Business Horizons (2015) **58**, 615—624

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

Internet of Things: Convenience vs. privacy and secrecy

Bruce D. Weinberg [a,*], **George R. Milne** [a], **Yana G. Andonova** [b], **Fatima M. Hajjat** [a]

[a] *Isenberg School of Management, University of Massachusetts Amherst, Amherst, MA 01003, U.S.A.*
[b] *Arthur J. Bauernfeind College of Business, Murray State University, Murray, KY 42071, U.S.A.*

KEYWORDS
Internet of Things;
Machine to machine;
Web 2.0. privacy;
Humanness;
Human experience

Abstract In this article we introduce the Internet of Things to the broad managerial community and explore one of its central tensions: convenience vs. privacy and secrecy. We clarify the ways in which IoT differs from Web 2.0 and then highlight opportunities, challenges, and managerial guidance. In addition, we explore the prominent issue of privacy and secrecy. Due to substantial increases in amounts of consumer-related data and their accessibility as well as potential tradeoffs in benefits associated with IoT and in properties of humanness associated with the consumer experience, the managerial issue of privacy is elevated to a level never before realized—perhaps on par with, or worthy of inclusion as an element of, the classic marketing mix.

1. It's all connected

Suppose a bicycle racer is on a training ride for the Senior Olympics. On the way home, the bike's shifter mechanism for the rear cogs gets a little wonky, making it difficult to use the full range of gears. More energy than expected will be required to propel the bicycle. Getting home is not an issue. However, there are two problems at hand: repairing the shifter and getting a bit more nutritional fuel so as to maintain the desired quality of the ride. Through technology, repairing the shifter may be handled as follows: First, a bicycle internal diagnostic mechanism identifies the problem with the shifter. The bicycle then engages the Internet and communicates the need for a shifter part to the rider's personal hub computer and database. Next, the personal hub, considering time to delivery, part cost, and other relevant factors, either sends out an order to a desired retailer or puts out a bid request to a variety of electronic devices that represent retailers and providers. Finally, a deal is struck and the part is ordered.

The second problem engages a different set of systems and processes. The racer is wearing clothing

* Corresponding author
E-mail address: weinberg@isenberg.umass.edu (B.D. Weinberg)

0007-6813/$ — see front matter © 2015 Kelley School of Business, Indiana University. Published by Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.bushor.2015.06.005

that keeps track of vital signs such as heart rate, hydration, body temperature, energy use, muscle strength, training 'zone,' and foods processed. In addition, this information is processed in real time by insurance providers to assess compliance with agreed premiums or to apply appropriate surcharges in accordance with activity and diet. An onboard mapping system is monitoring current location and can find a variety of places to obtain food or beverage in addition to calculating the distance to a destination. The health-vitals system and the mapping system coordinate in determining the additional energy needed by the rider and where to acquire nutrition to maintain the necessary energy level. A course to the retailer is mapped, as is the ensuing route back home.

Today, many of the systems described in this scenario are available. However, all of the technical aspects of infrastructure and communications to seamlessly facilitate the scenario are *not* in place. But the promise and notion of it is at hand—and reasonably close. Called the Internet of Things (IoT), it can solve problems and create opportunities for a variety of entities, including consumers, providers, employees, organizations, manufacturers, communities, cities, and governments, among others. Along with that, though, it may create new problems and raise concerns and associated costs, such as those pertaining to privacy.

In an accessible and non-technical manner, this article introduces the Internet of Things to the broad managerial community; clarifies the way in which it differs from Web 2.0 and earlier uses of the Internet and related communications; and highlights opportunities, challenges, and managerial guidance, with special attention to the highly prominent issue of privacy.

2. The Internet of Things is watching you

When the Web emerged, organizations and people purchased Internet real estate in the form of domain names and built it out with websites. Consumers shopped and people read the news online, but information applications were typically static and one-way in communication orientation (e.g., provider to consumer). Then Web 2.0 gathered steam. Services allowed for dynamic information in a variety of forms and enabled n-way conversations and collaboration. Blogging, liking, tweeting, writing online reviews, sharing videos and photos, and such became commonplace (see Kaplan & Haenlein, 2010). With social media, people keep private relatively fewer bits of information and reveal secrets more often. Now a new wave of Internet-connected technologies is gaining steam: The Internet of Things (IoT)—a class of devices and associated processes that will lead to sharing and exposing more information and keeping fewer secrets.

