Bryant University
DigitalCommons@Bryant University

Honors Projects in Computer Information Systems

Senior Honors Projects

4-2014

The Internet of Things

Kyle Ebersold
Bryant University

The Internet of Things

The Honors Program
Senior Capstone Project
Student's Name: Kyle Ebersold
Faculty Sponsor: Dr. Richard Glass
April 2014

Table of Contents

ABSTRACT

The Internet of Things (IoT) is the next evolution in Internet technology—creating a more dynamic and integrated entity that connects virtual and physical worlds in highly unified and increasingly useful ways. The IoT takes advantage of radio-frequency identification (RFID) and sensor technology to integrate extensively with our physical environment. The world is currently poised to experience widespread use of this potentially disruptive technology which employs radio tags to uniquely identify and create computerized inventories of all objects and persons. With the information that the IoT makes available on real-world objects, the world will become even more highly connected than it already is by connecting and facilitating human-to-human (H2H), human-to-thing (H2T), and thing-to-thing (T2T)--also referred to as machine-to-machine (M2M)—interactions. The purpose of this research project is to conduct a review of the IoT as it pertains to individuals and businesses, and to perform an exploratory study that focuses on individual perceptions and level of awareness relating to this technological revolution. The project's scope includes 1) a thorough literature review to define the IoT as it is currently understood and to discuss its potential as a disruptive technology with societal implications, and 2) a discussion of information ethics as it pertains to innovative and disruptive technologies. The latter part of the project presents and discusses the results of a survey of college students designed to explore their perceptions of the IoT with regards to the constructs of convenience, privacy, security, and trust surrounding this new technology. College students were selected as the focus of the survey as they will directly experience this technological revolution in full force as it continues to rapidly develop while today's students begin to take on greater responsibility as tomorrow's leaders in business and society.

LITERATURE REVIEW

Introduction

The Internet as it now stands exists as a nearly 50 petabyte data repository created by input information from human beings. Its structure was built via an unimaginable sum of entries by someone who either typed on a keyboard, pressed a button on a mouse or other device, took a picture, scanned a bar code, or otherwise performed a human interaction with a machine. Today, there is more information available to an individual via computer technology than ever before in the history of mankind. According to Google CEO Eric Schmidt at a California conference in August 2010, "Every two days now we create as much information as we did from the dawn of civilization up until 2003" (TechCrunch). Despite its status as the largest modern-day information source available, the Internet lacks the ability to connect back to the real-world in the direct way machine-to-machine (M2M) technology can.

Enter the Internet of Things, commonly abbreviated IoT—a way of revolutionizing the current Internet into a more dynamic and integrated entity that connects to the physical world in highly unified and increasingly useful ways. Accredited to Kevin Ashton from the Auto-ID Center at the Massachusetts Institute of Technology, the IoT takes advantage of radio-frequency identification (RFID) and sensor technology to integrate extensively with our physical environment.[19] The claim for success of a more integrated environment through use of these technologies stems from the notion that if all objects and persons were equipped with radio tags, they could be uniquely identified and inventoried by computers. With this information on real-world objects, people could then interact with their objects via the Internet to locate and/or control them remotely.

With the advent of Internet Protocol Version Six (IPv6) combined with the power of parallel computing, the IoT could effectively store addresses for an estimated 50 to 100 trillion objects and provide the infrastructural support needed to perform such actions as locating your car keys using tracking and GPS to controlling your home's climate control or lighting from the opposite side of the globe for the entire human population. Control of objects in this highly integrated manner provides for effective uses in numerous applications for the home, personal use, work environments, and public sector applications such waste management, urban planning, sustainable urban environment, continuous care, emergency response, intelligent shopping, smart product management, smart meters, smart grid, and other smart events.

The IoT would make the world even more highly connected than it already is. Its main philosophy is to make everyday objects completely interconnected in every possible way to provide for effective human-to-human (H2H), human-to-thing (H2T), and thing-to-thing (T2T) (or machine-to-machine (M2M)) interactions. It would quite literally place the world at one's finger tips through a cyber-physical system that connects computational processes and the physical world. With the current capabilities of RFID, sensor networks, and GPS, we are well-positioned to see this evolution of the Internet within the next two to three decades, and some of this development has even already begun. This trend toward greater interconnection and more massive amounts of data raises many questions in the field of information ethics, including privacy, accuracy, property ownership, and access. The implications of this revolutionary trend for individuals and businesses are of great importance to all members of modern society as the Internet entity continues to rapidly evolve.

Overview of The Internet of Things

M2M Design and Architecture

> *"Whether the Internet of Things comes to pass in a satisfying way will depend critically on how the emerging M2M ecosystem is architected."*
> By Charles McLellan[2]

> *"The proliferation of Internet-connected devices that interact without human intervention is creating new possibilities in data gathering, predictive analytics, and IT automation."*
> By Bill Detwiler[2]

Design of the Internet of Things will consist mostly of low-bandwidth, upload-based traffic that delivers and processes information in near to real-time. The microprocessors making up the "things"—the "machines" in machine-to-machine (M2M)—will be extremely low-power or self-powered devices that can be placed in goods, pets, cars, credit cards, passports, CCTV street cameras, elevators, and so on. These physical entities will report their identity and state, or state of surroundings, via to an Internet-connected IT infrastructure.[1] At its core, the IoT exists as tiny sensors collecting and automatically transmitting data to servers and/or the cloud. Useful charts and dashboards would then be quickly generated to provide deeper insights and real-time feedback for faster and better decision-making.[3]

Anything with a sensor becomes a node in the IoT. Sensors gather and/or disseminate data such as location, altitude, velocity, motion, temperature, humidity, illumination, humidity, blood sugar, air quality, soil moisture, and more. They are not computers as we know them, but rather hardware that records certain conditions and transmits and receives specifically related information via the Internet.

Several network structures effectively serve to support the underlying IoT architecture. Local area communications are short-range, local area network technology such as RFID, NFC, Wi-Fi, Bluetooth, XBee, Zigbee, Z-Wave, and Wireless M-Bus. Wired connections also support short-range applications, including Ethernet, HomPlug, HomePNA, HomeGrid/G.hn, and LonWorks.

Additionally, long-range, wide area communication technologies support an overarching infrastructure which includes mobile networks like GSM, GPRS, 3G, LTE, WiMAX; and satellite. Wired long-range connections, such as SIGFOX, TV white space, and NeulNet, also add to this application. See Figure 1 for communication technologies currently used with M2M systems.

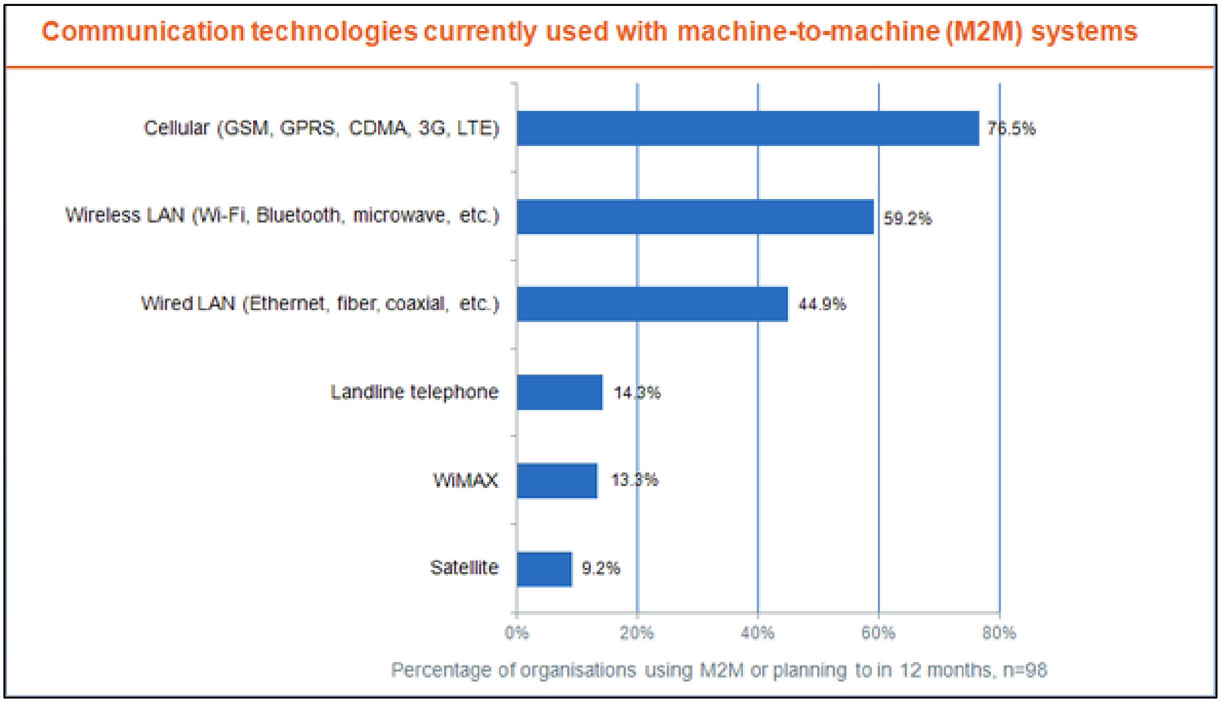


Figure 1 – Communication Technologies Currently Used with M2M Systems[4]

Local scanning devices made up of short-range sensors in a restricted area will also add to this infrastructure on a mobile and micro level. These devices can move between networks, but are scanned locally (e.g. RFID tags, credit cards).

Storage and analytics made up of massive, scalable storage and processing capacity will support data analysis of the sensor-reported data. Both transient and permanent capacity is highly likely to live in the cloud except for particularly sensitive cases involving great need for security.

User-facing services including the development of front-end web-based platforms for reporting and analytics will also complement the back-end storage and analysis architecture.

See Figure 2 for a visual depiction of the anatomy of the Internet of Things.

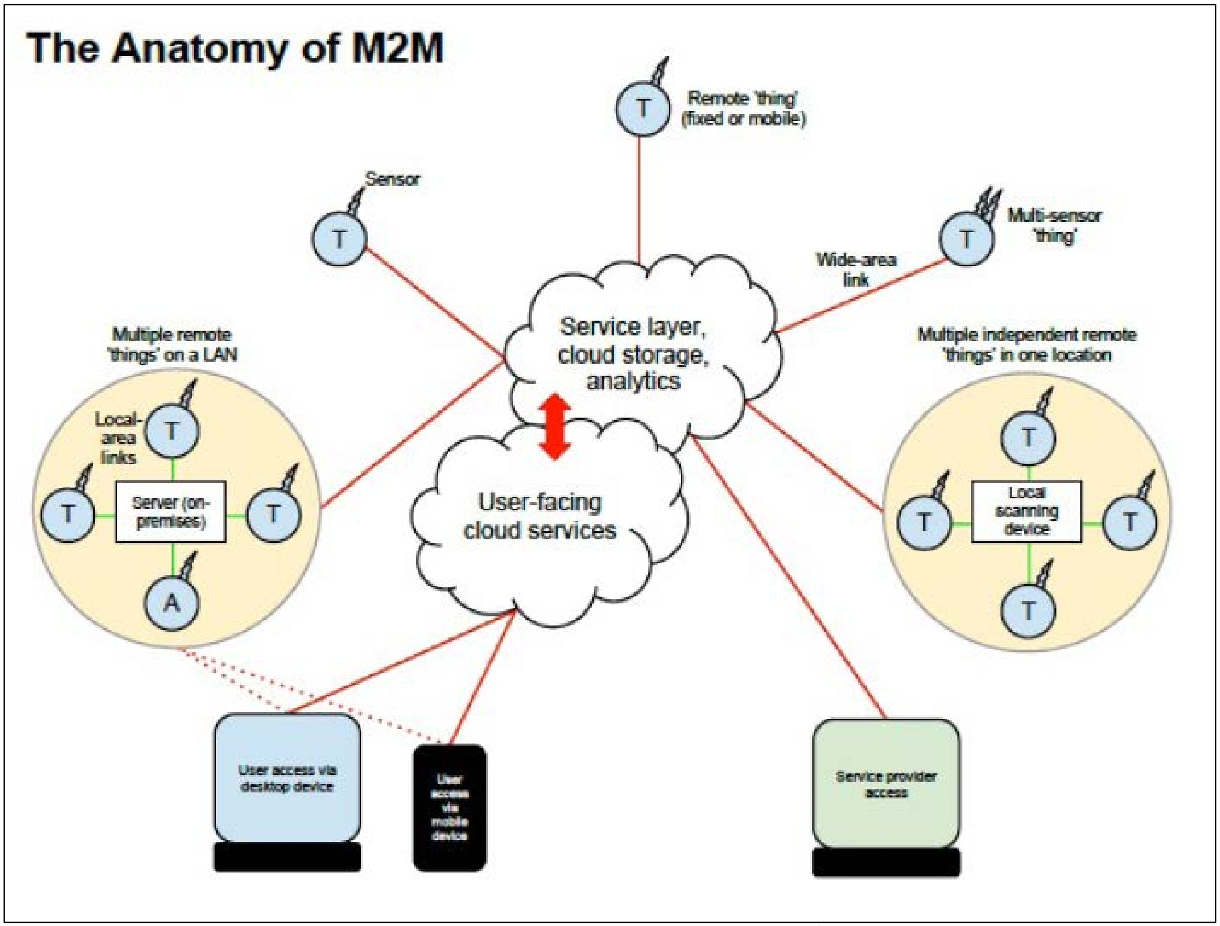

The Anatomy of M2M
T
Remote 'thing' (fixed or mobile)
Sensor
T
Multi-sensor 'thing'
T
Wide-area link
Service layer, cloud storage, analytics
Multiple remote 'things' on a LAN
Multiple independent remote 'things' in one location
Local-area links
T
T
Server (on-premises)
T
A
User-facing cloud services
T
T
Local scanning device
T
T
User access via desktop device
User access via mobile device
Service provider access

Figure 2 – The Anatomy of M2M[1]

Business and Household Applications

The Internet of Things has many applications in business, and as such quickly becomes entangled in the explosion and importance of Big Data. Manufacturing, health care, public utilities, and other industries and firms will see a huge impact in the immediate future from the evolution of the IoT.[3] Additionally, the household sector as the juxtaposed market to business would also see related benefits. See Figure 3 for some of the M2M technologies currently being used.

