Digital Trust in the IoT Era
The amount of personal data that companies can now collect on consumers is unprecedented and growing. New connected devices will help companies to capture whole new categories of data at scale and use datasets in ways not yet conceived. This provides immense opportunity for businesses that can turn data into insights to drive highly relevant and compelling products and services.
As the Internet of Things (IoT) matures, the success of businesses that participate in the world of connected devices depends on the level of digital trust consumers have in them.

In fact, trust is a hugely important factor. Consumers must have confidence that the organization is collecting, storing and using their digital information in a manner that benefits and protects them. It acts as a bond between the business and the consumer, and allows product and service adoption to flourish. As the Internet of Things (IoT) unleashes an exponential jump in the data businesses have on consumers, digital trust is the gateway to monetizing its value. Companies that can establish and maintain trust will have defensible differentiation that allows them to convert data into growth instead of massive risk.

For consumers, trust is a very personal sentiment. They want to know their information is in safe hands, so businesses must create a digital space that feels as secure to consumers as the physical space in their own homes. This hinges on the four keys to digital trust that Accenture previously identified: security, privacy, benefit/value and accountability. Consumers must believe that their devices and data are secure and that their personal information will be protected. They are willing to make benefit versus risk decisions in exchange for some perceived value, but businesses must remain accountable for any lapses in protecting consumers’ digital information. The challenge is that the IoT makes building the four keys to digital trust far more complex.

As companies look to the IoT, digital trust is at a deficit. The majority of consumers remain cautious about sharing their personal information online and, when they do, they trust established brands more than other companies (Figure 1). The time is now to close the gap in consumer confidence and gain their digital trust. It is simply a prerequisite for those wanting to leverage the IoT business and technology opportunities that are just over the horizon.

54% of digital consumers are cautious about the information they share due to lack of confidence in the online security that protects their personal data.

Source: 2015 Accenture Digital Consumer Survey

They prefer to trust established brands:

1. Telecom Operators
2. Commercial Banks
3. Consumer Electronics Companies

In fact, trust is a hugely important factor. Consumers must have confidence that the organization is collecting, storing and using their digital information in a manner that benefits and protects them. It acts as a bond between the business and the consumer, and allows product and service adoption to flourish. As the Internet of Things (IoT) unleashes an exponential jump in the data businesses have on consumers, digital trust is the gateway to monetizing its value. Companies that can establish and maintain trust will have defensible differentiation that allows them to convert data into growth instead of massive risk.
The importance of trust as IoT matures

As a result, the volume of data traffic across the network is set to explode. According to Cisco¹, Global Internet Protocol (IP) traffic will reach 1.6 zetta-bytes annually by 2018, an increase of almost 300 percent compared to 2013. Projected annual IP traffic in 2018 will be greater than all IP traffic that has been generated globally from 1984-2013. The data shows that the majority of the traffic will originate on devices other than PCs and that wireless traffic will exceed wired traffic. By 2018, 57 percent of IP traffic will come from devices other than PCs.

The 2015 Accenture Digital Consumer Survey shows that by 2020, nearly half of consumers will own a connected IoT device, with strongest demand for home cameras and security, smartwatches and fitness devices. The majority of those consumers will own multiple connected devices. Consumer interest is high across many other product categories as well, including in-vehicle entertainment systems, personal health monitors and 3-D printers (Figure 2).
The expected growth in connected devices and growing data traffic is preceded by a dramatic increase in security breaches. Although data breaches have been occurring for many years, the volume and severity of these breaches continue to increase. Growing media coverage combined with financial and even political implications have intensified security concerns. Due to heightened public awareness, executives and consumers are becoming more anxious about escalating security threats.

According to Accenture analysis, data breaches are up eightfold in the past decade. In 2014–2015, Accenture estimates that the number of data breaches will more than double compared to the previous two years. Since the beginning of 2014, Accenture estimates that data breaches have affected more than 550 million consumer accounts. At this rate, by the end of 2015, nearly 900 million consumer accounts will be impacted in 2014 and 2015 alone, with some consumers affected in multiple instances (Figure 3).

Although data breaches have been occurring for many years, the volume and severity of these breaches continue to increase.
Market evolution will further escalate the importance of digital trust

While interest in IoT devices is strong, the market for many types of IoT devices is nascent and there are a number of providers seeking to capitalize on growing demand. The result is a market that is highly fragmented with many potential players vying to gain consumer attention and trust.