Indeed, IoT may impact stealthiness in a variety of situations. For example, when a patient visits a doctor for a checkup, it may be harder to keep secret a lack of exercise and poor eating habits and behaviors. Home insurers may be able to more easily discover that doors to a house were unlocked during a breaking and entering crime. Auto insurers may be able to note when a vehicle exceeded the speed limit. Similarly, IoT could be used to an individual's advantage: It could reveal a flaw or hitch in one's golf swing and consequently correct the imperfection.

Consumers will have a heightened awareness that data associated with their being, actions, thoughts, and emotions are indeed a currency and are associated with their humanness. Thus, as society—including its business landscape—moves into a more ubiquitous technology and information era, consumers will place greater emphasis and importance on data ownership and data flow-related issues such as privacy, and relatively lesser weight on traditional marketing factors such as the marketing mix. Note that marketing mix elements are of the hand of the marketer but consumer data are generated by and of the consumer. These data are reflections of consumers and can be used to characterize and control them. Thus, organizational and marketer performance constructs, such as reputation and brand perceptions, will be based increasingly on privacy and respect for consumer data, which in turn can signal respect for consumers.

3. What in the world is the Internet of Things?

A wide variety of technologies are called IoT devices. It is estimated that there were about 16 billion IoT devices in 2014, and forecasts point to as many as 50 billion devices in 2020 (Clark, 2014; Middleton, Kjeldsen, & Tully, 2013; Press, 2014). Climate control devices like Nest regulate temperature within a building in a way that satisfies consumer preferences and minimizes energy costs. Fitbit products monitor physical activity and associated vital information, such as heart rate and calories burned, in order to enhance health and well-being. Similarly, Ralph Lauren offers the Polo Tech shirt, which also transmits biometric data. Self-driving cars will allow people to leave the driving to machines, and IoT-capable smart cars

Table 1. Classifying Internet of Things devices by application*

Wearables	**Health Care**
- Entertainment	- Remote monitoring
- Fitness	- Ambulance telemetry
- Smart watch	- Drug tracking
- Location and tracking	- Hospital asset tracking
	- Access control
Building and Home Automation	- Predictive maintenance
- Access control	
- Light and temperature control	**Smart Manufacturing**
- Energy optimization	- Flow optimization
- Predictive maintenance	- Real-time inventory
- Connected appliances	- Asset tracking
	- Employee safety
Smart Cities	- Predictive maintenance
- Residential e-meters	- Firmware updates
- Smart street lights	
- Pipeline leak detection	**Automotive**
- Traffic control	- Infotainment
- Surveillance cameras	- Wire replacement
- Centralized and integrated system control	- Telemetry
	- Predictive maintenance
	- Car to car, and car to infrastructure

Source: Adapted from Texas Instruments (2014)

that are driven by people will be able to provide functions such as detecting when a driver is sleepy and consequently taking corrective actions.

There are efforts to categorize IoT devices. Although we believe that a useful grouping will be emergent, a reasonable way to classify is by application. Texas Instruments (2014) identifies six main areas of application: wearables, building and home automation, smart cities, health care, smart manufacturing, and automotive (see Table 1).

3.1. Important distinguishing characteristics of Internet of Things

It can be challenging to comprehend what comprises an IoT device. We attempt to provide some clarity by identifying characteristics that, we believe, distinguish IoT. Technology devices are connected to and can receive or transmit data via the Internet; these include computers, laptops, servers, smartphones, tablets, and a variety of other devices that consumers now employ for utilizing the Web through a browser. However, as was discussed earlier, IoT devices extend beyond being technologies for consumers to directly access the Internet via the Web; they enable more of the physical and natural world to be integrated into and to become accessible via the Internet (see Figure 1). In order to better recognize potential opportunities in IoT, it is important to understand key distinctions between a Web-based environment and an IoT-based environment. In the following sections we explain defining characteristics as they relate to the nature of Internet-connected devices, emphasizing the key process-related aspects of data, data entry, data sharing, learning, and decision making. The differences are highlighted in Table 2.

