TRUST IN THE DIGITAL AGE

**RACHEL BARTON,
MARC BENDER,
FABRICE MARQUE**

In the digital economy, there's little room for secrets. Connected and wearable devices now provide access to consumer data that is exponentially more personal— and ultimately more valuable— than ever. But the reverse is also true. Consumers now have unprecedented visibility into the inner workings of the companies with which they do business.

How companies manage, secure and share that data is fast becoming the determining factor in profitable customer relationships. Those that get the trust equation right will be the ones best positioned to capture the most valuable customer data, as well as digital's full business potential.

TRUST COMES OF AGE

Digital technologies have dramatically increased the quantity and velocity of data that companies and customers now share. With a few clicks, consumers can determine if their providers' promises are credible, if their supply chains and work practices are ethical, or if their product information is accurate. Companies that fail to provide full transparency will see their consumers' trust erode. Our research shows that setting false expectations is the top frustration among consumers (cited by 75 percent as "extremely frustrating"). That particular breach of trust has serious consequences. Among our survey respondents, 63 percent indicated they would start looking for alternative providers, and 53 percent would stop doing business with that company immediately.[1] These percentages will likely climb, since consumers' access to digital technologies is driving ever-higher consumer expectations for visibility into a company's safety protocols, ethics policies and sustainability practices.[2]

On the flip side, digital technologies make it possible for businesses to collect and analyze massive volumes of data from individuals to personalize offerings, create new products and services, and diversify into new markets. In an Accenture survey of nearly 600 businesses around the world, 79 percent indicated they collect data directly from individuals' online activities. A third capture personal data from connected devices.[3] Figuring out how to capture, use and secure all that data has become a critical business activity.

COMPANIES COLLECT CUSTOMER DATA FROM A VARIETY OF SOURCES:

Individuals, through online customer accounts, for example: **79%**

Commercial or data-sharing partnerships: **42%**

Connected devices: **33%**

Third-party data suppliers: **33%**

PERSONAL DATA. PERSONAL DANGER.

One of the primary benefits of living in the digital world is being able to access services or transact business with the swipe of card or the click of a mouse. In exchange for that convenience, consumers have willingly shared their credit card numbers, age, marital status, gender and other information they deem to be fairly innocuous. For years, they have trusted companies to safeguard that information.

Today, that is changing. Consumers are increasingly placing conditions upon their willingness to share information. For example, 57 percent will share information if they know it won't be sold or shared. Nearly as many (56 percent) will share information if they can be guaranteed that data-protection safeguards are in place.[4] Their concerns are legitimate. Major data breaches are regular occurrences now, affecting millions of consumers.[5] Additionally, the type of data collected digitally these days is much more personal. Knowing that a company can ascertain your date of birth is one thing. Thinking that that company can access your health records, location or alarm codes is quite another.

Companies, of course, are doing all they can to pry this type of information loose. The more sensitive the data, the more insights they can generate about individuals' behaviors and preferences. And with those insights, they can tailor messages, products and services to create value for themselves or their consumers. Insurance companies use data from wearable fitness trackers to deliver personalized health tips.[6] Sneaker manufacturers invite customers to share running data to learn how their products are

THE PRIVACY OPPORTUNITY.

Consumer distrust can erode profitability. But the opposite is also true. Trust can open new opportunities to achieve sustainable economic growth. Amid growing concerns about cyber attacks and data breaches, Google, Apple and Amazon have made data protection a key element of their brand image. For them, "privacy marketing" capabilities are a stepping-stone to data monetization. Will others soon be able to monetize privacy, as well?

being used.[7] And utilities are encouraging customers to share their energy usage data with third-party providers interested in developing energy-efficiency solutions and apps.[8]

In each of these examples, companies are giving consumers control over the use of their personal data, which Accenture defines as the empowerment principle of digital responsibility.[9] It all sounds harmless—even beneficial. Thankfully, in most cases, it is. But it doesn't take much to recognize the potential danger of this information falling into the wrong hands. Imagine what a scam artist, robber, stalker or worse could do with data that reveals an individual's location, day-to-day activities, IP address, health records or alarm codes.

## DISTRUST: THE NEW FACE OF DIGITAL DISRUPTION

Customers' digital security and privacy concerns can affect businesses in expected and unexpected ways. For example, the manner in which a company secures personal data is a top determinant of loyalty for 37 percent of consumers.[10] Even more telling, 8 out of 10 consumers won't do business with companies they don't trust.[11] Adding insult to injury, their distrust is contagious. Digital enables them to voice their concerns or dissatisfaction in an amplified way.[12] In fact, we found that 40 percent of global consumers posted negative comments about an experience with a company via social media. Their digital distrust can easily influence thousands of potential customers to stay away.

Consumer privacy concerns can also hamper companies' future growth plans—particularly those companies looking to cash in on the IoT boom. It's estimated that advances in the Internet of Things and other technologies could generate business value of $100 trillion by 2025.[13] Developing products and services in the hyper-connected world of IoT depends on customers' willingness to share sensitive data about their lives, locations and behaviors. Yet, consumers' intent to purchase IoT devices and services has increased by only 1 percent in the last year.[14] Unless customers feel comfortable sharing their data, companies will not be able to reap the benefits of their IoT investments. Both companies and customers will revert to strictly transactional data exchanges.

TRUST IS A TEAM SPORT

As companies shift their focus from stand-alone products to services, they often partner with others to deliver more comprehensive solutions. Such collaborations raise additional security concerns. In an ecosystem, a company no longer has to worry just about the security of its own data, but also the risk associated with data breaches in companies with whom it is linked. This is causing companies to rethink their ecosystem involvement. In fact, 82 of companies say a lack of data security and ethical controls could exclude them from participating in other companies' digital platforms and ecosystems.[15] That might spell the end of ecosystems as we know them.

