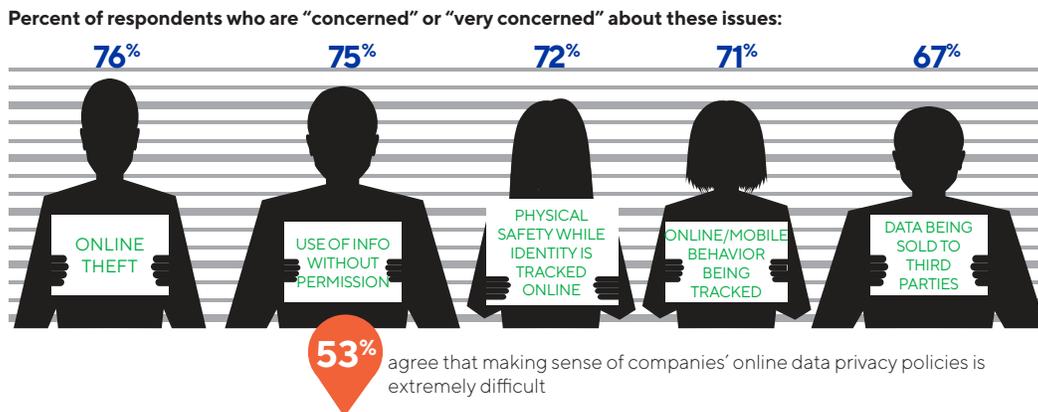
Getting personalized services in the age of data sharing is exciting, but consumers are increasingly concerned that their private data will be misused. No one wants an advertisement for health or life insurance pointing out that they haven't been exercising recently. Without a sense of trust between consumers and service providers, there is no common ground for privacy in our digital world.

Specific concerns are wide-ranging (see Figure 8) and experience-based, with one-third of respondents (or their family or friends) reporting that their personal data (credit card, bank details, health information, etc.) had been stolen or compromised in the last two to three years. Companies may believe it's enough to develop and publish data privacy policies, but more than half (53%) of respondents feel that understanding such policies is almost impossible.

The sheer amount of data collected — coupled with the complexity of ensuring privacy at that scale — creates a significant amount of consumer anxiety. Consider these examples:

- Acxiom Corp., a leading data broker, collects 1,500 data points per person for 700 million people worldwide. The company processes over 50 trillion sales transactions per year by selling consumer data multiple times to multiple customers.<sup>20</sup>
- 90% of mobile apps in Singapore do not adequately declare which consumer data is collected or how it is used, potentially failing to meet Singapore's Personal Data Protection Act guidelines.<sup>21</sup>

## Privacy recedes as trust issues accelerate



These companies are not doing anything wrong; however, when personal data is used in an unexpected way, consumers are bound to react. For instance, Facebook recently issued an apology for carrying out a psychological experiment on users’ data.<sup>22</sup> Although users had given consent, and Facebook was trying to better connect content to users, many still felt the company had breached their privacy.

## Consumers don’t worry about security – until it’s too late

Still, when it comes to their everyday behavior, consumers do not tend to keep data security top-of-mind – until something goes wrong. Alarm bells rang when news reports surfaced of cyber-attacks launched through refrigerators connected to the Internet of Things (IoT)<sup>23</sup> and even connected toys;<sup>24</sup> however, 58% of respondents report a fairly high perception of the security of their personal information when conducting various activities online (see Figure 9).

How can we explain this dichotomy? Perhaps, as *Wired* magazine founder Kevin Kelly said recently, their vanity trumps their concern for privacy. “When given a sliding scale from anonymous to fully tracked, we are usually more likely to let ourselves be tracked. Why? We know we will gain a more tailored experience,” Kelly said.<sup>25</sup>