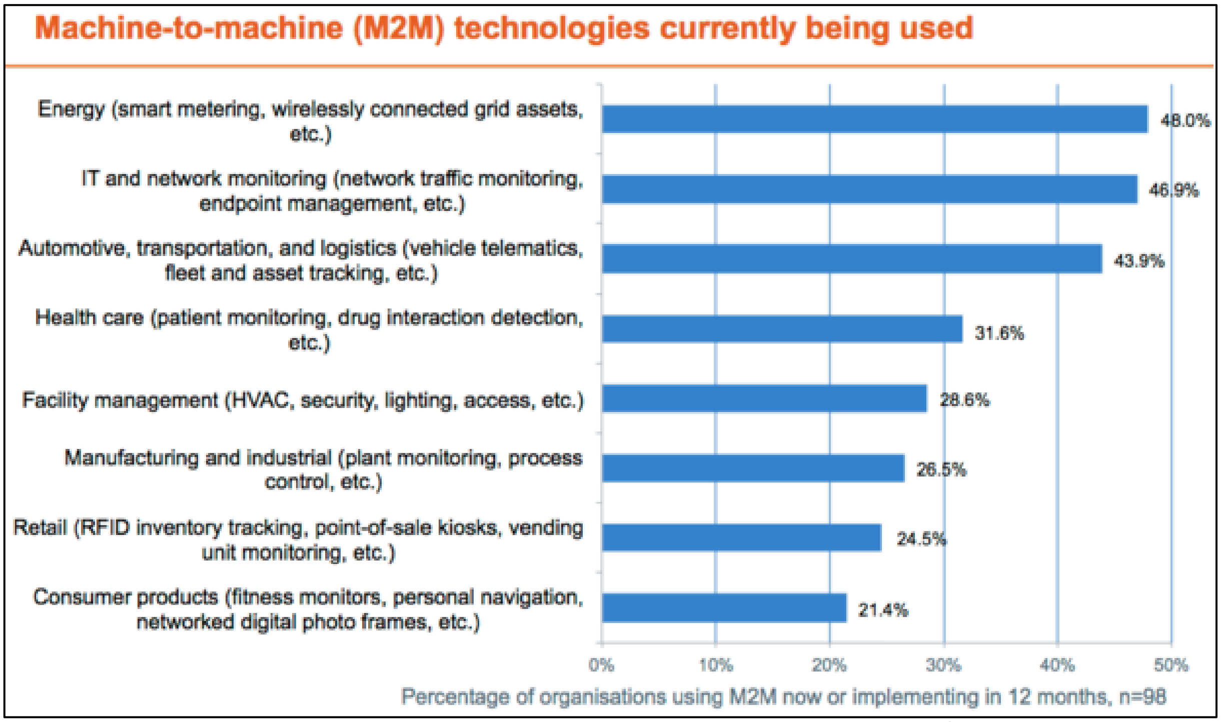


Figure 3 – M2M Technologies Currently Being Used[4]

In order of most to least important, what companies want from the IoT are new business opportunities, faster response time, enhancements of existing products and services, cost savings, expanded cellular coverage, regulatory compliance, and risk mitigation. Roadblocks to implementation of this technology in businesses, in order of most concerning to least are an immature M2M market, no clear business need, data security and privacy, implementation and maintenance costs, and complexity of M2M implementation.[4] See Figures 4 and 5 for survey results on what companies want from M2M technology and why business are not using M2M technology much yet.

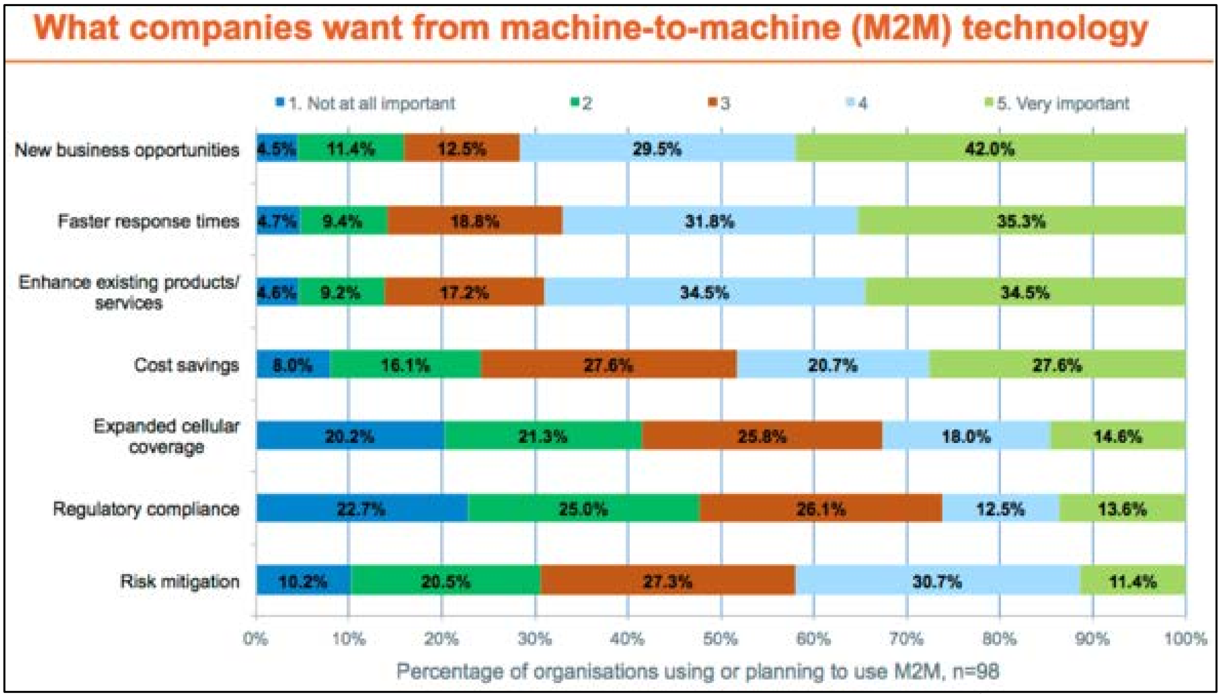


Figure 4 – What Companies Want from M2M Technology[4]

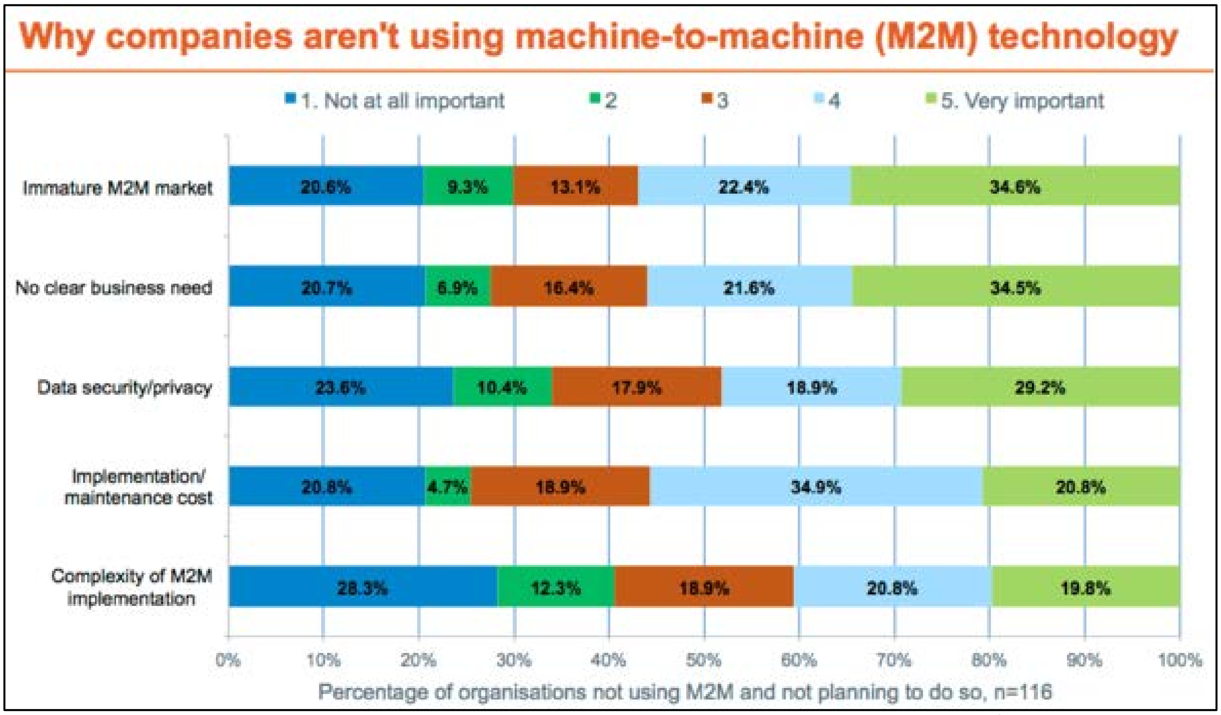


Figure 5 – Why Companies Are Not Using M2M Technology[4]

In healthcare, patients can be monitored and recover while at home. This saves cost for hospitals in terms of bed and room space, human monitoring costs, and other facilities and miscellaneous care costs, and therefore also lowers healthcare costs to patients. For traffic regulations, sensors can be used to enforce traffic laws and even adjust traffic flows more efficiently based on real-time traffic pattern data on roads and intersections. This would lead to more expedient ground transportation travel experiences for travelers of all types, and could be expanded to other ground applications such as buses, rail, subway, etc. Smartphones and smart TVs would become enhanced with live reactions to user interest, location, and time patterns. This would allow a smartphone's GPS signal to trigger a location-based advertisement in the appropriate time and place given a user's current location, as well as target advertisements and channel suggestions based on TV viewers' unique interests. The smart refrigerator would track food and beverage contents and expiry dates via smartphone or built-in LCD panels, make dish recommendations based on current contents, and could maintain a "Go Shopping" connection to manually and/or automatically order certain foods and beverages when they begin to run low. This would eliminate households' shopping trips for groceries, and save time in and ease meal preparation and cooking processes. Smart water metering by water utility companies would provide more accurate billing for customers based on exact consumption details per property, and would further assist effective water management, waste reduction, improved customer service, and better water resource safeguards. It could also provide for increased customer satisfaction by lack of utility house visits to check meters, automatic issuance of alerts for abnormal consumption to households, and other analytical opportunities for public water utilities. Furthermore, IoT technology supports real-time applications in the entertainment industry, such as the iLuminate bodysuits and costumes worn by The Black Eyed Peas at a concert. Wireless control replaces on and off buttons, and allows ease of circuit management on an extremely fast level to match patterns of many sorts, including music and choreography.[1]

The beginnings of some of these new technological advances are already starting to show for some applications. Remote home management in the form of mobile DVR scheduling, remote home security systems monitoring and administration, and remote home electricity grid usage monitoring via smart meters and smart grid technologies are currently emerging to near significant levels of awareness. Specific applications include DIRECTV Scheduler (a PC/mobile phone app), CPI Security (remote device control over home or business monitoring system, remote arm/disarm, energy source controls, email/text notifications, current status/recent activity views), and PlotWatt (free service connecting to smart utility meters at homes and businesses that records and displays electricity usage by day/range of days, has device-level statuses for heating/air conditioning, dryer, fridge, always-on devices, EV charging, and more). For a screenshot of the PlotWatt interface, see Figure 6. In some cases, these IoT technologies look strikingly similar to the services provided by Rosie the Robot butler in *The Jetsons* sitcom who provides a household with housework.[1]