More than half of consumers prefer to purchase from companies specializing in a specific type of device—especially for wearable fitness, health devices and smartwatches. Consumers also have a strong preference for their current mobile phone manufacturers, which gives brands like Apple, Samsung and even Google an edge over telecom providers for these devices and associated services. About 40 percent of consumers include their telecom provider on the short list of those they would consider for various connected devices. Interestingly, only 28 percent of consumers prefer to buy a smart thermostat device from their utility (Figure 4), indicating consumer preference to purchase from differentiated companies over the ones they view as commoditized.

Since connected devices are in a growth stage, a great deal of emphasis is currently being placed on the device itself. However, over time a lot of the revenue opportunity associated with connected devices will be for services associated with those devices:

- Smartwatches have the leading potential to mirror the smartphone industry
- Home surveillance capabilities will include recurring services for ongoing monitoring, video and storage services.
- In-vehicle entertainment systems will be closely tied to connected cars and both entertainment brands and connectivity providers will be well positioned to team with car manufacturers

An interconnected environment is emerging in which businesses are building products and services designed for, created for, and specifically centered on the individual. This device proliferation leads to an explosion of data sets that are far bigger and far more personal. Technology’s ability to capture data about the individual has moved well beyond demographic information, identifying information, web surfing patterns and favorite places.
New intelligent devices help companies to capture whole new categories of data at scale and use datasets in ways not yet conceived. A smart thermostat knows when a consumer is home and when the consumer is watching television. A personal health monitor has the data that could tell an employer if someone were really sick when they called in absent from work. A connected car knows how many times a consumer had to brake hard while driving. Apps that provide directions and track location know everywhere a consumer has been in recent history. Tremendous untapped value lies in the ability to aggregate this data across devices and leverage analytics to deliver and monetize services relevant to consumers. Companies are moving in this direction to offer new services, reshape experiences and enter new markets by creating digital ecosystems across the IoT value chain (Figure 5).

Nike’s shift in its FuelBand strategy indicates that leading businesses are already thinking this way. When Nike first launched the FuelBand it both built the device and maintained the app that tracked and shared users’ runs. However, Nike revised its strategy to focus on specific elements of the experience (data, analytics and insights) and discontinued hardware production. By operating as a data analytics provider, Nike is better positioned to become a partner in the wearable device market, rather than competing for a share of it.

Mercedes-Benz is also moving into a position as a connected hub, building into its cars an application programming interface (API) to Nest thermostats at the driver’s home. The car can notify the thermostat when the driver will arrive, and the thermostat in turn adjusts the in-home temperature to the driver’s desired settings. Appliance-maker Whirlpool is making similar moves: its smart dryers include a function that allows environmentally conscious consumers to schedule energy-intensive tasks for when electricity is more abundant and rates are lower.

This immense opportunity also comes with increased accountability for protecting the security and privacy of customer information. The varied and detailed types of customer data companies can collect and leverage is massive. In the connected ecosystem, companies no longer have to worry just about the security of their own data but also the risk associated with data breaches in companies with whom they are linked. Perhaps most importantly, they will be unable to reap the benefits if consumers don’t trust the entire value chain in which they operate.
Elevating digital trust in the IoT era

FIGURE 6 | Attitudes about personal data on the internet by age and region

Overall Response

46% I’m confident that the security of my personal data is protected on the internet

54% I’m not confident that the security of my personal data is protected on the internet

Response by Age Group

14–17

42

58

18–34

48

52

35–54

58

42

55+

67

33

Response by Region

North America

52

48

Western Europe

60

40

Asia Pacific

53

47

Middle East

46

54

Latin America

52

48

Source: 2015 Accenture Digital Consumer Survey

Trusted companies will be positioned to monetize the data generated from connected devices. To that end, there are specific considerations within each of the four keys to digital trust that arise in a world of complex connectivity and value delivery.

Accountability: Picking business partners that enhance consumer trust

Aggregating IoT data and building new teaming relationships that combine services to benefit the individual will prove lucrative for companies that execute against this concept. As companies join these new ecosystems, finding the appropriate business partners is imperative. For the many companies that will not be the key data aggregator and ecosystem hub, it will be critical to define the appropriate business partners with whom to collaborate. With consumers at the center of the connected ecosystem, a key factor in being accountable to them is selecting teaming relationships that consider the level of digital trust consumers have in all parties.

Most consumers do not trust the security of their personal data on the Internet. Less than half of consumers are confident in the security of their personal data, virtually no change in security confidence from the prior year. Ten percent of consumers never share personal data online because they are not confident at all that their data is secure.