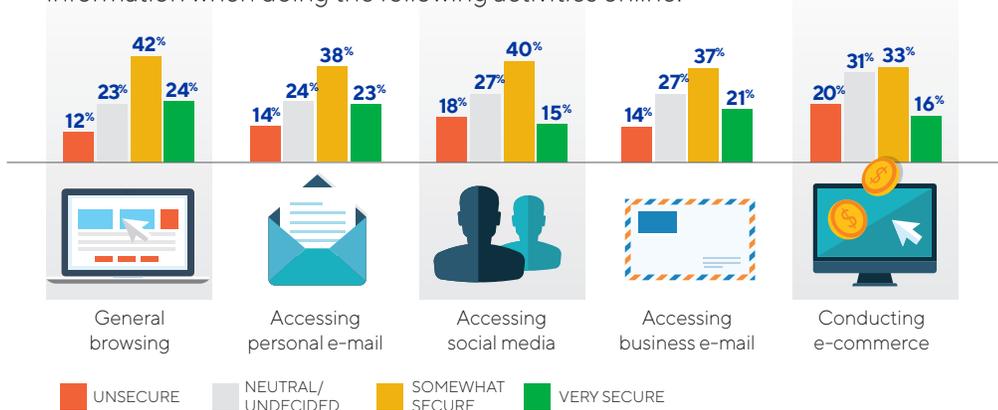
Further, the interpretation of risk can vary greatly between people and companies. Consumers continue to share data online, download apps, upload images, follow free sites, etc. because they are more focused on the benefits they’ll get out of the activity than the risk of doing so. Meanwhile, companies are more focused on the risk equation because they know that a single data breach can irreparably damage consumer trust.

## Trust is conditional: what’s in it for me?

In other words, consumers are saying, “I will trust you if I know – and value – what I’ll get.” In this environment, it is critical for companies to move away from mere data collection to a value-first mindset. As consumers become more educated about how a company is using their data, they want a personal, tangible and immediate benefit in return, and they’re willing to assume more risk.

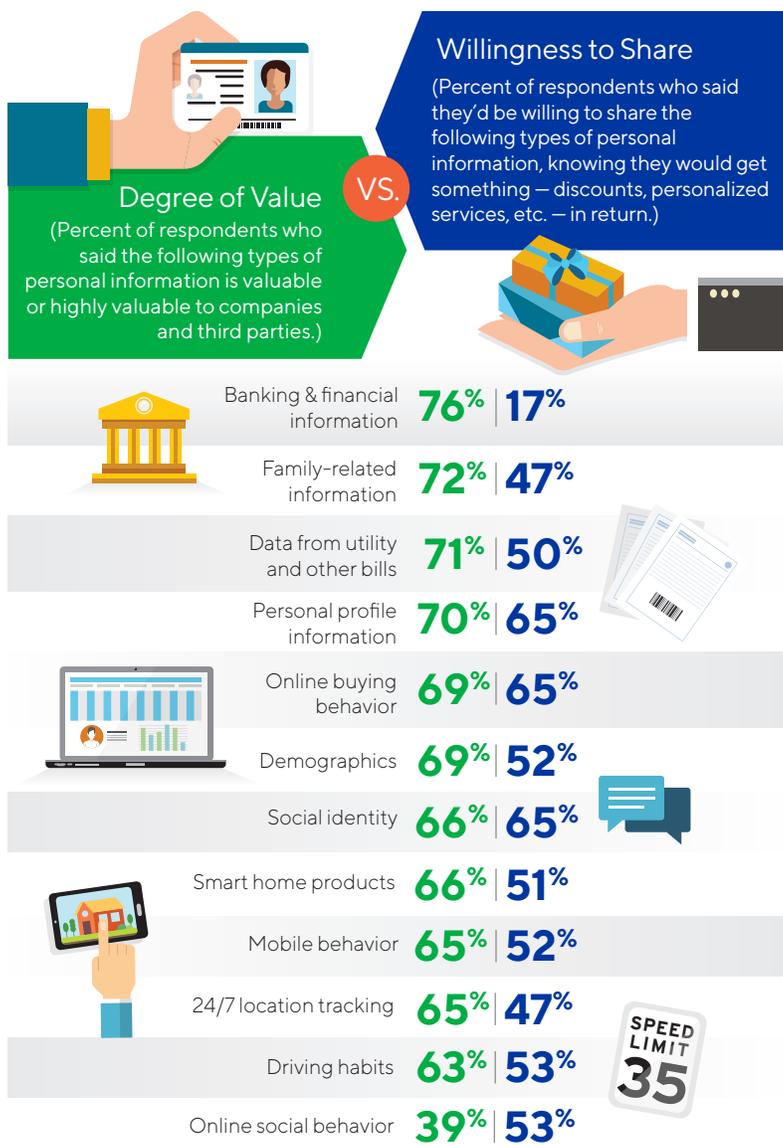
## Consumers don’t draw a strong line between data security and trust