3.1.1. Data

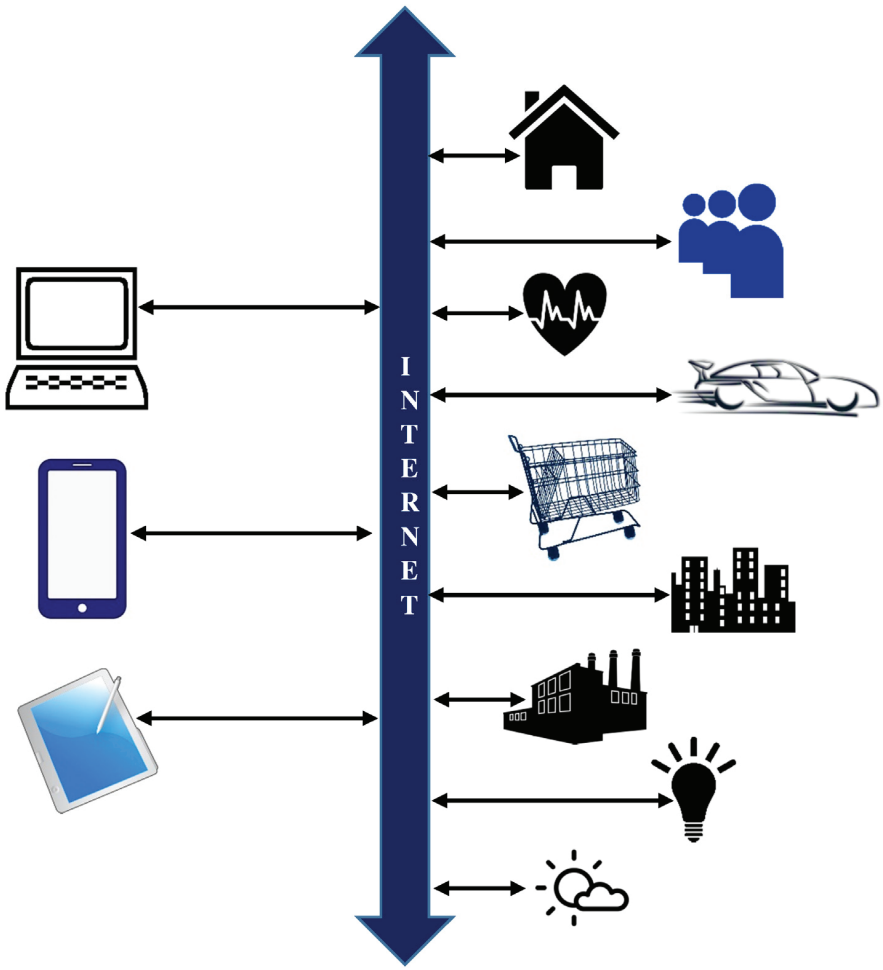
In a Web-based environment, consumer-related data reflecting behaviors is compiled by online interactions in a digital world. Data may be of a variety of types, such as text, image, video, audio, clicks, page visits, or other cookie-related types of information. This data tends to be created, generated, or entered by a consumer.

In an IoT-based environment, devices monitor and record data related to consumer behavior in the natural, non-digital environments in which a consumer behaves. For example, the Nest thermostat monitors and records temperature conditions and consumer behavior and preferences within a building in order to learn and optimally manage the temperature. A consumer does not have to actively participate for the device to collect data.

3.1.2. Data entry

Consumers in a Web-based environment actively manipulate devices to interact directly with the Web. For example, a consumer may use a laptop to shop online, direct a browser to a particular

Figure 1. Shifting from a Web-based Internet environment to an Internet of Things-based environment



webpage for a product at an online store, put a product in a digital shopping cart, and then purchase the product after clicking on checkout and entering relevant transaction information.