These findings are generally consistent across geographies, with less than half of consumers in most regions expressing confidence in the security of their personal information. Consumers in Western Europe show the lowest confidence in the security of their personal information—only four in 10 indicate they are confident (Figure 6).
Important considerations for digital trust in the IoT era

Among the most trusted with personal data are telecom providers and banks (Figure 7). This is not surprising given that these companies have had access to personal information for quite some time and have gradually built a level of trust. There are notable differences by age and by country. Overall, the older generation—those 55+—are significantly more likely to trust telecom providers and banks compared to younger consumers. There are also important regional and country-level differences that emerge:

- Telecom operators are highly trusted in China (56 percent), Australia (53 percent), and Germany (52 percent).
- Banks are most trusted in Sweden (61 percent), Netherlands (49 percent), and Canada (45 percent).
- Google is the most trusted brand in Indonesia (52 percent), India (43 percent), and Brazil (29 percent).
- Facebook is the second most trusted brand in each of those same countries.
- Amazon is the second most trusted brand in the US (29 percent) and UK (27 percent), trailing only banks in those two countries.

The general lack of confidence implies that companies must walk a fine line to maintain digital trust as they work to capitalize on the connected world of consumers. Within the connected ecosystem, companies need to design infrastructure that enables them to amass data while creating a trusted environment for partners and more importantly for consumers. Monitoring what data is accessed, and by whom, will become a critical function of maintaining trust. As companies are pushed to build digital trust together, a higher level of collaboration will be required.
Security: Moving away from passwords to less penetrable security

With data sharing across the IoT, security is a necessary part of every activity of every cooperative initiative, regardless of use case. There are already too many possible points of entry for security to be airtight, and with the IoT, these will be multiplied exponentially. Each company may require unique security solutions to address its own set of risks. The most immediate imperative is to verify software and security controls are able to address the latest risks and a plan is in place for responding to new risks in a timely fashion.

Consumers are feeling less secure about the reliability of usernames and passwords to protect their personal data and are increasingly frustrated with the often tedious and inconvenient process of having to manage and remember multiple passwords and usernames. To address this challenge, innovative biometric authentication methods for connecting to the internet, such as use of human finger and palm prints, irises and voice recognition, are being developed rapidly.

New data protection measures can be seen in the strategies of both Apple and Google: encrypted file systems are the default in iOS 8 and Android L.24. Importantly, the decryption key now resides on the user’s phone, outside of the corporation, shifting the burden of data protection from the provider to the user. Others are following suit. Microsoft recently announced it will support biometric authentication for devices that use its new Windows 10. The technology will allow people to use their fingerprint, iris or face to gain access to laptops, tablets, phones and other devices. Yahoo is also moving away from having users remember passwords with its new “on-demand” password. When the user clicks a button that says “send my password,” the company texts a four-character password to their phone. While similar to two-factor authentication—where the user first enters their own password, then enters a second password the company sends to their phone—Yahoo’s process eliminates the personal password step.

The 2015 Accenture Digital Consumer Survey confirms that consumers truly want alternatives to usernames and passwords to protect their security and privacy online. More than three-quarters (76 percent) of consumers are interested in using replacements for usernames and passwords and 60 percent find usernames and passwords cumbersome to use (Figure 8).
Globally, consumers want alternatives to usernames and passwords even if they do not fully understand options related to encryption, biometrics and two-factor authentication. On the high end, 92 percent of consumers in China and 84 percent in India are open to alternatives.

Using these more reliable and more secure alternative methods could increase consumers’ feeling of security and therefore trust. The challenge is to think about how to put them in place without burdening the consumer.

Privacy: Walking the fine line

For businesses focused on building digital trust, transparency and control are key components to meet consumer privacy needs. An overwhelming 90 percent of consumers felt that a range of activities violated their personal privacy, including activities related to sharing information along with ads, recommendations and offers based on location (Figure 9).

Consumers clearly want the ability to opt in for such activities. If consumers are not given the opportunity to opt in—or if they do not recall giving permission—they are likely to consider ads and offers targeted to them as a violation of their privacy.

For companies seeking to collect, store and analyze consumer data to cross-sell and up-sell by directing customers to the products they are most likely to be interested in, it will be critical to clearly and simply articulate how data will be leveraged.

Today, companies often rely on consumers clicking through terms and conditions that few consumers actually read. For example, the enrollment form for the frequent flyer program of a large US-based airline consists of nearly 3,500 words. How can a consumer be expected to understand what information they gave permission to share?

FIGURE 9 | Activities consumers consider violations of their privacy

- **38%** Sharing information about me that I do not recall giving permission to be shared
- **24%** Ads or recommendations based on my online behavior or online searches
- **23%** Ads or recommendations based on my physical location
- **22%** Offers (e.g. emails, messages), based on my online purchases
- **20%** Offers (e.g. emails, messages), based on my offline purchases
- **33%** Any of these if consumer has not opted in

Source: 2015 Accenture Digital Consumer Survey
Benefit/Value: Offering value in exchange for personal information

There are still a number of barriers to mass adoption of IoT that must be addressed in the near term. Quite often, consumers show a lack of understanding about the benefits of intelligent devices and smart technology, signifying an opportunity for providers to educate consumers about those potential benefits.