Most companies simply aren't equipped to build or manage an ecosystem that maintains digital trust. Three barriers stand in their way. The first is the inability to identify where data ownership starts and
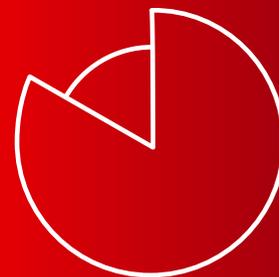
82 percent of companies say a lack of data security and ethical controls could exclude them from participating in other companies' digital platforms and ecosystems.

ends. The second is the lack of consistent protocols and standards for transparency, security, traceability or data sharing. And the third is an IT-only focus. Many companies see digital trust as a pure security or IT issue. Of course, data protection mechanisms are critical, but digital trust is also dependent on ethical standards and each organization's commitment to use data safely.

BUILDING TRUST FOR COMPETITIVE ADVANTAGE

To build the trust that the digital age demands, companies should:

- **Elevate trust to a C-suite imperative.** As trust becomes more strategic and more complicated, it's important that a Chief Trust Officer or other senior leader step up to provide strategic direction and oversight. Assign a leader capable of bringing different functional areas of the business together—customer engagement, IT and sustainability, to name a few—to create sustainable customer models and a culture of transparency and trust based on strong ethical standards.

- **Rewrite the trust equation.** Digital trust is no longer solely about firewalls and encryption. It is a reflection of the character of the organization. As such, identify its many elements—from how data is secured, managed and shared, to how ethical standards are created and enforced, to how credibly and reliably the company delivers on its promises. Strengthen each component to win the confidence of every customer.

- **Keep the customer at the center.** Building trust with consumers is, at its core, about building relationships. Give customers something in return for their personal data. Capture only what is necessary, be transparent about what you are doing, and use that information to enhance the customer experience. Finally, empower customers by allowing them to set their preferences for data sharing.

- **Embed trust into the fabric of the organization.** Data security and digital trust cannot be managed in isolation. They must be at the center of customer strategies, operating models and even product development. Foster collaboration among groups focused on digital disruption, data management, customer experiences and other business areas to optimize the value exchange and forge stronger customer connections. Encourage teams to embrace the concept of "privacy by design" and consider privacy management at the beginning of any new project.

- **Make trust a cornerstone of partnership models.** If consumers distrust one company in the value chain, they distrust all companies in the value chain. Establish common ethical standards, technical safeguards and holistic controls for all participants. Select partners that share your commitment to digital trust.

TRUST IS CURRENCY IN THE DIGITAL AGE

Businesses are banking on the opportunities afforded by digital technologies and new forms of customer engagement. A lack of digital trust can quickly derail those ambitions. In today's always-on, data-rich environment, companies need to redouble their efforts to ensure data privacy and security. They need to maximize trust along the customer journey and across all channels. Above all, they need to place trust at the center of their customer strategies and regain the customer confidence that is the prerequisite for success.

JOIN THE CONVERSATION

@AccentureStrat

https://www.linkedin.com/company/accenture-strategy

CONTACT THE AUTHORS

Rachel Barton
rachel.e.barton@accenture.com

Marc Bender
marc.c.bender@accenture.com

Fabrice Marque
fabrice.marque@accenture.com

ADDITIONAL CONTRIBUTOR

Melissa Barrett
melissa.barrett@accenture.com

REFERENCES

[1] Accenture Strategy's 2016 Global Consumer Pulse research.

[2] Accenture Sustainability Research

[3] Tim Cooper, Archie Maitland, Jade Siu and Kuangyi Wei, "Guarding and growing personal data value," Accenture Institute for High Performance, May 2015.

[4] Accenture Strategy's 2016 Global Consumer Pulse research.

[5] informationisbeautiful.net, January 5, 2017.

[6] "The Vitality Group Motivates With Data," Sync Magazine, March 15, 2016.

[7] Greg Petro, "Nike Just Does It - Keeping An Eye On The Customer," Forbes Magazine, July 8, 2016.

[8] Stuart Iler, "How to Leverage Green Button Initiative Data for Energy Consumption Apps," ProgrammableWeb, August 17, 2015.

[9] Tim Cooper, Jade Siu and Kuangyi Wei, "Corporate digital responsibility: Doing well by doing good," Outlook (Accenture), 2015.

[10] Accenture Strategy's 2016 Global Consumer Pulse research.

[11] Accenture: Digital Trust & Responsibility, Sustainability Practice, 2016

[12] Accenture Sustainability Research

[13] WEF Digital Transformation of Industries, 2015

[14] Accenture: Igniting growth in Consumer Technology, 2016

[15] Accenture: Customer Vision

ABOUT THE RESEARCH

In July-August 2016, Accenture surveyed 25,426 consumers in 33 countries to gain a better understanding of their buying preferences, attitudes and behaviors. The 2016 survey collected and analyzed responses from the largest sample of consumers in the 11 years of our conducting this research.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE STRATEGY

Accenture Strategy operates at the intersection of business and technology. We bring together our capabilities in business, technology, operations and function strategy to help our clients envision and execute industry-specific strategies that support enterprise wide transformation. Our focus on issues related to digital disruption, competitiveness, global operating models, talent and leadership help drive both efficiencies and growth. For more information, follow @AccentureStrat or visit www.accenture.com/strategy.