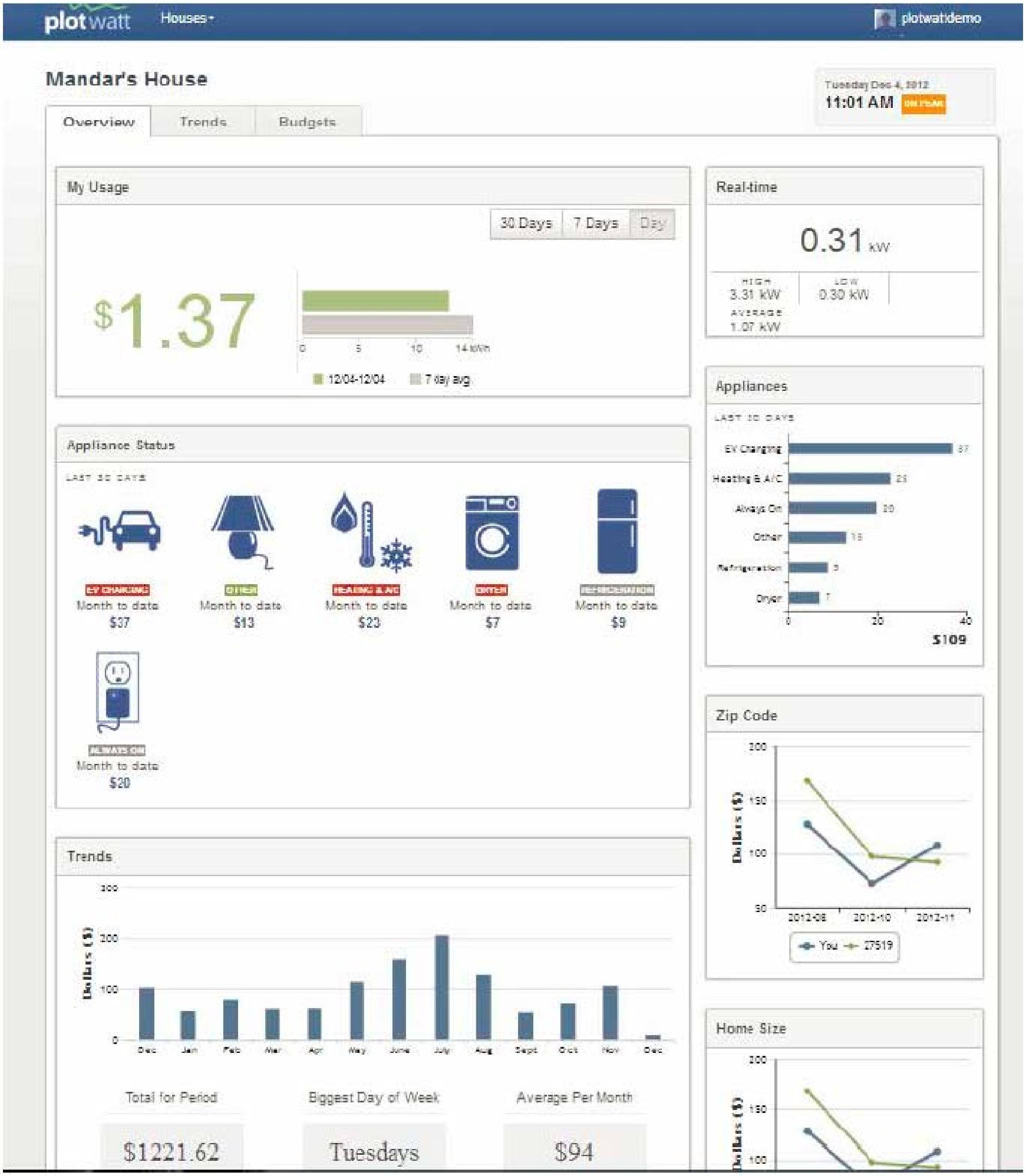


Figure 6 – PlotWatt User Interface[1]

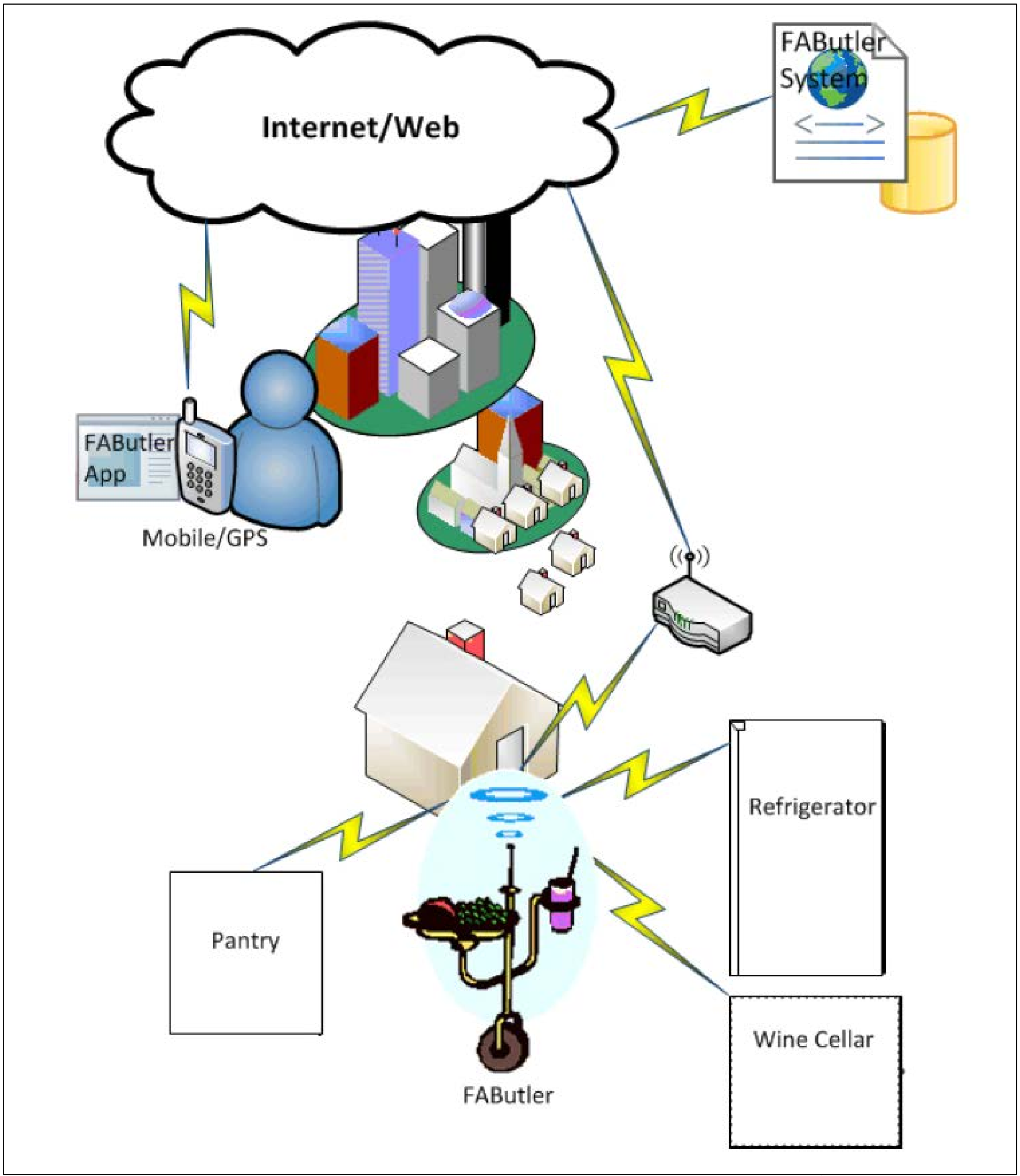


Figure 7 – The Food and Beverage Butler, or "FAButler"[1]

Businesses are, of course, profit-driven and value-adding institutions at their core. Information technology enhancements must win over business leaders by proving that they increase revenue, decrease cost, and/or add unique value for customers and/or internal users. Due to low levels of awareness, business leaders across the globe do not currently have a movement toward acceptance of the technology as a whole.[1] However, this movement will continue to build as standards for M2M technology further develop, and business benefits begin to emerge with more clarity and real implementation stories.

Case Study: DBS Bank

DBS Bank, incorporated in Singapore, has advanced its infrastructure to a point where IoT technology currently helps drive certain aspects of its business. The extent of its old ATM transactional system used to consist of queries to the bank core system with a request to dispense funds. Now, a separate repository from the transactional data has been created to collect unstructured data from customers' mobile devices, social media accounts, and other bank-related experiences in order to better understand and meet customers' needs. Additionally, the bank's ATM downtimes have been significantly reduced through "listening" to what the machines are saying in terms of cash remaining, maintenance needed, and more. This has reduced instances of ATM cashouts by 80 percent, resulting in a dramatic decrease in customer complaints and greater customer satisfaction at being able to conveniently withdraw money.[1]

From this implementation of sensor-driven machine reporting and unstructured data gathering, we observe both positive and negative impacts of this type of technology. In the ATM instance, customers and the institution experience a win-win through improved customer experience. The unstructured data collection and associated repository give bank employees the chance to mine this data for useful patterns and other analytical insights. These analyses may result in more effectively targeted marketing efforts and a better understanding of customers' needs and transactions. A potential downside to this type of massive data collection occurs when considering what should and should not be done with this type of customer data. Who owns the data? Who has the right to access it and who should not? Is it okay for the bank to sell the data to a third-party or other sponsor for further marketing efforts? Should the bank be allowed to even collect this kind of data on customers in the first place? These questions and more will only continue to arise as IoT technology gains further awareness and business interest.

Case Study: Rural India

Rural parts of India are seeing a critical opportunity to give M2M a chance to succeed in a meaningful way. Many agricultural areas find it useful to monitor weather conditions and live market crop prices via mobile 3G technology. Mobile phone apps that remotely monitor and switch on irrigation pumps in remote locations assist in efficient farm management. SmartMoo, an app that automates cow-milking to reduce wastage, is finding some success in dairy production. Water management applications are also assisting in more efficient methods for utilities supplying rural areas. Even in pregnancy in rural locations, IoT technology in the form of sonography machines like Silent Observer are helping to make child delivery a more informed activity.

Multiple challenges exist with respect to these applications, however. The rural market is price-sensitive, lacks access to resources like power, and low-cost devices are a concern for individuals and businesses in these developing areas. Lack of high-speed Internet connectivity also complicates this situation, as well as a lack of awareness in areas where traditional wire-based communication systems are still widely used for transmission.

Operators could potentially mitigate or resolve these issues by establishing network-sharing partnerships to lower costs of M2M services in rural areas. The government also needs to identify opportunities and design policies encouraging M2M deployments. In the energy sector, the Indian government has already mandated deployment of smart meters and frequent energy readings to counter the massive power loss and theft the country continues to experience. The government estimates only half the power transmitted is actually billed for, and expects the deployment of more than 200 million smart meters in the coming years to greatly assist in solving this problem. It is also expected that the private sector will jump on board once the government can successfully prove initiatives in M2M.[1]

Case Study: Isle of Wight

On a small island just south of the English mainland, IBM Master Inventor Andy Stanford-Clark developed an idea to hack his house in order to better understand his electricity usage. After much effort trying to develop appropriate sensors, devices, and software himself, his house—now known as the “tweeting house”—automatically tweets about electricity consumption via sensors. “As of 2012, Stanford-Clark’s house is reporting about 20 data channels, most of which refresh every six seconds” (source 1). Today, off-the-shelf software packages are available that do the same work that Stanford-Clark originally developed from scratch.

When others heard of Stanford-Clark’s hobby, they quickly jumped on board to promote efficient energy use. The effort grew to such a degree that the Isle of Wight has now become a model for M2M and smart grid technology as a hot bed for cutting-edge renewable energy developments. Social housing in particular has been the largest implementation on the island, leading to data insights on power bill and household equipment problems via near real-time info after initial wiring and setup challenges are overcome.

From this effort launched the Chale Community Project, a Department of Energy and Climate Change-back scheme to retrofit social houses in the village of Chale on the Isle of Wight with solar panels, heat pumps, and other environmentally friendly technology. Around the time of Stanford-Clark’s invention, the project ran into a need for monitoring that had yet to be addressed. Stanford-Clark ended up performing pro bono work eventually sanctioned by IBM based on the word-of-mouth generated from his hobby project. 40 homes on the housing estate are now outfitted with energy-monitoring equipment, with savings per year estimated at around $280.

From the Chale Community Project launched the Ecoisland scheme. Developed by a member of the project, David Green, the goal is to spread modern M2M and sustainable technology to make the Isle of Wight (pop. 150,000) a prototype for other UK community and the wider world. The initiative would reduce electricity bills and carbon footprint on a significant scale if successful.

The Isle of Wight proves a good test bed for this type of wider implementation of IoT technology because of its finite and realistic deployment size. At 148 square miles, the island can support an isolated smart grid, completely renewable energy as a power source, and electric vehicles. As drivers can never be more than 24 miles from home, electric cars and other electric transportation become highly feasible. An island-wide smart grid consisting of automation and monitoring technology to collect and analyze sensor and energy meter data is supported by mesh network for power distribution as opposed to traditional tree and branch models. The mesh network approach only works over a small area due to physical distance limitations, but more efficiently distributes energy by load and demand. Coupled with smart meters, the mesh smart grid soundly supports renewable energy applications and more accurate billing to customers simultaneously. Smart grids work best when there is a significant contribution from renewable energy, and on the Isle of Wight about 40 megawatts of solar energy is available to the entire island when the sun is shining. The mesh network has the ability to rapidly distribute loads through a mesh of lines rather than predefined distribution points, which leads to better maintenance of voltage and greater stabilization of the overall grid. This island-wide grid build-out is currently underway and expected to reach completion by 2015 to 2016.

Ecoisland's end result would outfit 10,000 homes with Home Energy Management systems based on Stanford-Clark's design that could subsequently expand to 35,000 homes. The systems would allow homeowners to enter into agreements with the power company where the company can remotely turn off household items to regulate demand in exchange for a rebate on their bill. Preliminary observations indicate householders typically reduce power consumption by around 25% under this method. Ecoisland hopes to become a cookie-cutter model for similar scenarios worldwide as its success gains awareness and credibility.[1]

Standards: OneM2M

An important consideration in the proliferated adoption of disruptive technologies, particularly in business, is a set of widely accepted, applicable, and meaningful standards. By 2016, Cisco projects 9 billion extra Internet-connected devices to exist. To handle the standards around this explosive growth, OneM2M is an industry-driven standards body with a goal "to hammer out the standards that will define how the Internet's next few billion devices talk to one another without running into difficulties".[1] Companies and cross-country major standards bodies participating in current discussions include Alcatel-Lucent, Ericsson, HP, Juniper Networks, Motorola Mobility, Qualcomm, Samsung, and Texas Instruments. They represent collaborative standards work among Japan, China, Korea, Europe, and the US.