Overall, two-thirds of consumers are willing to share their personal information in exchange for some perceived value. While consumers say that cash incentives (35 percent) work best, valued content alone is often enough to incent consumers to give their personal information. Simply consider the millions of apps that are downloaded in exchange for information about that consumer.

About one in four are willing to share personal data in exchange for a better level of service or the ability to choose which data can be shared with third party business partners. Treating consumers’ personal data as a currency, and its exchange as a transaction, helps businesses to move past the perceived conflict between privacy and offering tailored services designed to fit each consumer’s requirements. That willingness to exchange personal data is built on digital trust.

Once again, we see some important differences by geography and age. There are minimal differences by gender, though men are more likely than women to provide additional personal data. Not surprisingly, consumers in emerging markets are most willing to provide additional personal information in exchange for some value—76 percent compared to only 55 percent of consumers in developed markets.

Age is also a significant factor in achieving the benefit/value balance, with 73 percent of consumers under 35 willing to exchange personal data for some perceived value, compared to only 41 percent among those 55+. Teens are twice as likely to exchange personal data for some non-monetary incentives, such as free service or loyalty points, compared to older consumers (30 percent for teens, 15 percent for 55+).

With unprecedented levels of personal data available to companies, there is tremendous opportunity for businesses to turn that data into highly relevant and compelling products and services based on an individual’s real-time information and value preferences.
Building digital trust:
Three actions to take today

To take the first steps, any company—device manufacturers, internet and social brands, telecom providers, semiconductor firms—seeking to lead in the IoT market should build upon the four keys to digital trust and consider taking these actions:

1 Nominate a chief security officer

Companies should consider having a security officer who would attend meetings where the highest-ranking leaders make major strategic decisions. The officer should have a more direct reporting relationship to the chief executive officer, providing recommendations for the company's strategic direction from a security and data privacy perspective. In most large companies, executive board members tend to have a direct role in either protecting or building shareholder value. This top security officer’s responsibilities would encompass this as well.

2 Evaluate product and service security risks—including those of your business partners

Companies need to rethink how to design and build products and services to make them more secure. More security needs to be built into each high tech product when it is designed. Security should protect a high tech company's products while adhering to ecosystem security requirements in which that product will be used. This also means that greater scrutiny is required for understanding the capabilities and risks for all partners within the IoT ecosystem, making it critical to develop the appropriate processes for screening and evaluating partner companies.

3 Use proactive product testing methods

Companies should perform proactive tests to prepare for breaches. Tests should anticipate what could go wrong and take steps to avoid them. Companies should do active penetration testing that tries to hack into their own products. The goal should be to find security vulnerabilities so they can be preemptively fixed.

Perhaps most importantly at the board and c-level, information security must be considered a business priority and security objectives should be aligned with business requirements. Given the increasing number of data breaches and growing accountability at the highest levels within an organization, the risks are greater than ever before.
Final thoughts

By taking these steps, companies can strengthen security strategies to build digital trust, which is all about consumers believing companies will protect their personal data. Digital trust is the high tech currency that should be invested in and traded to help gain competitive differentiation and help high performance.

Once companies gain digital trust, they can leverage IoT business and technology opportunities. Most importantly, they can access more consumer data from those who trust them, use analytics to unlock more value from that data, deepen customer loyalty and offer more relevant, revenue-generating services and applications.
About the 2015 Accenture Digital Consumer Survey

The Accenture Digital Consumer Survey for communications, media and technology companies was conducted online between October and November 2014, with 24,000 consumers in 24 countries: Australia, Brazil, Canada, China, Czech Republic, France, Germany, India, Indonesia, Italy, Japan, Mexico, Netherlands, Poland, Russia, Saudi Arabia, South Africa, South Korea, Spain, Sweden, Turkey, United Arab Emirates, United Kingdom and United States.

The sample in each country is representative of the online population, with respondents ranging in age from 14 to 55+. The survey polled respondents about their usage, attitudes and expectations related to digital devices ownership, content consumption, broadband constraints, digital trust and the internet of things.

References


7 2015 Accenture Digital Consumer Survey

About the Authors

Robin Murdoch
Global Managing Director
Accenture Internet & Social
robin.murdoch@accenture.com

Paul Johnson
Manager
Accenture Research for Communications, Media & Technology
paul.d.johnson@accenture.com

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 323,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.