Consumers can interact with IoT devices, but in many cases they don't directly enter the data. Rather, IoT devices by themselves monitor and retrieve relevant data from the environment and a person. For example, an activity tracking Fitbit product can monitor a consumer's exercise and sleep behavior and can record data such as number of steps taken, duration length of a workout, distance traveled, and heart rate.

3.1.3. Data sharing

Consumer information related to Web behavior is typically shared internally within an organization or externally with affiliated third parties or partners, although some organizations do share data with others.

In an IoT environment, data are shared with providers *and* with other devices. For example, while driving home from work on a hot day, an automobile embedded IoT-device—or even a smartphone—may communicate a consumer's location and estimated arrival time to the home climate control IoT-device. This would enable it to set the temperature in the house at the right time based on consumer preference and habit.

3.1.4. Learning

Providers, marketers, and websites learn about consumers based on their activities inside the digital world, such as shopping online and using social media. Again, these activities may be recorded in the form of cookies or transactional purchase information. These Web-related behavioral data can be used for learning consumer behaviors.

IoT devices learn about consumers by observing their habits, tendencies, and preferences as well as

Table 2. Key distinctions between Web-based and IoT-based environments

Data and Related Processes	Web	Internet of Things
Data	Online/Digital, environment/context largely constructed by providers	Physical. Environment/context largely constructed by nature, with many aspects/contexts created by consumers.
Data Entry	Active, Consumer	Passive, Devices
Data Sharing	With other providers	With other machines
Learning	Actions in online/digital world	Actions in natural/physical world
Decision Making	Providers, more fixed/static, less real time	Machines, dynamic, more real time

their environments. Learning is based on behaviors and phenomena in the natural, physical world as opposed to the strictly online world.

3.1.5. Decision making

Marketers use Web-related data in making decisions about engaging and serving consumers with respect to their online behaviors. Decisions are not necessarily made in real time from a consumer perspective, as some 'more than immediate' amount of time may pass between the recognition of a consumer problem and the provision of a provider solution.

On the other hand, IoT machines are constantly monitoring the environment through sensors and dynamically making decisions and associated changes in real time given these environmental conditions and consumer or other stakeholder preferences. For example, smart pills—that is, pills that include microchips which communicate with other devices and thereby a consumer, physician, or some other stakeholder—can provide information about their journey and employment through a consumer's body. This real-time monitoring and communication could yield, if warranted, dynamic changes in treatment or action toward a consumer who ingests a smart pill.

4. Opportunities and concerns

Many are predicting that the economic impact of IoT will be huge. Estimates by a number of well-respected organizations range widely. For example, IDC forecasts a global market for IoT of $7.1 trillion in 2020, and General Electric estimates that IoT could add as much as $15 trillion to global GDP by 2030 (Press, 2014). However, there may be several tradeoffs and concerns associated with the proliferation of the IoT. This section highlights more prominent aspects from both sides of the coin; the central issue of privacy is accorded its own distinct, more detailed analysis.

4.1. Benefits

IoT can benefit organizations by enhancing data collection, enabling real-time responses, improving access and control of devices, increasing efficiency and productivity, and connecting technologies.

One benefit of IoT is enhanced data collection. Today's big data will soon be tomorrow's little data. IoT creates an opportunity to more frequently collect data of a known type(s) or of a finer grain. For example, a consumer wearing a health-related IoT device may allow for constant collection of vital information, such as pulse, body temperature, and distance traveled. These data could be used to optimize outcomes (e.g., weight loss or fitness) for a person. Data could also be collected for finer grain health-related phenomena such as blood flow, neural activity, or—ultimately—protection from life-threatening afflictions.

As an added benefit, the data can be collected immediately to allow for real-time decision making and action. This would enhance restocking or other supply chain management services. For example, pay-as-you-go could be broadened beyond mobile phone services and automobile rentals (e.g., Zipcar) to almost any application, such as insurance. In addition, pricing in a variety of contexts that tend to be fixed, such as parking meters or vending machines, could become dynamic.