Most of the standards' concerns with IoT technology surround service-layer architecture protocols and APIs. Service layers are the systems used to pass M2M messages through a network, transfer data in and out of other IT infrastructures, present information to the administrator, and communicate with other M2M clouds. There already exist about 180 methods of communicating, authenticating, and securing data transfer between M2M devices and service layers. Supporting this many technologies is a problematic issue for M2M communications uptake. Lower cost and easier implementation and support will result from the further work of standards organizations like OneM2M, and will expedite the acceptance of the new technology.

Another issue revolves around interoperability across countries and local service layers. A good bought in Asia should seamlessly communicate data with a local service layer while being easily transferrable and connectable to a different service layer in a completely different geographic area of the world. Global standardization would make this smooth integration possible.

Currently, adoption of proprietary standards is also a concern. A company willing to invest a great deal in creating an emerging leading standard for this new technology stands to gain a great return if their standards prove widely acceptable. There are varying opinions on whether a standards body like OneM2M or a large corporation platform should drive M2M standards overall. Furthermore, some people say creation of standards in certain degrees goes too far, while others believe establishing some standards would not go far enough in addressing many of the issues with this disruptive technology.[1]

Security

The IoT phenomenon is the notion that nearly everything will be Internet-connected to provide data or control. The number of "things" that will actually compose this spectacle is unclear, but it will be enormous. Cisco projects that by 2020 there will be 50 billion such devices, while Gartner estimates a total of 30 billion. Verizon has identified the IoT as one of five key business tech trends for 2013 and expects the Asia-Pacific region to experience a rapid lead.[1] Security for this great a number of devices is of definite importance.

Supervisory control and data acquisition (SCADA) systems have been in use for decades at power stations, building control and management systems, and water utilities. These systems are usually custom implementations running proprietary software without any regard for a standard or security as their designers never imagined SCADA systems to become Internet-connected. CT scanners, MRI scanners, dialysis machines, and other such computerized apparatuses all run highly vulnerable operating systems, most frequently embedded Windows versions. Security roll-outs to these machines are very infrequently distributed, and SCADA systems are widely regarded as vulnerable by nature. These flaws pose relevant concerns for sensor and monitoring technology such as those posited by the IoT.

Traditional disruptive attacks, such as Denial of Service (DoS), are effective because of battery-power to devices. This power source exposes the device to a security flaw through which the device can be forced offline via increased processor usage and encryption bypass. Encryption is a processor-intensive, and thus power-intensive, activity. Until battery and/or nanotechnology advances are made, the need for encryption limits a more solid security method.

In addition to these security barriers, there exists great complexity in managing each individual end point for 30 to 50 billion expected devices by 2020. This has led some to believe the end point cannot be viewed as an effective security measure. Chris King, Palo Alto Network global product marketing lead, says, "The place to exercise security in the Internet of Things is on the Internet, not the things. That may be the only thing you've got control over" (pg 30).[1] End point security involves certificate management for updates and revocations of established trust relationships. This may make large-scale IoT device proliferation very difficult to manage via an end point solution.

Further consideration must also be given to these devices in light of the corporate security environment. "'If it has an IP address, regardless of whether it's fixed or mobile or a device, it needs a security protocol, and that security policy should be in line with the full-blown policy that the enterprise has," says Robert Le Busque, Vice President for Strategy and Development at Verizon Business (pg 30).[1] Successful business cases and measurable savings from M2M technologies will serve as the catalyst for business leaders to invest in developing effective security solutions, but until the M2M uptake in business may be rather slow until that proof surfaces.

Overview of Disruptive Technologies

Importance of disruptive technologies

There are four characteristics of important technologies: high rate of technology change, broad potential scope of impact, large economic value that could be affected, and substantial potential for disruptive economic impact. A high rate of technology change results from technology that rapidly advances or experiences breakthroughs. A broad potential scope of impact affects multiple social and economic facets. Technology which could affect a large economic value or has substantial potential to create disruptive economic impact could significantly change the economic playing field.[6]

Disruptive technology was first devised as a term by professor Clayton M. Christensen at Harvard Business School to describe a new technology that unexpectedly displaces an established technology. Two categories for new technology were proposed: sustaining technology and disruptive technology. Sustaining technology relies on incremental improvements to an already established technology, such as upgrades to a system or enhancements to existing technology in use. Disruptive technology lacks refinement, often has performance problems because it is new, appeals to a limited audience, and may not yet have a proven practical application. Examples of disruptive technology include the motor vehicle and Alexander Graham Bell’s “electrical speech machine” known today as the telephone.

Large corporations and organizations are designed to work with sustaining technologies. Businesses know their market, and all organizations stay close to their customers or clients and have mechanisms in place to develop existing technology. Large organizations subsequently face difficulty capitalizing on potential efficiencies, cost-savings, or new marketing venues offered by low-margin disruptive technologies. They also more frequently dismiss disruptive technology value—becoming blindsided later when the technology matures, gains audience and market share, and threatens the market and social status quo.[5]

A report by McKinsey Global Institute states that “…leaders need to focus on technologies with potential impact that is near enough at hand to be meaningfully anticipated and prepared for,” (pg 2).[6] Technologies with the potential to dramatically disrupt social and economic status quos are therefore highly important for the leaders of today and tomorrow to make note of and follow. For a list of twelve potentially economically disruptive technologies and their purposes, see Figure 8.

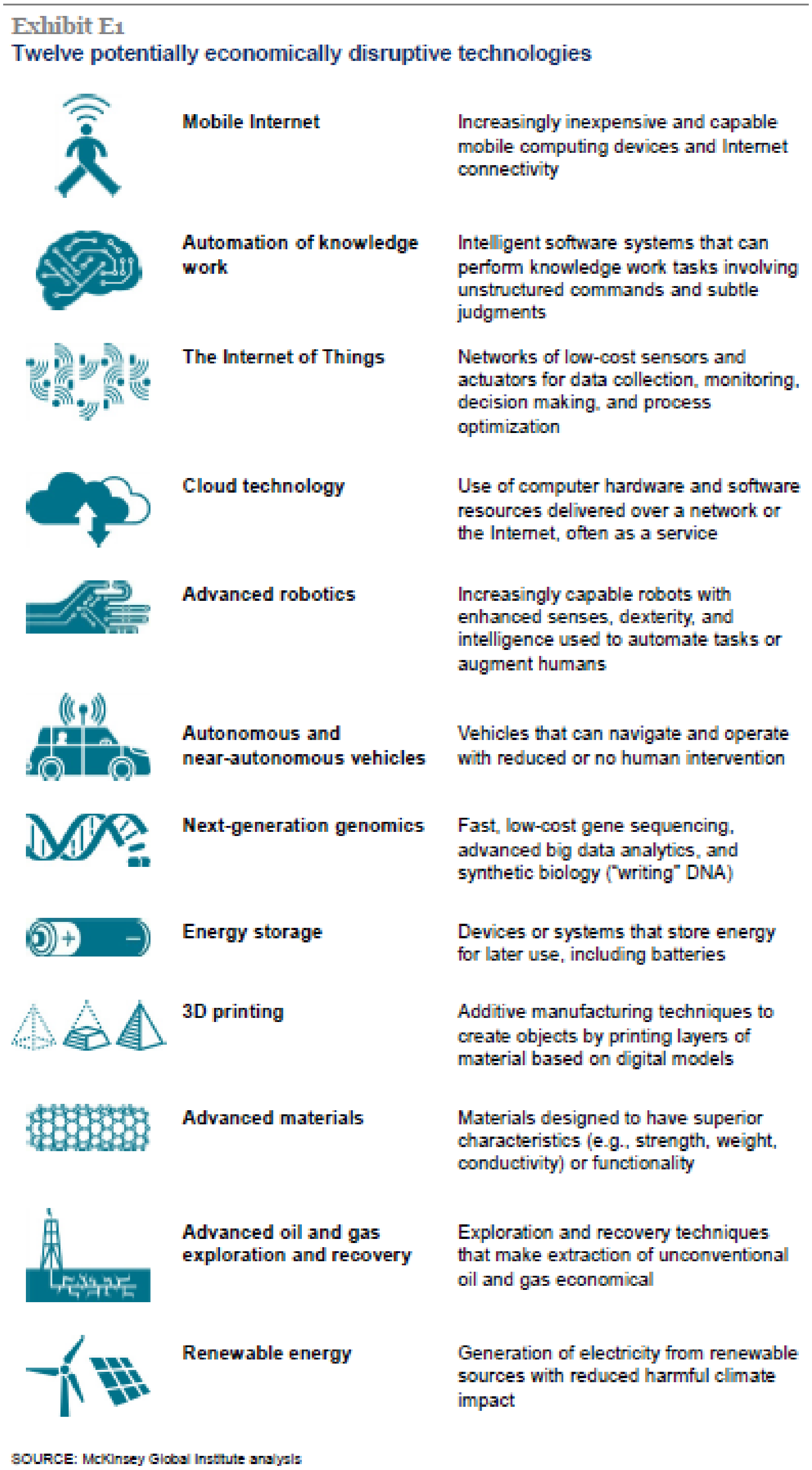


Exhibit E1

Twelve potentially economically disruptive technologies

Mobile Internet	Increasingly inexpensive and capable mobile computing devices and Internet connectivity
Automation of knowledge work	Intelligent software systems that can perform knowledge work tasks involving unstructured commands and subtle judgments
The Internet of Things	Networks of low-cost sensors and actuators for data collection, monitoring, decision making, and process optimization
Cloud technology	Use of computer hardware and software resources delivered over a network or the Internet, often as a service
Advanced robotics	Increasingly capable robots with enhanced senses, dexterity, and intelligence used to automate tasks or augment humans
Autonomous and near-autonomous vehicles	Vehicles that can navigate and operate with reduced or no human intervention
Next-generation genomics	Fast, low-cost gene sequencing, advanced big data analytics, and synthetic biology ("writing" DNA)
Energy storage	Devices or systems that store energy for later use, including batteries
3D printing	Additive manufacturing techniques to create objects by printing layers of material based on digital models
Advanced materials	Materials designed to have superior characteristics (e.g., strength, weight, conductivity) or functionality
Advanced oil and gas exploration and recovery	Exploration and recovery techniques that make extraction of unconventional oil and gas economical
Renewable energy	Generation of electricity from renewable sources with reduced harmful climate impact

SOURCE: McKinsey Global Institute analysis

Figure 8 – Twelve potentially economically disruptive technologies[6]

The associated speed of new technology adoption and diffusion, scope of applications for new technology, and degree of economic value in the new advancements help leaders determine the importance of various new technologies in light of current trends and organizational needs. For an overview of the speed, scope, and economic value at stake in upcoming disruptive technologies, see Figure 9.

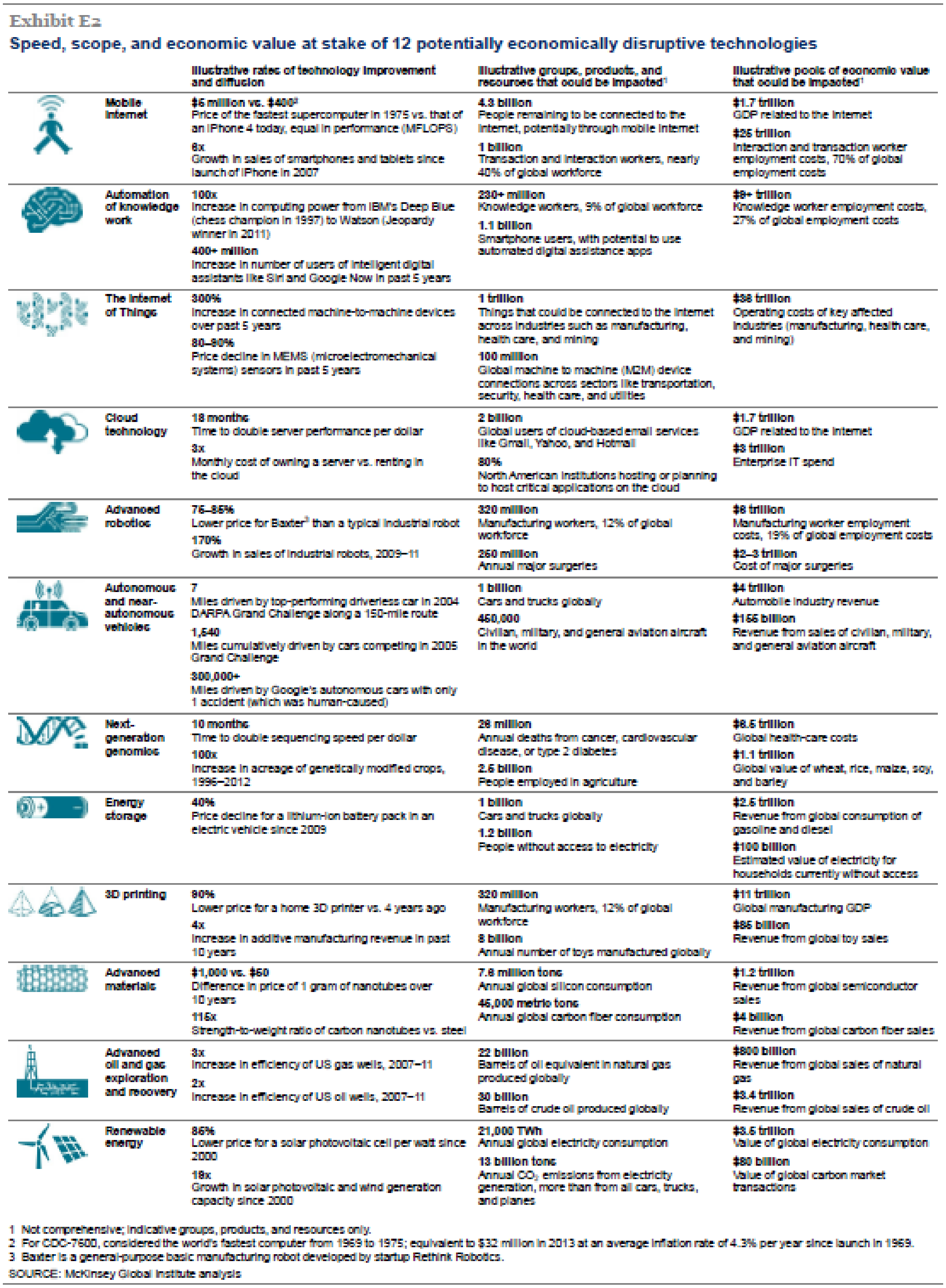


Exhibit E2

Speed, scope, and economic value at stake of 12 potentially economically disruptive technologies