Respondents were asked how secure they felt about their personal information when doing the following activities online.



Response base: 2,404 consumers; multiple responses permitted; percentages may not add to 100 due to rounding  
 Source: Cognizant Center for the Future of Work  
 Figure 9

## The risk of sharing personal information is worth the return



Response base: 2,404; consumers; multiple responses permitted  
 Source: Cognizant Center for the Future of Work  
 Figure 10

In fact, 46% of consumers believe the risk of sharing personal information is worth the personalized products, services and offers they'll get in return. About 66% view their personal information as valuable, and 50% are willing to share it in exchange for personalized engagement, cash rewards, better customer service, special promotions, relevant experiences and friendly interactions (see Figure 10). We call this the "give-to-get" ratio, and managing this trade-off transparently is essential for trust. (For a full treatment of the give-to-get ratio concept, read our book *Code Halos: How the Digital Lives of People, Things and Organizations Are Changing the Rules of Business*.<sup>26</sup>)

To date, market-leading consumer-facing businesses (Google, Netflix, Amazon, etc.) are thriving in large part because the give-to-get ratios in their business models weigh so significantly in their customers' favor. Consumers give very little, and get a lot in return.

To develop a positive give-to-get ratio, it is vital for companies to understand which information consumers consider to be the most valuable and how willing they are to share that information. Key dynamics that companies must consider include:

**I Consumers consider their financial information to be extremely private and are highly reticent to share it.** A total of 76% of respondents view their banking and other financial information as highly valuable, but only 17% are willing to share that information for any benefit in return.

**I Personal information and online buying behavior are the sweet spots.** Respondents view their name, gender, age and online buying behavior (70%) as highly valuable and are also willing to share this data (65%) for a tangible benefit in return.

**I Online social behavior is valued least by consumers but used most by companies.** Surprisingly, only 39% of respondents view their online social behavior as valuable, and 53% are willing to share it with companies. We believe companies that have been aggressively tracking online social behavior of consumers may not be getting the maximum benefits of their investments, considering the value consumers place on this information.