A widely realized benefit of the Internet is the ability to have greater access to and control of Internet-connected devices. For example, people can access and utilize their home computers or cable television service when away from home. This type of access and control will extend to IoT devices. For example, a CMO could view a dashboard that shows real-time traffic flow patterns within a retail outlet, and have control of in-store elements, such as display monitors, audio, lighting, and shelf stocking. IoT-embedded smart cars, traffic lights, parking areas and meters—and, even more broadly, cities—could reduce the number or impact of traffic jams or time to find a parking space, which in turn

could yield better quality of life in both professional and personal aspects (Kavis, 2014).

As with many technologies, it is easy to imagine increased efficiencies in a variety of applications, such as energy use. Porter and Heppelmann (2014) see the potential for a huge gain in productivity and improvements in value chain processes such as product design, marketing, manufacturing, and after-sale service. It is reasonable enough to imagine that IoT components and products with embedded sensors and other 'smart' IT-related componentry would enhance many processes. For example, Stanley Black & Decker placed wireless-enabled RFID tags on a variety of manufacturing materials to provide real-time information to assembly workers, supervisors, and managers. This yielded significant productivity gains in a variety of areas including equipment effectiveness, inventory management, labor utilization, and customer service and delivery (Cisco, 2014).

IoT can also enhance productivity at a larger scale and in systems where coordination of many pieces is vital. With proper coordination of IoT, systems could be formed and blended to work together seamlessly. For example, homeowners could have a system where a variety of property-related elements—such as lighting, locks, televisions, and kitchen appliances—could be tied together into a 'connected' home. Combined, these elements could be used to deliver greater efficiency, effectiveness, and satisfaction.

4.2. Concerns

Aside from privacy, which is discussed in its own section, there are a number of concerns and problems which may prove challenging to manage.

More data will be generated, will need to be stored, and will need to be processed. Some estimates place growth in the world's data generation from about 4 zettabytes (i.e., 10^{21} bytes) currently to approximately 40 zettabytes in 2020 (Adshead, 2014). New technologies and algorithms for processing and storing data will be needed.

Ownership is also a concern. Who owns the data in a system where a variety of parties co-creates and adds value? This has been an issue in social media and in other cases where data are generated or shared through third-party agents. We suspect that issues related to data ownership may create friction and disputes, particularly when the data are of a personal nature.

In addition to concerns related to data processing, storage, and ownership, unanswered questions regarding interoperability, communication, and standards will need to be addressed. Providers and manufacturers will employ a variety of different approaches with respect to IoT, such as data structures and communications, but for devices to ultimately work together, some sort of coordination or set of standards will need to be defined. Organizations with existing popular ecosystems such as Amazon, Apple, and Google may attempt to exert power to control IoT. This could have positive effects with respect to accelerating applications; however, it could also have negative effects in that it might stunt innovation and squelch consumer choice.

5. Privacy

Data and data-related processes such as generation, acquisition, transmission, and interpretation are central drivers in the design and application of IoT. Without data, IoT does not exist. Indeed, IoT is about the data, particularly that which is consumer related. It is one thing for an organization to obtain and utilize for decision making one's birthdate, income, clicks on a website, comments on social media, and the like, but it will be something entirely different for a connected set of organizations and machines to have access to and to utilize information about the environment in which one behaves and exists—for example, personal health-related information such as blood composition and dietary habits such as foods and beverages purchased and consumed. As IoT-related systems capture more of the entirety of a consumer's being in the form of data, it will be as if more of a person will be inside the Internet and is being passed around from machine to machine. Thus, respect for consumers' being and their privacy is at the heart of the consumer experience with IoT. Consumers will consider and act on the tradeoffs associated with the conveniences offered by IoT and the costs and losses in privacy.

5.1. Privacy, security, and hacking

Privacy and security are arguably the most prominent issues; they are at the heart of trust, relationship building, and exchange. With the proliferation of technology and the associated growth in data and databases, the opportunity for compromise can increase, and the effects can be great. Widespread hacking has hit some of the largest companies in the world—including Anthem, Apple, Home Depot, JP Morgan Chase, Sony, and Target—and it has exposed highly sensitive information such as social security numbers, credit card numbers, and corporate strategy, and has created negative outcomes such as costs associated with stolen money and identities.