	Illustrative rates of technology improvement and diffusion	Illustrative groups, products, and resources that could be impacted[1]	Illustrative pools of economic value that could be impacted[1]
Mobile Internet	**$5 million vs. $400**[2] Price of the fastest supercomputer in 1975 vs. that of an iPhone 4 today, equal in performance (MFLOPS) **6x** Growth in sales of smartphones and tablets since launch of iPhone in 2007	**4.3 billion** People remaining to be connected to the Internet, potentially through mobile Internet **1 billion** Transaction and interaction workers, nearly 40% of global workforce	**$1.7 trillion** GDP related to the Internet **$25 trillion** Interaction and transaction worker employment costs, 70% of global employment costs
Automation of knowledge work	**100x** Increase in computing power from IBM's Deep Blue (chess champion in 1997) to Watson (Jeopardy winner in 2011) **400+ million** Increase in number of users of intelligent digital assistants like Siri and Google Now in past 5 years	**230+ million** Knowledge workers, 9% of global workforce **1.1 billion** Smartphone users, with potential to use automated digital assistance apps	**$9+ trillion** Knowledge worker employment costs, 27% of global employment costs
The Internet of Things	**300%** Increase in connected machine-to-machine devices over past 5 years **80–90%** Price decline in MEMS (microelectromechanical systems) sensors in past 5 years	**1 trillion** Things that could be connected to the Internet across industries such as manufacturing, health care, and mining **100 million** Global machine to machine (M2M) device connections across sectors like transportation, security, health care, and utilities	**$36 trillion** Operating costs of key affected industries (manufacturing, health care, and mining)
Cloud technology	**18 months** Time to double server performance per dollar **3x** Monthly cost of owning a server vs. renting in the cloud	**2 billion** Global users of cloud-based email services like Gmail, Yahoo, and Hotmail **80%** North American institutions hosting or planning to host critical applications on the cloud	**$1.7 trillion** GDP related to the Internet **$3 trillion** Enterprise IT spend
Advanced robotics	**75–90%** Lower price for Baxter[3] than a typical industrial robot **170%** Growth in sales of industrial robots, 2009–11	**320 million** Manufacturing workers, 12% of global workforce **250 million** Annual major surgeries	**$6 trillion** Manufacturing worker employment costs, 19% of global employment costs **$2–3 trillion** Cost of major surgeries
Autonomous and near-autonomous vehicles	**7** Miles driven by top-performing driverless car in 2004 DARPA Grand Challenge along a 150-mile route **1,540** Miles cumulatively driven by cars competing in 2005 Grand Challenge **300,000+** Miles driven by Google's autonomous cars with only 1 accident (which was human-caused)	**1 billion** Cars and trucks globally **450,000** Civilian, military, and general aviation aircraft in the world	**$4 trillion** Automobile industry revenue **$155 billion** Revenue from sales of civilian, military, and general aviation aircraft
Next-generation genomics	**10 months** Time to double sequencing speed per dollar **100x** Increase in acreage of genetically modified crops, 1996–2012	**26 million** Annual deaths from cancer, cardiovascular disease, or type 2 diabetes **2.5 billion** People employed in agriculture	**$6.5 trillion** Global health-care costs **$1.1 trillion** Global value of wheat, rice, maize, soy, and barley
Energy storage	**40%** Price decline for a lithium-ion battery pack in an electric vehicle since 2009	**1 billion** Cars and trucks globally **1.2 billion** People without access to electricity	**$2.5 trillion** Revenue from global consumption of gasoline and diesel **$100 billion** Estimated value of electricity for households currently without access
3D printing	**90%** Lower price for a home 3D printer vs. 4 years ago **4x** Increase in additive manufacturing revenue in past 10 years	**320 million** Manufacturing workers, 12% of global workforce **8 billion** Annual number of toys manufactured globally	**$11 trillion** Global manufacturing GDP **$85 billion** Revenue from global toy sales
Advanced materials	**$1,000 vs. $50** Difference in price of 1 gram of nanotubes over 10 years **115x** Strength-to-weight ratio of carbon nanotubes vs. steel	**7.6 million tons** Annual global silicon consumption **45,000 metric tons** Annual global carbon fiber consumption	**$1.2 trillion** Revenue from global semiconductor sales **$4 billion** Revenue from global carbon fiber sales
Advanced oil and gas exploration and recovery	**3x** Increase in efficiency of US gas wells, 2007–11 **2x** Increase in efficiency of US oil wells, 2007–11	**22 billion** Barrels of oil equivalent in natural gas produced globally **30 billion** Barrels of crude oil produced globally	**$800 billion** Revenue from global sales of natural gas **$3.4 trillion** Revenue from global sales of crude oil
Renewable energy	**85%** Lower price for a solar photovoltaic cell per watt since 2000 **19x** Growth in solar photovoltaic and wind generation capacity since 2000	**21,000 TWh** Annual global electricity consumption **13 billion tons** Annual CO_2 emissions from electricity generation, more than from all cars, trucks, and planes	**$3.5 trillion** Value of global electricity consumption **$80 billion** Value of global carbon market transactions

1 Not comprehensive; indicative groups, products, and resources only.
2 For CDC-7600, considered the world's fastest computer from 1969 to 1975; equivalent to $32 million in 2013 at an average inflation rate of 4.3% per year since launch in 1969.
3 Baxter is a general-purpose basic manufacturing robot developed by startup Rethink Robotics.

SOURCE: McKinsey Global Institute analysis

Figure 9 – Speed, scope, and economic value at stake of 12 potentially economically disruptive technologies[6]

Disruptive Impacts of the IoT

As an identified disruptive technology with very near future impacts, the Internet of Things has uniquely positioned itself on the radar of leaders worldwide.

The IoT would embed “sensors and actuators in machines and other physical objects to bring them into the connected world,” (pg 6).[6] This would provide for effective monitoring of the flow of factory products, moisture measurements in a field of crops, tracking utility water flows, remote monitoring of patient health in healthcare, and more. The most promising uses for this technology lie with healthcare, infrastructure, and public-sector services. Currently, nine billion devices are connected to the Internet. Within the next decade, we are set to see 50 billion to one trillion devices. “The Internet of Things has the potential to create economic impact of $2.7 to $6.2 trillion annually by 2025,” (pg 51).[6] This explosion of sensor-driven devices will surely cause a disruptive ripple effect across organizations both large and small, public and private.

For a summary of the IoT’s disruptive impacts across several applications, see Figure 10.

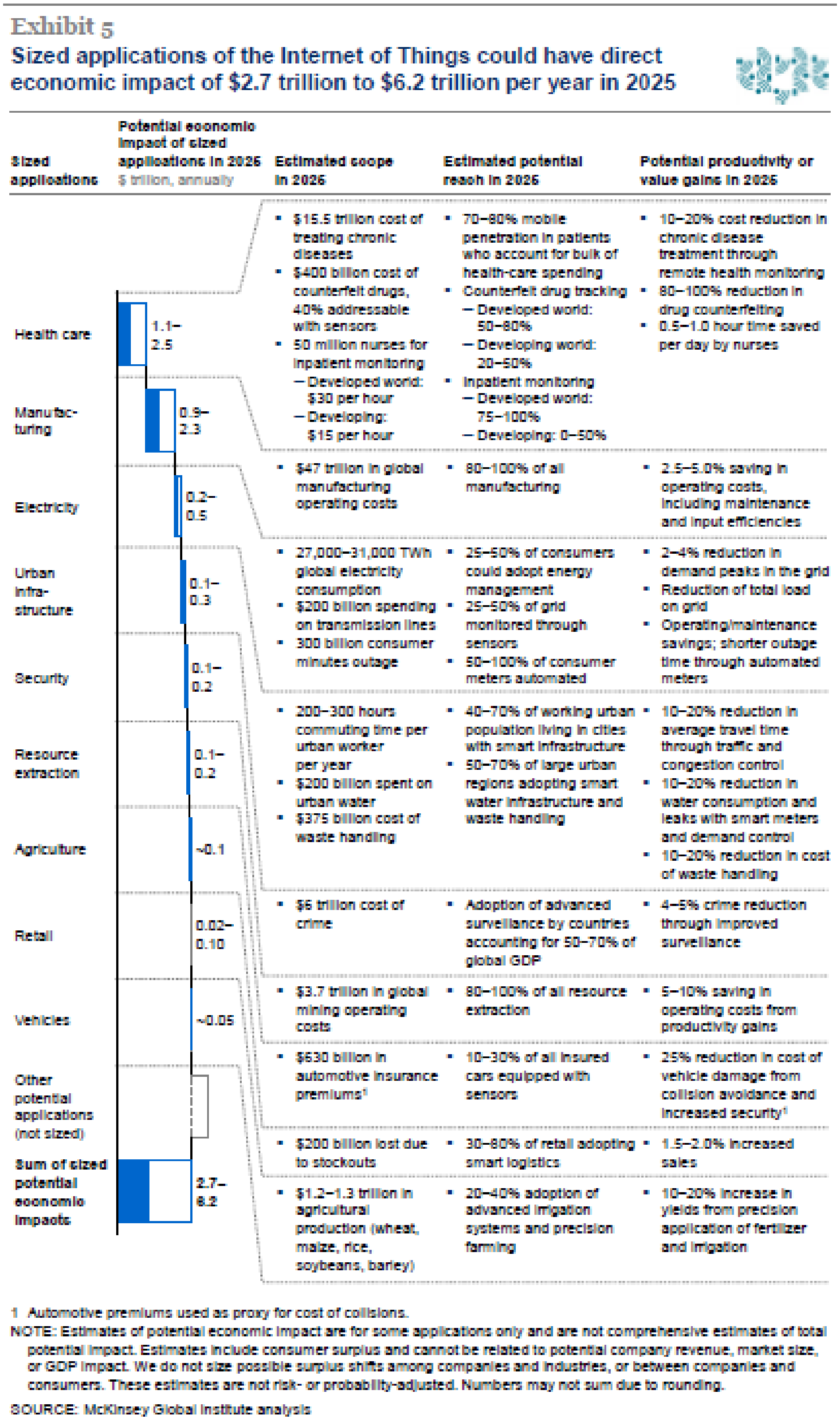


Exhibit 5

Sized applications of the Internet of Things could have direct economic impact of $2.7 trillion to $6.2 trillion per year in 2025

Sized applications	Potential economic impact of sized applications in 2025 $ trillion, annually
Health care	1.1–2.5
Manufacturing	0.9–2.3
Electricity	0.2–0.5
Urban infrastructure	0.1–0.3
Security	0.1–0.2
Resource extraction	0.1–0.2
Agriculture	~0.1
Retail	0.02–0.10
Vehicles	~0.05
Other potential applications (not sized)	
Sum of sized potential economic impacts	2.7–6.2

Estimated scope in 2025	Estimated potential reach in 2025	Potential productivity or value gains in 2025
▪ $15.5 trillion cost of treating chronic diseases ▪ $400 billion cost of counterfeit drugs, 40% addressable with sensors ▪ 50 million nurses for inpatient monitoring – Developed world: $30 per hour – Developing: $15 per hour	▪ 70–80% mobile penetration in patients who account for bulk of health-care spending ▪ Counterfeit drug tracking – Developed world: 50–80% – Developing world: 20–50% ▪ Inpatient monitoring – Developed world: 75–100% – Developing: 0–50%	▪ 10–20% cost reduction in chronic disease treatment through remote health monitoring ▪ 80–100% reduction in drug counterfeiting ▪ 0.5–1.0 hour time saved per day by nurses
▪ $47 trillion in global manufacturing operating costs	▪ 80–100% of all manufacturing	▪ 2.5–5.0% saving in operating costs, including maintenance and input efficiencies
▪ 27,000–31,000 TWh global electricity consumption ▪ $200 billion spending on transmission lines ▪ 300 billion consumer minutes outage	▪ 25–50% of consumers could adopt energy management ▪ 25–50% of grid monitored through sensors ▪ 50–100% of consumer meters automated	▪ 2–4% reduction in demand peaks in the grid ▪ Reduction of total load on grid ▪ Operating/maintenance savings; shorter outage time through automated meters
▪ 200–300 hours commuting time per urban worker per year ▪ $200 billion spent on urban water ▪ $375 billion cost of waste handling	▪ 40–70% of working urban population living in cities with smart infrastructure ▪ 50–70% of large urban regions adopting smart water infrastructure and waste handling	▪ 10–20% reduction in average travel time through traffic and congestion control ▪ 10–20% reduction in water consumption and leaks with smart meters and demand control ▪ 10–20% reduction in cost of waste handling
▪ $6 trillion cost of crime	▪ Adoption of advanced surveillance by countries accounting for 50–70% of global GDP	▪ 4–5% crime reduction through improved surveillance
▪ $3.7 trillion in global mining operating costs	▪ 80–100% of all resource extraction	▪ 5–10% saving in operating costs from productivity gains
▪ $630 billion in automotive insurance premiums[1]	▪ 10–30% of all insured cars equipped with sensors	▪ 25% reduction in cost of vehicle damage from collision avoidance and increased security[1]
▪ $200 billion lost due to stockouts	▪ 30–80% of retail adopting smart logistics	▪ 1.5–2.0% increased sales
▪ $1.2–1.3 trillion in agricultural production (wheat, maize, rice, soybeans, barley)	▪ 20–40% adoption of advanced irrigation systems and precision farming	▪ 10–20% increase in yields from precision application of fertilizer and irrigation

[1] Automotive premiums used as proxy for cost of collisions.