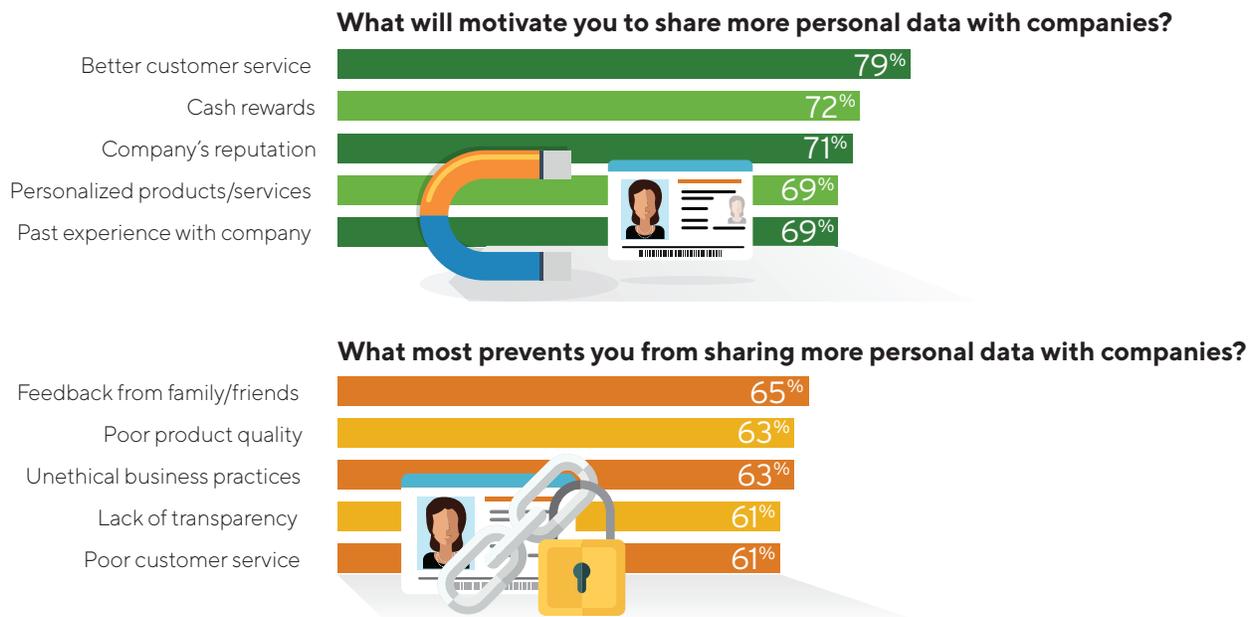
There are both positive and negative give-to-get ratios that determine consumer propensity to share or not share their personal information. For instance:

- I Take my information, but please improve your customer service.** Interestingly, almost 80% of respondents say better customer service would motivate them to share more personal data with companies (see Figure 11, next page).
- I My grandma doesn't trust your company, so neither do I.** Consumers trust the opinion of family and friends, so it's not surprising that 65% of respondents named negative feedback from people they know as a top reason they would not share personal data with a company.
- I There is no second chance for creepiness.** Most respondents say unethical business practices (63%) and lack of transparency (61%) would deter them from sharing data. There is a thin but clear privacy line between providing a personalized service to improve the give-to-get ratio and being overly intrusive. For instance, some employees have voiced concerns after discovering their employers were quietly using big data to track employee pregnancies.<sup>27</sup>

Some companies have done extremely well in making the trade-off worthwhile. For instance, Disney collects and analyzes profiling and location data through its MagicBand™ bracelet to enhance the experience of its park guests, who gain convenience and a sense of privileged access in return.<sup>28</sup> Why does this work so well? Because Disney spells out the purpose of data collection clearly so consumers know what they're signing up for.

It's not surprising that 65% of respondents named negative feedback from people they know as a top reason they would not share personal data with a company.

## Service and opinion can make or break the “give-to-get” equation



Response base: 2,404 consumers; multiple responses permitted  
 Source: Cognizant Center for the Future of Work  
 Figure 11

## Looking forward: turn trust issues into your biggest asset

Winning companies will radically change their business models to break away from the old mentality and take risks to revamp their customer engagement strategy and deliver value that matters most to consumers. The increasing value and quality of the data that companies gather has changed not only the way products and services are delivered, but also the way consumers make decisions. Consider the following recommendations to win with trust in the burgeoning digital economy.

- I Ensure manageable “gives” and positive “gets.”** If the “give” factor is imposed upon consumers in a cryptic and nontransparent way (such as a dense description of terms, followed by an “I Accept” button), trust can be instantly damaged. Open communication about data-sharing trade-offs is the foundation for making things work.
- I Give customers a delete button.** Customers should have a complete 360-degree view of their information and full control of it. A good example is the Metadistretti e-monitor that provides flexibility to cardiac patients to control what data goes to whom, using a browser and an app.<sup>29</sup> Patients can set up networks of healthcare providers, family and friends, or fellow users and patients, and select which information they are willing to share with each group independently.

# Ethics must become a key performance indicator for every employee who has a direct or indirect connection with customer data.