Although a tremendous hassle to live through, solutions for cleaning up the mess associated with security breaches have been put in place (e.g., credit card protection, identity theft protection).

A security breach associated with IoT could be more costly. One might wonder: What could be more costly than identity theft? Loss of life. Really? Really! Recall that IoT devices connect physical objects to the Internet. Hacking into a database of information is one thing; hacking into a physical device in the proximity of a person and gaining control of it could be disastrous. Consider automobiles. Imagine the outcome of someone wrestling away control of a motor vehicle. This is not hypothetical. There are actual reports of automobiles being vulnerable to hacking (Shepardson, 2015).

Imagine the risk with respect to health care. The effectiveness and degree of care associated with connectivity to a consumer's vital signs and systems can be comforting on the benefit side. However, were these systems to be hacked, allowing uninvited access to, say, a person's heart or any other major organ with which a device interacts for monitoring and regulation, a nefarious actor could potentially create significant or catastrophic damage to a person.

There is greater need for privacy and security lock-down when it comes to IoT. There will be more (sensitive) data and more access to the physical world in which society lives, and it can't be assumed that successful, experienced companies with great talent will always do the right thing. Consider Lenovo's installation of Superfish Adware on its computers, which tracked consumers' every online movement, even when they thought they were using the computer in a private/secret mode. It made Lenovo users increasingly susceptible to hacking threats and the loss of privacy (Rosenblatt, 2015).

5.2. Privacy and relationship marketing

Given the increased importance of privacy in a more advanced technological and connected world, it is critical for privacy to be a more common consideration throughout an organization and the various processes employed in serving customers and solving their problems. Just as the relationships among various inputs and outcomes is considered in Total Quality Management, the relationships among privacy and various consumer-related decisions and actions (e.g., product offerings) need to be considered.

In an IoT-based world, privacy evolves from something elementary for which there needs to be a policy or checkbox to being a prominent factor in the consumer experience. Again, in a world with significant increases in connectivity, data, personal sensitivity of data, data transmission, and potential impact of data on a consumer's being, a consumer's trust and relationships will be based more on how well privacy is respected and maintained. Indeed, an organization's management of privacy is becoming increasingly representative of its respect for consumers and, in turn, consumers' trust in the organization and brand.

5.3. Privacy and humanness

In IoT exchange environments, there are more data that can be used to define and to influence people. Will these data, which in digital form are coded as strings of zeroes and ones, lead marketers to view consumers strictly as data, slotting them into fixed categories and treating them with sterile precision in accordance to their assignment? And through the acquisition and sharing of these data—perhaps in the end, without much choice by those from whom the data are sourced—will consumers relinquish important aspects that define their humanness, and thus feel less satisfaction?

In the context of mortality and being human, Gawande (2014, p. 86) draws upon Dworkin (1986) and his perspective on autonomy to put forth, "we want to retain the autonomy—the freedom—to be the authors of our lives. This is the very marrow of being human. . . .All we ask is to be allowed to remain the writers of our own story. That story is ever changing. . . .We want to retain the freedom to shape our lives in ways consistent with our character and loyalties." Although he was writing about mortality when framing that "the battle of being mortal is the battle to maintain the integrity of one's life" (Gawande, 2014, p. 86), we believe it applies when one, through technology and associated data, can be increasingly represented, influenced, and controlled and as a result have choices censored. The autonomy of one's data and thus one's self should be respected and the individual should be provided freedom of control.

We believe that the human condition calls for and requires sufficient privacy. Indeed, privacy and all that it represents or entails is a sine qua non of humanness. Without it, consumers may feel like—and become—empty souls and vessels through which organizations derive profits.

6. Managerial recommendations for engaging the Internet of Things

Technology takes on a greater presence and role in a world where the Internet of Things is applied to problem solving and life. A prominent part of this

will involve more machine-to-machine communication, interaction, decision making, and action. However, given the limited nature for machines to learn on their own, the importance of effective process design and associated execution becomes more critical. There will not only be more moving pieces, but also less direct human involvement and presence in many IoT-related actions. Organizations that plan to employ or develop IoT-entwined solutions to problems should devote careful attention to a variety of areas, including privacy by design.