NOTE: Estimates of potential economic impact are for some applications only and are not comprehensive estimates of total potential impact. Estimates include consumer surplus and cannot be related to potential company revenue, market size, or GDP impact. We do not size possible surplus shifts among companies and industries, or between companies and consumers. These estimates are not risk- or probability-adjusted. Numbers may not sum due to rounding.

SOURCE: McKinsey Global Institute analysis

Figure 10 – Sized application-based impacts of the Internet of Things[6]

Implications of Disruptive IoT technology

Merging the physical and digital worlds has implications for privacy, security, and organizational structure of existing and future institutions. "As with any data connection, the connections that allow remote machines to take action without a human operator are subject to hacking by criminals or terrorists," (pg 52).[6] When more sophisticated operations fall under supervision of sensor-based systems, data security and network reliability become more important concerns. Furthermore, liability issues exist with closed-loop systems where an algorithm dictates the actions of a machine.

The best-positioned organizations for this disruption are perhaps suppliers of big data and analytical software which help extract meaning from enormous data flows. Big Data, however, also brings along serious concerns about how information gathered and insights generated will be used. The ability to put sensors anywhere—from observing traffic on a residential street to monitoring a home's electricity usage down to the appliance level—creates a vast level of surveillance activities which the public may reject. Laws and acceptable policies related to these activities may eventually require government intervention to ensure a comprehensive, fair policy is established that works across many borders and can be well-enforced. Yet, even Big Data continues to generate its own challenges. These include continuing efforts in creating software that can effectively aggregate and analyze data, and convey complex findings in useful ways to human decision makers and/or automated systems.[6]

Public surveillance applications may be the most hotly debated application for the IoT. On one hand, Big Brother (or Some Brother) concepts create great unrest for citizens. On the other, reduction in crime and better public safety and law enforcement could result from these technological advancements. "The economic cost of crime is estimated to be 5 to 10 percent of GDP around the world. If 4 to 5 percent of this could be eliminated, the potential economic impact could be $100 billion to $200 billion per year in 2025," (pg 58).[6] Varying opinions exist on the costs and benefits of these views.

Applications of Disruptive IoT Technology

Several concepts have achieved rapid growth as part of recent IoT developments. The smart house, striving to make household life more convenient and enjoyable, is one of the more interesting applications. Plug-in intelligence like Belkin's WeMo gives simple devices like light bulbs and appliances the ability to report respective data on their operative and resting states via a simple visual programming language. This technology is being developed through crowdsourcing to determine further suggestions from users who share their results from using the device. Belkin can then comb through the suggestions to develop further useful features and future applications, and updates the toolset available to customers accordingly.

In the realm of media, technology endeavors to connect to consumers in a uniquely captivating manner. Content "fingerprinting" by media companies and websites like

YouTube automate location and removal of unlicensed user uploads and copyright and/or Terms of Use violations. Apps are being created that follow a TV show in real-time such that while a user watches a show they can receive uniquely complementary material in the form of interactive activities and related ads on their smartphone or other handheld device. Facial "coding" further enhances the effectiveness of commercials and creation of superior marketing efforts by measuring a viewer's emotional response to the digital marketing material stimuli. This creates value for both consumers and businesses resulting from consumers receiving less ads they do not want to view as well as more effective expenditure of marketing dollars for businesses. A downside to these "fingerprinting" or "coding" activities may result, however, if a privacy panic erupts when this technology hits mainstream.[7]

Organizational leaders

Organizational leaders need to determine when, how, and whether to implement new technology sooner rather than later to avoid being caught off guard if and when a new technology begins exerting a strong influence among their market and/or clients. It is highly important that all leaders strive to understand technology and stay up on developments. Leaders must move quickly when implementing to seize opportunities immediately and not be left behind as this influence takes effect.

Several methods exist through which to ensure leaders are in tune with the technological forces in touch with their markets and customers. They must pay attention to tech-savvy customers and what they are doing and saying. In some cases, "A teenage customer halfway around the world may offer a better perspective on technology than a panel of experts in a conference room," (pg 148).[6] To effectively compete and continue providing exceptional experiences in the modern environment, institutions must continuously develop sources of value or competitive advantage. "Strategies can quickly fall behind, so the rhythm of planning has to keep pace. When technologies have disruptive potential, the stakes are even higher and the range of strategic implications is wider," (pg 148).[6] Leaders cannot be afraid to disrupt their own organizations in affecting technological change; organizations must continually reinvent themselves to keep up in the modern age by focusing on new markets and opportunities, not just existing ones.[6] The time to plan is not once new technologies begin exerting their influence, but rather right now.

Policymakers

Policymakers must recognize that they have conflicting responsibilities related to new technologies. While rising productivity provided by automation helps drive productivity growth, the impact on employment might cause social and economic problems which policymakers must adequately address also. Labor-saving technology can create new and higher value-adding jobs over the long term that allow workers to become more competitive overall, but short-term shocks resulting from rapid technological advancement are a concern for policymakers. "Governments often provide initial funding and incentives for technology development and even act as early buyers to speed progress and adoption," (pg 150).[6] In the past, government support for new technologies was often in the form of decades-long projects. Today's developments need a model that supports smaller, more frequent developments.

Standards-setting efforts are another area in which the government plays an influential role in helping disruptive technologies to proliferate. The IoT will need a high level of interoperability among different types of sensors and across both public and private networks, with sufficient security applied internationally. Other issues such as intellectual property rights and liability also could perhaps best be ironed out by government.[6]

Policymakers have the ability to effectively limit adoption or progress of technological advancements through various legislative tools. As IoT technology begins to disrupt the status quo more and more, the social and economic welfare of citizens needs to be rigorously evaluated in light of technological innovations.

Information Ethics and the Internet of Things

> *"'IE suggests that there is something even more elementary and fundamental than life and pain, namely being, understood as information, and entropy. IE holds that being/information has an intrinsic worthiness...'"*
> By Floridi[16]

Information ethics is the branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, including the ethical standards and moral codes that govern human conduct in society. Areas of interest in terms of information ethics include privacy, moral agency, environmental issues and behaviors (especially in the infosphere), and problems arising from the information life-cycle. It stands on the edge of the fields of computer ethics and philosophy of information.

Information ethics discusses information in terms of information entities which inhabit the Floridian infosphere. An information entity is an autonomous information object inhabiting an infosphere comprising both tangible and intangible informational patterns. The infosphere encompasses the environment inhabited by information entities, and includes informational interactions among material objects.[13] Four rules exist regarding the infosphere:

1. Entropy ought not to be caused in the infosphere.
2. Entropy ought to be prevented in the infosphere.
3. Entropy ought to be removed from the infosphere.
4. The flourishing of information entities as well as the entire infosphere ought to be promoted by preserving, cultivating, and enriching their properties.

Despite much overall progress in the field, a widely accepted theory of information ethics is also still needed to lend coherence to law and harmonize treatment of data across a wide range of legal doctrines. Additionally, information ethics may be less suitable for dealing with problems of moral motivation and moral distance as people do not usually connect entropy with wrongdoing; would you be distressed if you increased the amount of entropy in the infosphere? The concept of "well-being" is therefore usually replaced as a more tangible form of concern with wrongdoing in terms of information ethics, and is the IE approach that applies best to IoT.

Privacy as a requirement stands as the consensus view across the literature surrounding the Internet of Things. Two ethical frameworks originating in the United States and European Union exist with regard to much of privacy law and intellectual property law: 1) the economic benefits of information policy and 2) autonomy of the individual.[13] While informed consent should be given priority importance, this could be very difficult to achieve given the nature of IoT technology. A hindering situation to its development could result if users must give explicit permission for devices to function as intended, particularly in terms of passive surveillance applications in public spaces. "IoT challenges user control, or at least shifts the locus of control" (pg 3).[8] Control in a world of numerous interconnected machines constantly talking to each other and observing the real-world environment will have a much different meaning then it does in terms of today's Internet devices.

Three general perceptions of relationship between IoT and the Internet exist (see Figure 11). The first is that the Internet is simply a part of IoT. This view describes the Internet as just one part of a broader realm of IoT and thus suggests that the IoT is something more than the Internet as we know it. The second view defines the IoT as the opposite—simply an application within the Internet we are familiar with today. This would mean that the IoT falls within the boundaries and existing rules of Internet technology in general. A third view displays the IoT as a range of different applications that constitute a whole construct. In this interpretation, IoT applications are independent of each other altogether, each having its own unique design and purpose for existence.[8] The differences in IoT perceptions have important implications for society as they will directly impact the views of IoT technology development created by technology professionals.

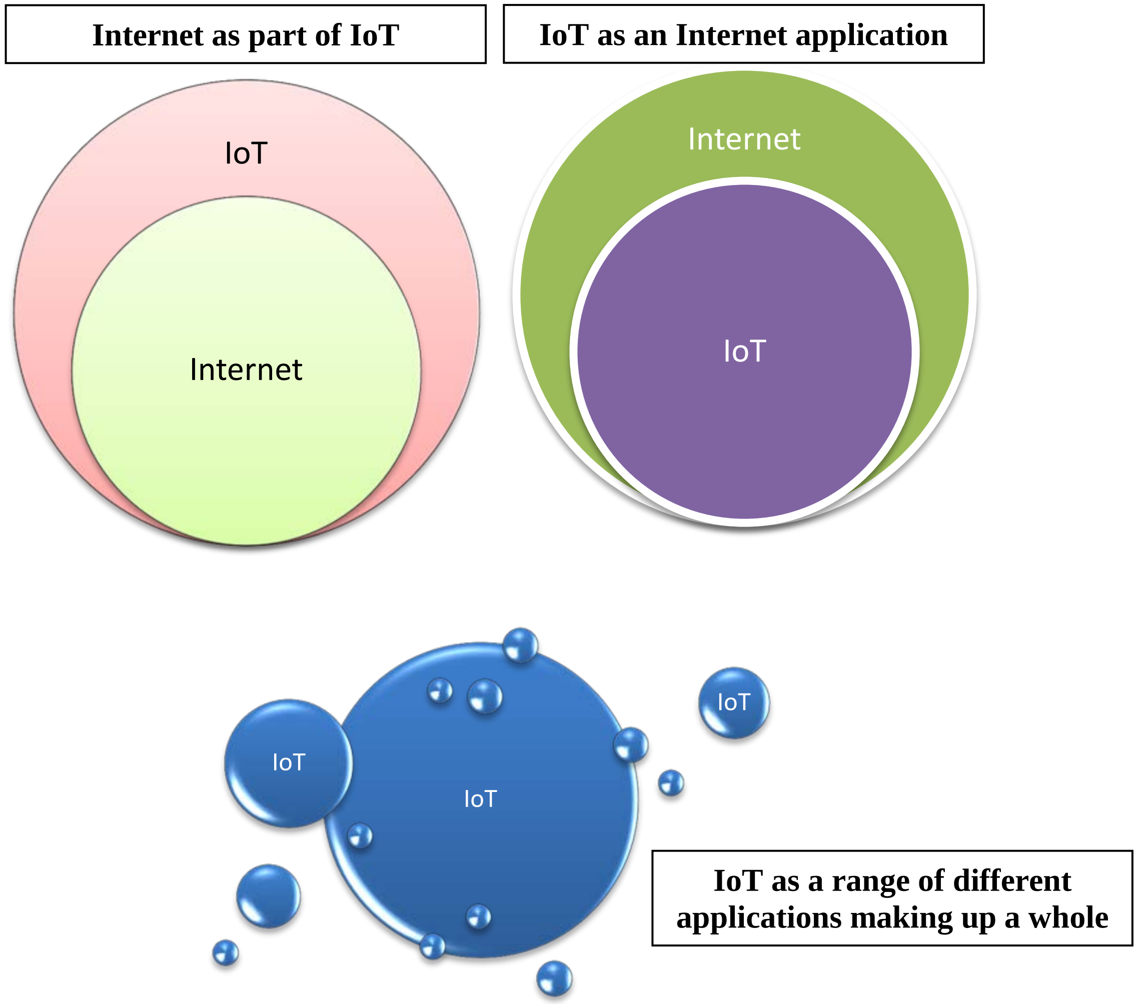

Internet as part of IoT
IoT
Internet
IoT as an Internet application
Internet
IoT
IoT
IoT
IoT
IoT as a range of different applications making up a whole

Figure 11 – Three Perceptions of the Internet of Things

Privacy

Everyone will be affected by the IoT, but not many people or organizations may necessarily realize it quickly or equally. Well-designed data protection at the design stage is critical so that profiling is performed correctly and corruption opportunities are as limited as possible. Data re-purposing (contextual integrity) should also be carefully monitored as large amounts of data may become deanonymized or repersonalized as availability of so many data sets may create opportunities of data convergence that would defeat anonymity. Moreover, the enormous amounts of data present ethical issues in terms of harm prevention, equality, and moral autonomy.