- I **Tear down the wall between IT and business with a “chief trust officer.”** Trust is not an issue of compliance, privacy, security or technology (as many companies presume it to be) but a brand-level risk/opportunity that belongs in the C-suite. The role of the chief trust officer would be to ensure that the monetization of data assets conforms to ethical guidelines. In particular, the role will have a dual responsibility to execute the following:
  - I **Add human intelligence to existing analytics capabilities.** We believe the future of analytics will lie in its intelligent ability to differentiate between appropriate and inappropriate use of data. The chief trust officer would work with relevant teams to develop an ethics framework (depending on the industry, data usage capabilities, etc.) and add it as a tool to the company’s current analytics solutions. The use of an embedded ethics monitoring mechanism, either via pre-built frameworks or use of a tool, would assist, guide or notify users if their machine/mining algorithms crossed the ethical line and take necessary steps to avoid unwanted situations. This level of transparency would help companies win consumer trust.
  - I **Make data ethics a key performance indicator.** Ethics must become a key performance indicator for every employee who has a direct or indirect connection with customer data. The starting point should be establishing onboard training for all new employees, and then initiating a company-wide program to help people understand the legal and business consequences of unethical data practices. Follow-up actions should include suggesting early interventions to avoid or mitigate risk, and reinforcing the goals and outcomes of the ethical framework. All of these activities would help develop a culture in which employees feel comfortable with talking about ethics openly.
- I **Be quick to respond to failures.** In spite of world-class technology infrastructures, history shows that organizations cannot promise customers that nothing bad will happen to their digital information. Organizations need to recognize, understand and proactively manage potential negative issues. For instance, after a recent cyber-attack, Vodafone was quick to notify customers and financial institutions of the incident, and this quick action helped minimize damage to trust.<sup>30</sup>
- I **The law will never catch up, so develop self-control.** A discussion on the importance of consumer trust would be incomplete without considering the legal implications and regulatory frameworks that impact digital business. More than 50% of respondents feel that digital regulations (e.g., laws about the use of data and the Internet, or regulations of “collaborative commons” systems such as Uber and blockchain) will help increase trust. In reality, however, regulations are always behind the curve compared with technological advancements. While digital regulations will evolve at their own pace across geographies, they should not be considered as the only resort for protecting consumer data. Instead, businesses need to focus on self-regulation based on openness and accountability, with an obsession for maintaining consumer trust.

Consumers are a business’s brand ambassadors, and losing their trust will directly impact the brand and the future of the business.

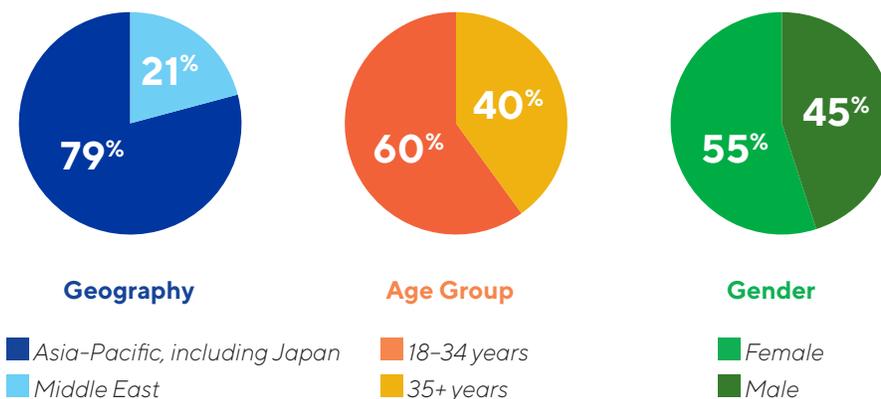
### Either I trust you, or I don’t – there is nothing in between

There is no such thing as blind trust in today’s business world. In the digital era, consumer trust is driven by data ethics, transparency and the give-to-get equation. As the digital revolution unfolds, trust will become even more important because consumers will not just expect but assume businesses have put their interests before everything else. If consumers feel their trust is impacted, they’ll move on. Consumers are a business’s brand ambassadors, and losing their trust will directly impact the brand and the future of the business.