6.1. Technologist and analytics skills become more critical

We see an increasing need for marketers and managers to have training and take an approach to think more like a technologist or computer scientist. At the core of IoT devices is computer technology with associated programs and hardware for sensing, communicating, and delivering benefits. A telephone becomes a computer with phone-calling capabilities (e.g., smartphone); a watch becomes a computer and communication device that can keep time (e.g., Apple watch); an automobile becomes a computer on wheels (e.g., self-driving cars). And a central part of computer-based technology is data and data processing. Thus, it is critical to have greater data management and analytical skills. Organizations that can raise their skillset in these areas are going to have more potential to effectively leverage the IoT.

6.2. The human condition

Thinking more like a technologist does not suggest thinking less like or about people. In fact, we argue that it becomes more important to consider the human condition when designing technology-based solutions. We believe there is a tendency to use technology as a mass market solution to a problem in which solutions address the major issues or are believed to be robust enough to provide a reasonable solution to any problem. However, such solutions may overlook smaller details or individual preferences that may comprise the long tail and therefore may be less satisfactory than imagined.

For example, consider automated phone call-in systems where customers "Listen closely as options may have changed. . .Press 1 for. . .Press 2 for. . . ." It seems like a grand way to handle a large volume of calls on a variety of topics. However, in application, too many consumers may be frustrated by such systems. Brands take a hit when this happens. A method intended to enhance customer service can ironically result in annoying customers. Thinking more fully through the human condition will yield more effective solutions.

6.3. Design, planning, and product checking

It will become critical to think more broadly about design and planning as offerings become entwined in a collaborative network of technology, people, and other offerings. In a system where people may be less involved and machines more directly involved in real-time problem solving, it will be very important to plan along a variety of dimensions, such as product design, customer experience design, and privacy design. It will become more important to get it right the first time. However, increased connectivity should allow for faster problem identification, diagnosis, and corrective action.

6.4. Real-time network minded

As the Web and social media utilization have become more commonplace, we've observed that users of these technologies expect greater speed in response, information flow, and problem solving. Indeed, more people expect their problems to be handled in real time, and for corresponding solutions to be quickly developed and delivered. Although Web 2.0 applications and tools of today allow for faster input and response than did the first generation of Web solutions, the need for speed will increase with IoT.

IoT will further increase the speed of and possibility for real-time, solution-related actions to problems. It will be critical not only for people to design machines that can deliver real-time solutions but also for employees of organizations to think, respond, and act faster in IoT contexts. In addition, it will be critical for providers to think more in terms of networks and connectivity when developing solutions. To make this point more concrete, we'll recall a time not too long ago when it was not that uncommon for a car dealer to take days or weeks to locate a vehicle of choice that was currently unavailable on the lot. Today, a car dealer had better be able to tap into a dealer network and provide this sort of information soon after a consumer asks for it; if he or she cannot, a potential sale could be walking out the door faster than it would take for a car to go from 0 to 60 miles per hour.

6.5. Further blurring of lines between professional and personal lives

As more elements of one's surroundings and aspects of one's life become connected via the Internet, we expect more blurring between one's personal and

private lives. Today, through social media, employees and organizations can share broader viewpoints, including those that are their own; and employers can search and learn more about an employee's, prospective employee's, or consumer's personal life via his/her social media behavior. The impact or usability of this information may vary; it could range from hiring to promoting to firing. Whatever the impact and usability, we expect more blurring of professional and personal lives as more elements of life become connected via IoT devices.

6.6. Privacy by design

Heretofore, marketers in a predominantly analog world have placed substantial weight on the marketing mix and the aspects of quality within those elements, such as service quality. They have devised ways to enhance the mix offering, such as through product design. However, now, with extensive consumer data inextricably linked to the implementation and effectiveness of IoT and the resulting elevated importance of privacy, it becomes critical for marketers to raise their game as regards privacy quality, respecting consumers, and building and maintaining strong, trustworthy customer relationships. Privacy by design is a mechanism for doing this.