People may experience a feeling of lost control as IoT implementations create data in largely invisible and unnoticeable manners. Additionally, automatic decisions may results from control shifting toward devices and algorithms. Depending on the application, some people may find this desirable or beneficial while others may not.

> *"Agency becomes an ethical issue when the intentionality of delegated actions is not fully controllable by the user, does not identify with the user's identity and compromises her integrity and eventually her freedom"*
> By Internet of Things Expert Group[19]

> *"All human agents need to be identified for their intentionality, the morals they sustain, otherwise the risk is that no responsibility can be attributed once the objects mediate and operate within an IoT."*
> By Internet of Things Expert Group[19]

IoT expression may occur through multiple "smart" technology solutions such as smart building control and energy systems, smart transportation options, and the smart grid. Privacy is about control—how you control data about yourself and your habits, and how businesses and other entities control that information as well. It is not just the amount of information that creates privacy challenges, but also about the insights that can be generated from sensors and information technologies. Outside of healthcare organizations and electronic medical records, government regulations are scarce around privacy. Businesses and others need to carefully consider how information collected by smart buildings or smart cars or smart refrigerators could be used for purposes that infringe on freedom in some way. For example, authoritarian government could use information collected by smart cards to track and locate dissidents. In another application, smart building energy systems may open the door for surveillance applications by outside entities.[18]

As IoT solutions are developed, people may get stuck in a monopolistic or oligopolistic service provider structure. If existing cellular networks are engaged in activities that would connect IoT infrastructure to the Internet, this would likely increase the power of existing providers to supply their services at a higher cost to the customer.

In health applications, IoT devices may directly increase health risks in a situation of failure. An Internet-connected pacemaker, for example, opens the door to many questions such as the security of such an essential life-support device and the amount of trust people may have in using it.

Three main conclusions have been presented on privacy issues relating to the IoT:

1. Data protection legislation needs further consideration with respect to IoT-specific applications.
2. Privacy should be included by default in all IoT device designs and service schemes.
3. Standardization is crucial to ensure the effective and speedy adoption of IoT devices.

The terminology of "right to privacy" possesses intrinsic problems itself because in American law it is a term with many different aspects and no universal meaning. In terms of physical and bodily integrity, most constitutional rights prevent against governmental invasion of the home or of reproductive activities. Personal data generated in the ordinary course of human activity, such as records of financial dealings, creditworthiness, social security identification, and medical history, generally is also protected. But privacy rights in terms of ubiquitous IoT technology are much more obscure. How data is collected and used in the world of new interactions created by the IoT have no stated privacy rights as of now—only ideas and beliefs. In some cases, privacy is ethically incoherent—pointing in several different directions and adopting disparate models to assign responsibility and control for data representations. Unstated rights of privacy currently tend toward treating personal data representations as constitutive of individuals with potential to treat them as information entities.[13]

Moreover, rights to privacy are "socially constructed" meaning that they change over time as the influences of many human forces and institutions shifts, including those relating to technology, culture, and law. Rights and views to privacy include:

- Freedom—The right to conceal our behavior protects us from punishment, discrimination, ostracism, and criticism. Individual liberty weakens if privacy diminishes freedom.
- Property rights—Should a "consumer profile" or "public profile" be considered property that cannot be used unless chosen by the owner to be sold about themselves?
- Informed consent—The idea that we should not do things to others without their permission has a long history. This has important consequences for data collection without informed consent of a person being monitored.
- Personality development—We need opportunities for private reflection and experimentation if we are to develop complex personalities. We must be able to try out attitudes and values in private so that we can reject them later without being permanently viewed and held to everything we have said and done in the past as they change. Individual consumer tailoring also freezes interest, preferences, and activities as they have been and disallows the opportunity for change in these areas to take place.
- Avoidance of discrimination—Protecting privacy prevents powerful people and entities from acquiring prejudicial information in the first place.

- Avoidance of defamation—We should avoid false statements and groundless criticisms of others.
- Happiness—Generally, we think it is right to make people as happy as possible. Human beings usually seem happier when they have a zone of privacy—a chance for solitude.
- Equality of power—Knowing information about people is a source of power. Protecting the rights of ordinary people to withhold information strengthens them against governments and large firms.
- Separation of zones—Many people believe that it is important to keep society carefully divided into zones such as the market, the family, the military, religion, politics, scholarship, and social relationships. Zones are distinguished by rules and expectations regarding privacy.
- Rights of association—Legal and moral rights exist to associate in voluntary groups. To "associate" is to share information only within the organizations that one joins. If information can be bought, the result could be a weakening of associations.

A key question is whether we should altogether block the sale of private data at any price as we do for sex, human organs, and votes? Privacy also can be influenced by individuals and companies acting in a marketplace, parents when they set norms for their children, professionals when they establish rules of conduct for their peers, and software designers when they invent technology that either protects or erodes privacy.[17] It is also important to note to that Generation Y doesn't have the same idea of privacy as older generations.[18] Given all of these unique concerns and different views, where should privacy land in each of these spheres?

Security & Trust

> *"[Cybersecurity] threats reduce trust: 30% of Europeans do not trust the internet for banking or for online purchasing, and 90% choose not to reveal personal information online."*
> By Internet of Things Expert Group[19]

It is important to note that trust and confidence are different. Users may have trust in IoT, confidence in IoT, both, or neither. Handling trust issues well increases the value of the IoT.[8]

Concerns about dataveillance, systematic data surveillance via use of a person's electronic records relating to their use of credit cards, mobile phones, email, and the Internet, must be addressed head on.[11] Consumers and the general public have expressed a great concern over informed consent, and unchecked dataveillance will only serve to frustrate the common citizen at length if they believe entities are surveilling them unduly.

Whereas the Orwellian Big Brother world presented a totalitarian system which purposefully controlled the citizen's life, it had a mission. A new related concept for the IoT is "Some Brother". "Some brother is not a single player, but a whole, which consists of societal players like public sector authorities, citizens' movements and NGOs, economic players, big global companies and SMEs and finally all of us as citizens. Big brother had one address, Some brother has several of them, of which some are visible, some are not" (pg 111).[12] Some Brother has not one mission, but several as more than one master are served depending on the type of dataveillance application.

A ubiquitous society has three key features: control, knowledge, and eternal memory.[12] All recorded data becomes eternally accumulated and stored for various uses as it is collected. Knowledge increasingly flows between different information systems allowing opportunity for highly detailed profiles to be generated from many data sources. As profiles are established, society begins to form an unchangeable view of individuals and unpleasant issues cannot be escaped from as data is collected on them even in the briefest of moments. Control shifts from individuals to the collectors of the data from mobile phones, the Internet, e-mails, surveillance cameras, self-driving cars, and more all leave digital traces behind which can be scraped up and refined into the broader profile. The shift in this control, while perhaps well-meaning endeavors of Some Brother, creates viable concerns for the public citizen who loses some control over his/her physical and digital lives.

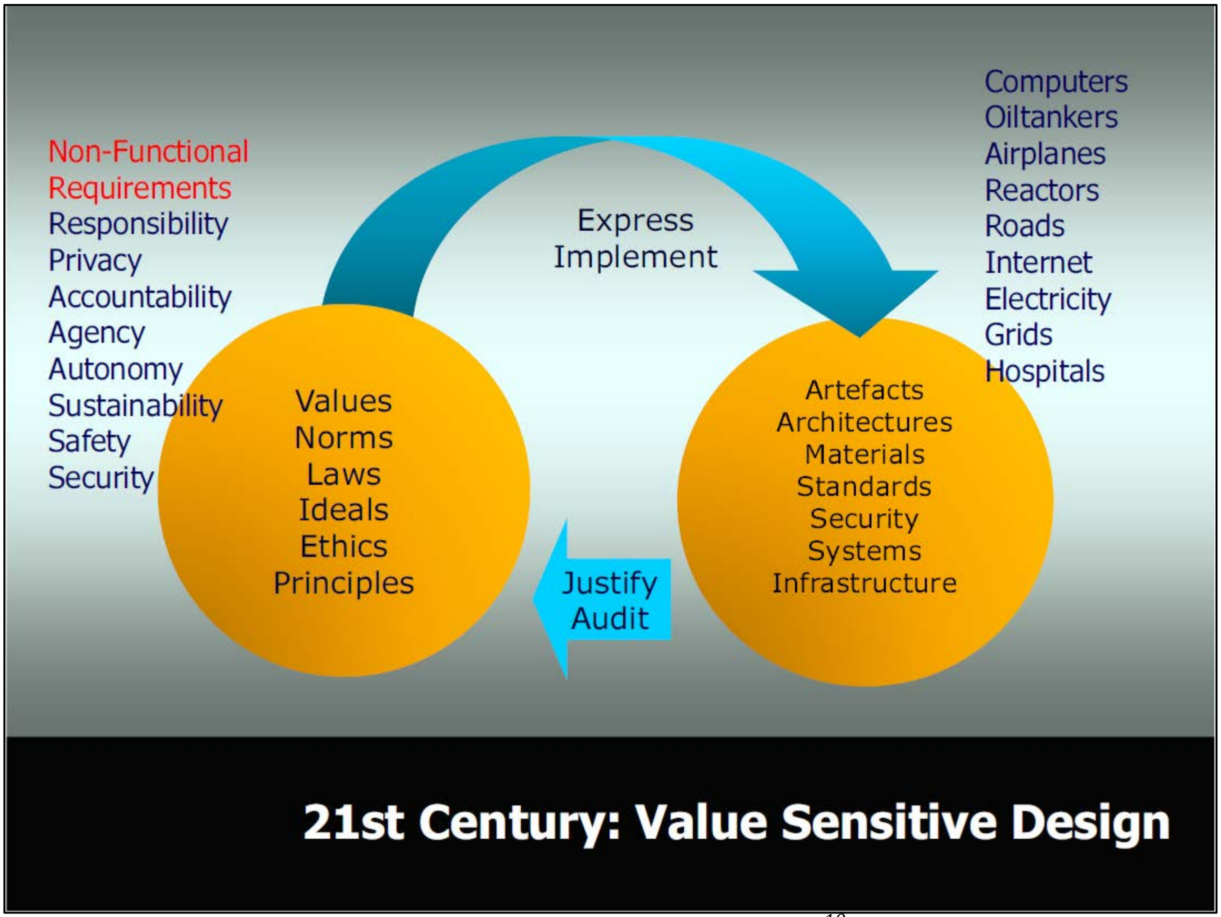
One critical way to create trust is by promoting reliability. Technology users trust a device or service more and more as they use it and find it works as expected. This expectation then compounds on itself until evidence is given the contrary. Events such as failures, errors, or unexpected outcomes should therefore be minimized in IoT devices and applications as much as possible to best promote the technology. Standardization relatedly assists in creating reliability from a technical perspective, and management of perceptions on the user-end promotes a more qualitatively sounded reliance

Perceptual Context

Perception, adoption, and success of the IoT are dependent on how metaphors relating to the technology are framed. For instance, while the technology has the potential to make people's lives easier and provide organizations with vast amounts of useful and detailed data, it could also be viewed as widespread implementation of the Orwellian Big Brother concept. The manner in which discourse framing occurs will have important impacts on IoT perceptions and willingness of adoption for the resulting new devices.

Furthermore, the way in which architects go about designing and constructing IoT technology will directly impact IoT perceptions and M2M uptake. Value-sensitive design is an approach to the design of technology that accounts for human values in a principled and systematic manner throughout the design process. The method concerns itself with values that center on human wellbeing, human dignity, justice, welfare, and human rights. It connects designers and stakeholders affected by the systems in an integral and inseparable way that demands broadened goals and special focus on technological advancement which advances human life in the most successful manner.[9]

Figure 12 by the Delft University of Technology's Scientific Director 3TU Centre for Ethics and Technology displays the highly connected, fundamental way in which non-functional requirements, including privacy and security, play into the reality of technology design implemented by architects. Figure 13 complements this concept by displaying both small and large-scale implementations involving choice by technological engineers.