Data ethics has become the new purpose for businesses. As many industries and businesses face disruption over the next decade, winners and losers will be determined by how they manage the trust equation. Trust will increasingly be seen not as the end objective but as a necessity for business success.

## Appendix A

This study was conducted across a variety of geographies and age groups.



## Appendix B: research methodology

Online panel-based research was conducted with 2,404 consumers across the Asia-Pacific region, including Japan and the Middle East. The sample was distributed across several age groups. Consumers who have access to the Internet at least once a month were included in the survey. The research was conducted over six weeks by an independent research agency on behalf of Cognizant. Areas studied include:

- Views toward digital technologies, their importance, online behavior and spending patterns.
- Degree of trust across industries and likeliness to switch product or service providers.

- Factors that influence trust in selecting a company.
- Concerns over privacy, data security and their association with the value of trust.
- Consumers' view on the degree of value of their personal information and willingness to share different types of data.
- Drivers and inhibitors of personal data sharing with companies.

Note: Code Halo™ is a registered trademark of Cognizant Technology Solutions.

## Endnotes

- 1 "Annual Study of Intangible Asset Market Value from Ocean Tomo," Ocean Tomo, March 5, 2015, <http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/>.
- 2 "Gartner Says, by 2018, Half of Business Ethics Violations Will Occur through Improper Use of Big Data Analytics," Gartner, Inc., Oct. 7, 2015, <http://www.gartner.com/newsroom/id/3144217>.
- 3 Brent Dykes, "31 Essential Quotes on Analytics and Data," Analytics Hero, Oct. 25, 2012, <http://www.analyticshero.com/2012/10/25/31-essential-quotes-on-analytics-and-data/>.
- 4 For more on the trust equation, see page 124 of our book *Code Halos: How the Digital Lives of People, Things, and Organizations are Changing the Rules of Business*, by Malcolm Frank, Paul Roehrig and Ben Pring, published by John Wiley & Sons. April 2014, <http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118862074.html>.
- 5 Jack Hershman, "Volvo Group CIO: Data and Trust as Currency in the Digital Age," Hot Topics, <https://www.hottopics.net/stories/consumer/volvo-group-cio-data-and-trust-in-the-digital-age/>.
- 6 Ivana Kottasova, "Volkswagen Stock Crashes 20% on Emissions Cheating Scandal," CNN Money, Sept. 22, 2015, <http://money.cnn.com/2015/09/21/investing/vw-emissions-cheating-shares/>.
- 7 David Amerland, "The Cost of Losing Trust," Medium.com, Oct. 15, 2015, <https://medium.com/@davidamerland/the-cost-of-losing-trust-97d764a1e696#.n0sclvwsa>.
- 8 Maggie McGrath, "Target Profit Falls 46% on Credit Card Breach, and the Hits Could Keep on Coming," *Forbes*, Feb. 26, 2014, <http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#19ab1a045e8c> and U.S. SEC filing, <https://www.sec.gov/Archives/edgar/data/27419/000002741915000012/tgt-20150131x10k.htm>.
- 9 Alexander Sword, "Rebuilding Brand Trust: TalkTalk's Path Back from Cyber Attack," *Computer Business Review*, Jan. 22, 2016, <http://www.cbronline.com/news/cybersecurity/data/rebuilding-brand-trust-talktalks-path-back-from-cyber-attack-4790671>.
- 10 "Telstra Fined after Breaching Privacy of 15,775 Customers," ABC News, March 10, 2014, <http://www.abc.net.au/news/2014-03-11/telstra-breaches-privacy-of-15775-customers/5312256>.
- 11 "Two Companies Fined over Direct Marketing Offences," Kennedy's, Sept. 22, 2015, <http://www.kennedyslaw.com/hkdirectmarketingoffences/>.
- 12 Shoba Rao, "Kmart Australia Customers Hit by Online Privacy Breach in Security Hack," News Corp Australia Network, Oct. 2, 2015, <http://www.news.com.au/technology/online/hacking/kmart-australia-customers-hit-by-online-privacy-breach-in-security-hack/news-story/9eb8eed08aedb63c28fa8164ff1e726b>.
- 13 Natasha Singer, "InBloom Student Data Repository to Close," *New York Times*, April 21, 2014, [http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/?\\_php=true&\\_type=blogs&\\_r=1](http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/?_php=true&_type=blogs&_r=1).