Privacy by design is a process that calls for proactive consideration of privacy objectives and aims from the start, then continues throughout the design and delivery process of products and related actions (Cavoukian & Jonas, 2012; Milne, 2015; Rubinstein, 2011). Cavoukian (2009) identified seven foundational principles associated with a privacy by design process: (1) privacy should be proactive and preventative rather than reactive and remedial; (2) privacy is a default condition rather than an option to be selected; (3) privacy is embedded in the design of a product or interaction and is not an add-on, after the fact consideration; (4) privacy does not impede the full functionality of a product; (5) security is applied to protect privacy throughout an entire system wherever sensitive data may travel and throughout the lifecycle of the data; (6) privacy procedures are visible and transparent to support accountability and trust in delivering on privacy related promises and objectives; and (7) privacy design reflects respect for users' interests and being and empowers them to manage their data through actions pertaining to consent, accuracy, access, and compliance.

7. Summary

The Internet of Things is underway yet much of the script related to it is unwritten. We believe that it represents the next substantial phase of Internet use that will significantly influence consumer behavior and as a result bring about a variety of new offerings from providers and ways in which consumers and firms *and machine*s will engage. In this article, we provided an accessible overview of IoT; distinguished it from Web 2.0; introduced benefits, costs, opportunities, and concerns; and gave special attention to privacy, an issue that we believe will be elevated to a level of importance to at least equal that of the marketing mix elements.

References

Adshead, A. (2014, April 9). *Data set to grow 10-fold by 2020 as internet of things takes off*. Retrieved April 3, 2015, from http://www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario, Canada. Retrieved April 3, 2015, from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Cavoukian, A., & Jonas, J. (2012, June). *Privacy by design in the age of big data*. Information and Privacy Commissioner of Ontario, Canada. Available at https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf

Cisco. (2014). *Leading tools manufacturer transforms operations with IoT*. Retrieved April 3, 2015, from http://www.cisco.com/web/strategy/docs/manufacturing/c36-732293-00-stanley-cs.pdf

Clark, D. (2014, January 5). 'Internet of Things' in reach: Companies rush into devices like smart door locks, appliances, but limitations exist. *The Wall Street Journal*. Retrieved April 3, 2015, from http://www.wsj.com/articles/SB10001424052702303640604579296580892973264

Dworkin, R. (1986). Autonomy and the demented self. *The Milbank Quarterly, 64*(2), 4–16.

Gawande, A. (2014). *Being mortal: Medicine and what matters in the end*. New York: Metropolitan Books, Henry Holt & Company.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons, 53*(1), 59–68.

Kavis, M. (2014, July 21). Don't underestimate the impact of the Internet of Things. *Forbes*. Retrieved April 3, 2015, from http://www.forbes.com/sites/mikekavis/2014/07/21/dont-underestimate-the-impact-of-the-internet-of-things/2/

Middleton, P., Kjeldsen, P., & Tully, J. (2013, November 18). Forecast: The Internet of Things, worldwide, 2013. *Gartner*. Available at https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-

Milne, G. R. (2015). *Digital privacy in the marketplace*. New York: Business Expert Press.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 66–68.

Press, G. (2014, August 22). Internet of Things by the numbers: Market estimates and forecasts. *Forbes*. Retrieved April 3, 2015, from http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/

Rosenblatt, S. (2015, February 20). Lenovo's Superfish security snafu blows up in its face. *cnet*. Retrieved April 3, 2015 from http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/

Rubinstein, I. (2011). Regulating privacy by design. *Berkeley Technology Law Journal, 26*(3), 1409—1456.

Shepardson, D. (2015, February 8). Report: Cars are vulnerable to wireless hacking. *The Detroit News*. Retrieved April 3, 2015, from http://www.detroitnews.com/story/business/autos/2015/02/08/report-cars-vulnerable-wireless-hacking/23094215/

Texas Instruments. (2014). *Application areas for the Internet of Things*. Retrieved April 3, 2015, from http://www.ti.com/ww/en/internet_of_things/iot-applications.html