- <sup>14</sup> Doug Drinkwater, "Does a Data Breach Really Affect Your Firm's Reputation," CSO Online, Jan. 7, 2016, <http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html>.
- <sup>15</sup> Airfrov website, <https://www.airfrov.com/>.
- <sup>16</sup> Video on Fortune Mother Exchange, April 25, 2015, <https://youtu.be/h22M4-OrAUg>.
- <sup>17</sup> "OECD Digital Economy Outlook," OECD, 2015, [https://books.google.co.in/oks?id=T9lqCgAAQBAJ&pg=PA64&lp-g=PA64&dq=Google+issued+the+first+transparency+report+in+2009+the+number+has+grown+with+over+30+companies+now+issuing+public+reports.&source=bl&ots=ITEez\\_P7VM&sig=Nr\\_X754evTspD1UxSgH9Q\\_z-98&hl=en&sa=X&ved=0ahUKEwiZ2vvg1avLAhWHQJ4KHVapC20Q6AEIHjAA#v=onepage&q=Google%20issued%20the%20first%20transparency%20report%20in%202009%20the%20number%20has%20grown%20with%20over%2030%20companies%20now%20issuing%20public%20reports.&f=false](https://books.google.co.in/oks?id=T9lqCgAAQBAJ&pg=PA64&lp-g=PA64&dq=Google+issued+the+first+transparency+report+in+2009+the+number+has+grown+with+over+30+companies+now+issuing+public+reports.&source=bl&ots=ITEez_P7VM&sig=Nr_X754evTspD1UxSgH9Q_z-98&hl=en&sa=X&ved=0ahUKEwiZ2vvg1avLAhWHQJ4KHVapC20Q6AEIHjAA#v=onepage&q=Google%20issued%20the%20first%20transparency%20report%20in%202009%20the%20number%20has%20grown%20with%20over%2030%20companies%20now%20issuing%20public%20reports.&f=false).
- <sup>18</sup> Samuel Gibbs, "Blackphone2 Review: Privacy Doesn't Have to Come at the Cost of Usability," Nov. 11, 2015, <https://www.theguardian.com/technology/2015/nov/11/blackphone-2-review-privacy-usability-silent-circle>.
- <sup>19</sup> Kendrick Sands, "How Alibaba Is Transforming Payments and Banking in China," Euromonitor International, June 19, 2014, <http://blog.euromonitor.com/2014/06/how-alibaba-is-transforming-payments-and-banking-in-china.html>.
- <sup>20</sup> Tiemoko Ballo, "5 Fatal Misconceptions about Digital Privacy," Nov. 12, 2015, Medium.com, <https://medium.com/@tiemokoballo/5-fatal-misconceptions-about-digital-privacy-9ee4412ef4c6#.o717916f7>.
- <sup>21</sup> "90% of Mobile Apps Could Be in Breach of Singapore Privacy Law," *Straits Times*, Nov. 2, 2015, <http://www.straitstimes.com/tech/90-of-mobile-apps-could-be-in-breach-of-singapore-privacy-law>.
- <sup>22</sup> Samuel Gibbs, "Facebook Apologises for Psychological Experiments on Users," *The Guardian*, July 2, 2014, <http://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users>.
- <sup>23</sup> Danny Palmer, "Cyber Attack Launched through Fridge as Internet of Things Vulnerabilities Become Apparent," *Computing*, Jan. 17, 2014, <http://www.computing.co.uk/ctg/news/2323661/cyber-attack-launched-through-fridge-as-internet-of-things-vulnerabilities-become-apparent>.
- <sup>24</sup> Jeff Stone, "VTech Admits 6.4 Million Kids Affected in Massive Data Breach; Hong Kong Regulators Investigating Toy Maker," *IB Times*, Dec. 1, 2015, <http://www.ibtimes.com/vtech-admits-64-million-kids-affected-massive-data-breach-hong-kong-regulators-2206752>.
- <sup>25</sup> Richard Wise, "SXSW 2016: Niche Is the New Mainstream," *Field Journal of a Brand Anthropologist*, March 17, 2016, <http://rwise.tumblr.com/post/141215832307/niche-the-new-mainstream>.
- <sup>26</sup> For more information on Code Halos, see our website, <https://latestthinking.cognizant.com/code-halos>.
- <sup>27</sup> Valentina Zarya, "Employers Are Quietly Using Big Data to Track Employee Pregnancies," *Fortune*, Feb. 17, 2016, <http://fortune.com/2016/02/17/castlight-pregnancy-data/>.
- <sup>28</sup> Timothy Morey, Theodore Forbath, Allison Schoop, "Customer Data: Designing for Transparency and Trust," *Harvard Business Review*, May 2015, <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>.
- <sup>29</sup> Ibid.
- <sup>30</sup> Dateme Tamuno, "Trust in the Digital Age, How Far Is Too Far? A Vodafone and TalkTalk Case Study," *Customer Think*, Nov. 3, 2015, <http://customerthink.com/trust-in-the-digital-age-how-far-is-too-far-a-vodafone-and-talktalk-case-study/>.

## About the author



### Manish Bahl

#### Associate Vice President, Cognizant's Center for the Future of Work, Asia-Pacific

Manish Bahl is a Cognizant AVP who leads the company's Center for the Future of Work in Asia-Pacific. A respected speaker and thinker, Manish has guided many Fortune 500 companies into the future of their business with his thought-provoking research and advisory skills. Within Cognizant's Center for the Future of Work, he helps ensure that the unit's original research and analysis jibes with emerging business-technology trends and dynamics in Asia-Pacific, and collaborates with a wide range of leading thinkers to understand how the future of work will take shape. He most recently served as Vice-President, Country Manager with Forrester Research in India.

Manish can be reached at [Manish.Bahl@cognizant.com](mailto:Manish.Bahl@cognizant.com)

LinkedIn: <https://in.linkedin.com/in/manishbahl>

Twitter: [@mbahl](https://twitter.com/mbahl)

## Acknowledgments

The author would like to thank Dr. Paul Roehrig, Vice-President and Global Managing Director, and Benjamin Pring, co-lead at Cognizant's Center for the Future of Work, for their significant contributions to the research and writing of this report.



---

## About the Center for the Future of Work

Cognizant's Center for the Future of Work™ is chartered to examine how work is changing, and will change, in response to the emergence of new technologies, new business practices and new workers. The Center provides original research and analysis of work trends and dynamics, and collaborates with a wide range of business, technology and academic thinkers about what the future of work will look like as technology changes so many aspects of our working lives. For more information, visit [Cognizant.com/futureofwork](https://www.cognizant.com/futureofwork), or contact Ben Pring, Cognizant VP and Managing Director of the Center for the Future of Work, at [Benjamin.Pring@cognizant.com](mailto:Benjamin.Pring@cognizant.com).

---

## About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 195 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at [www.cognizant.com](https://www.cognizant.com) or follow us [@Cognizant](https://twitter.com/Cognizant).

---

# Cognizant

### World Headquarters

500 Frank W. Burr Blvd.  
Teaneck, NJ 07666 USA  
Phone: +1 201 801 0233  
Fax: +1 201 801 0243  
Toll Free: +1 888 937 3277

### European Headquarters

1 Kingdom Street  
Paddington Central  
London W2 6BD England  
Phone: +44 (0) 20 7297 7600  
Fax: +44 (0) 20 7121 0102

### India Operations Headquarters

#5/535 Old Mahabalipuram Road  
Okkiyam Pettai, Thoraipakkam  
Chennai, 600 096 India  
Phone: +91 (0) 44 4209 6000  
Fax: +91 (0) 44 4209 6060

© Copyright 2019, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.