Non-Functional Requirements
Responsibility
Privacy
Accountability
Agency
Autonomy
Sustainability
Safety
Security

Values
Norms
Laws
Ideals
Ethics
Principles

Express
Implement

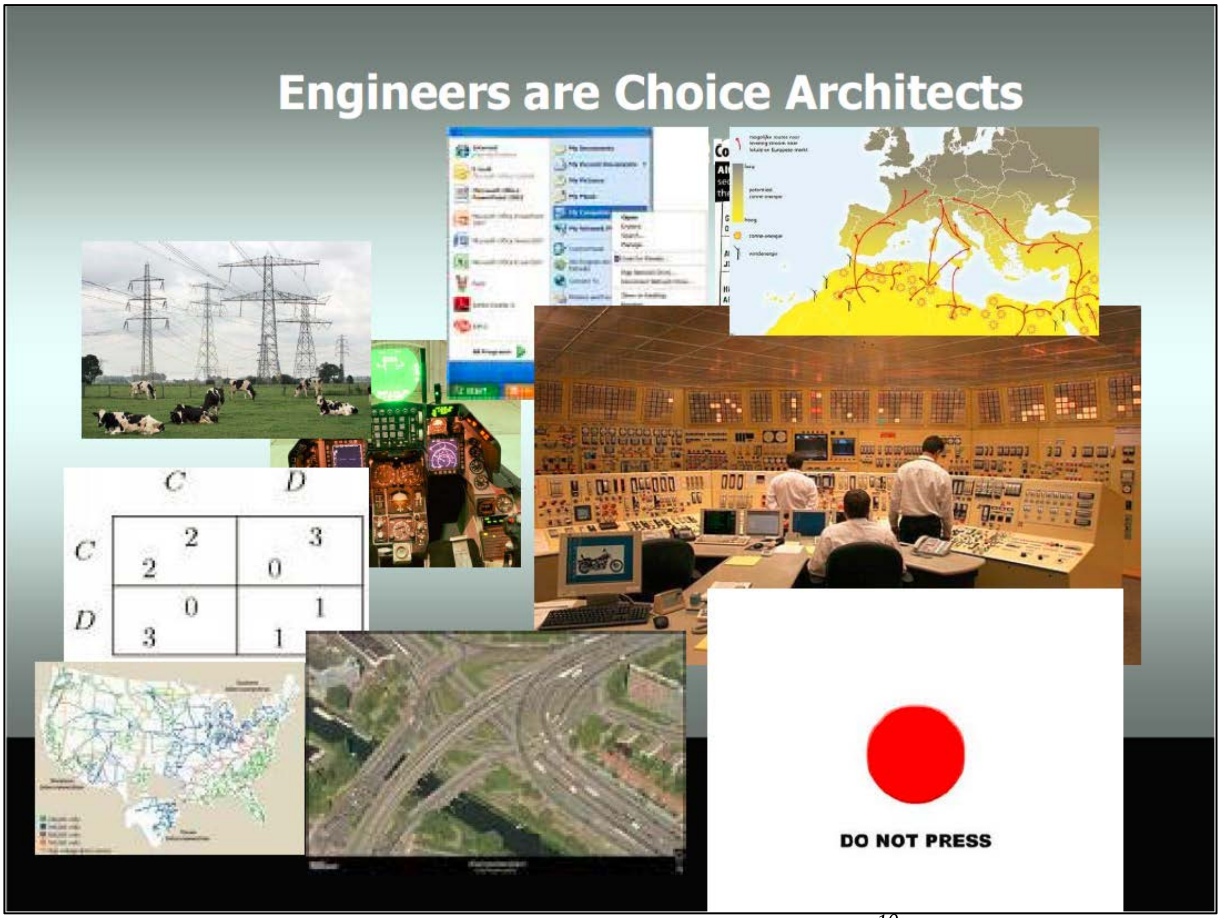
Justify
Audit

Artefacts
Architectures
Materials
Standards
Security
Systems
Infrastructure

Computers
Oiltankers
Airplanes
Reactors
Roads
Internet
Electricity
Grids
Hospitals

21st Century: Value Sensitive Design

Figure 12 – Value-Sensitive Design[10]



Engineers are Choice Architects

DO NOT PRESS

Figure 13 – Engineers as Choice Architects[10]

Value synergy designs things with the most value in mind by taking advantage of all value available in multiple elements. In maximizing value across multiple areas, a resulting synergy should assist at least somewhat related concepts that lead to a best-case scenario. In terms of privacy and sustainability, it is especially difficult to reach that ideal quadrant as shown in Figure 14. Value synergy, however, allows us to reach beyond liner notions to achieve that desired scenario with a high level of both factors as in Figure 15.

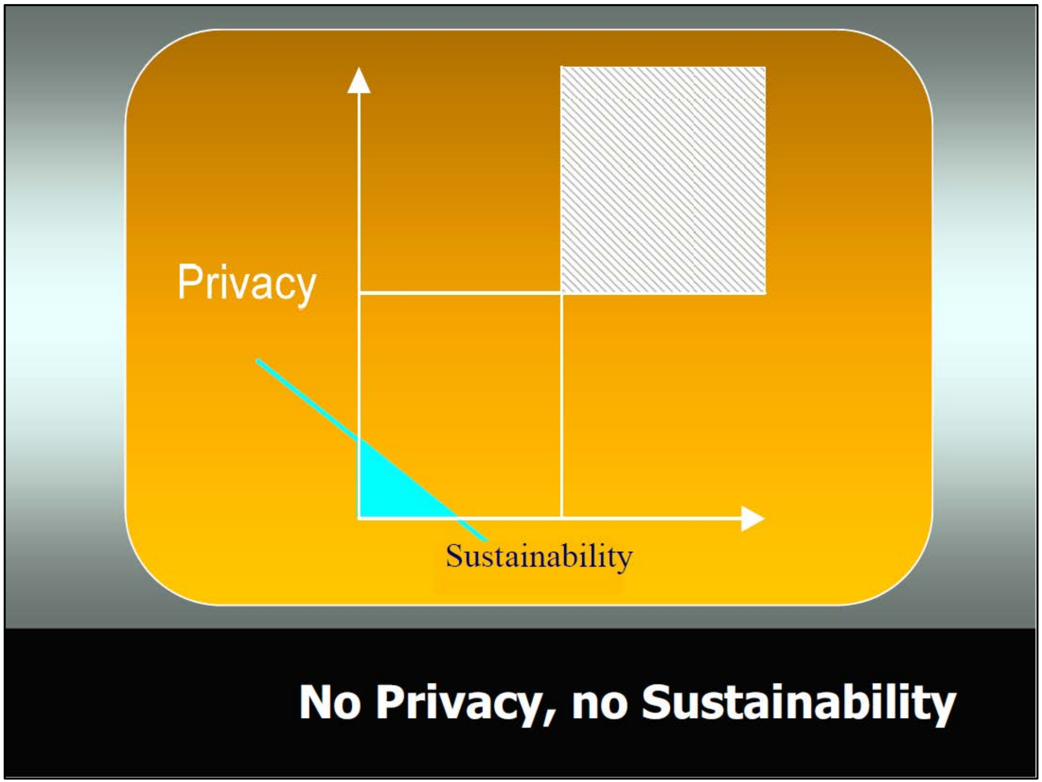


Figure 14 – Privacy and Sustainability without Value Synergy[10]

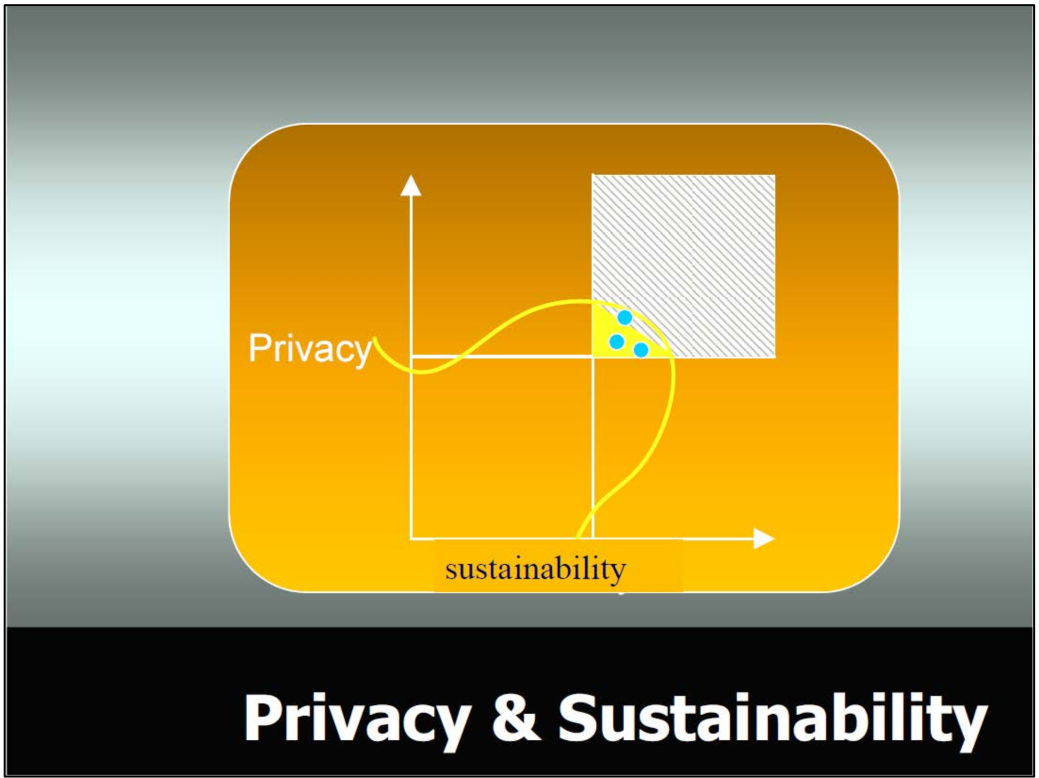


Figure 15 – Privacy and Sustainability with Value Synergy[10]

Governance Issues

At the 10th Meeting of The Internet of Things Expert Group in Brussels, a number of governance issues were presented for consideration. These included the following:

- Should governance be administered using Internet platform, or are new platforms required?
- Should IoT-specific legislation be required to govern privacy and security?
- Should IoT legislation be a soft (non-binding) legislation or something more stringent?

Additionally, governance will have to address privacy, security, and competitiveness.

No consensus exists on whether existing governmental bodies or new ones should govern IoT. As a result, no specific actions on policy are currently proposed as they are considered premature at this time. However, three major views have been observed to exist in terms of legal legislation relating to IoT technology. [8]

- Legislation is believed to potentially introduce considerable burdens and quickly become obsolete. IoT-specific legislation is, therefore, not suitable for consideration.
- There is no one-size-fits-all prescription for privacy by default. Therefore, even general legislation is not suitable for consideration.
- No decision on legislation or similar can be made at this time. More time is needed for further consideration.

As policy is developed, it should strive to maintain several objectives.[19]

- **Policy should avoid the emergence of social injustice.**
  IoT assumes the societal divide between those who have and do not have access to Internet technology is a null factor. In truth, much debate still exists around the importance of this divide as it also creates a knowledge divide which separates those who have knowledge to master the new technology from those who are dependent on experts. Many argue that fair access to IoT technology and qualification of the citizens to use it, as well as alternatives for those who voluntarily do not want to engage with IoT, be included in the design of the new technology.
- **Establish trust in the IoT.**
  Design of IoT devices and architecture must support users' ability to trust IoT. Effective technical functioning, protection of personal data, and ensured privacy and usable security management should all be included.
- **Ensure the adequateness of IoT metaphors.**
  Researchers and industry must fairly represent IoT through metaphors that not only highlight its conveniences, but also its dangers. Metaphors used in discourse framing must also keep up with the development of the technology to ensure dissemination of the most accurate information as it advances.
- **Creating a social contract between people and objects.**
  By using things in the IoT, people must delegate actions to objects. The actions being taken should be those actually intended by the user, and should not be deceptive in any

way. Algorithms used may also be blind toward special needs of individuals, and these procedures must consider moral implications as they are designed and used.

- **Allow for informed consent.**
  It is highly important in privacy scenarios for contemporary information technology that persons being exposed to the technology be informed that they are interacting with it in some way. Focus must emphasize making otherwise invisible IoT technology visible to those interacting with it for inspection purposes.

> *"We should not be concerned with self-parking cars but with the ethical foundations and consequences of delegating parking decisions to automotive systems"*
> By Internet of Things Expert Group[19]

When governmental authorities do initiate efforts in terms of legislation surrounding IoT, it will be difficult to silo such decisions as the IoT is a global phenomenon. Based on current efforts, Europe appears most likely to be the first adopters of any such legislation. Other foreign actors would then have to follow suit.

> *"Internet is bringing the world closer to one, integrated society."*
> By Lee Freeman & A. Graham Peace[15]

In terms of organizations and ethically sound IoT technological advancement, those establishments most likely to adopt IoT technology in an ethically agreeable manner are most likely organic rather than mechanistic in culture and environment. In a 2007 empirical study conducted on information technology professionals' perceived organizational values and managerial ethics, organic organizations were defined as openly collaborate, creative, encouraging, sociable, relationship-oriented, equitable, empowering, and trusting. This is also the assumed norm for a democratic society. Mechanistic organizations were the other form under consideration, and were defined as cautious, task-oriented, rigidly structured, and maintained hierarchical values oriented toward centralization, pressure, power, and procedures. This form is generally regarded as more bureaucratic. The key finding of the study was that moral reflection by employees tends to decrease as centralization (frequented by bureaucratic or mechanistic organizations) increases.[14] Mechanistic organizations are therefore most likely to desire IoT technology applied in a manner opposite that of the general public compared to organic organizations.

> *"We are clearly less protected than 20 or even 10 years ago. The increase in the power and use of information technology, and the corresponding inability of governmental agencies to develop applicable laws in a timely manner, ensures that intellectual property rights and privacy are much less protected in today's society than before the widespread adoption of the Internet."*
> By Lee Freeman & A. Graham Peace[15]

While information ethics in relation to IoT is the current subject of a very heated and multi-directional debate, one agreed upon matter does exist with great certainty: "a debate on the future values of living is necessary" (pg. 21).[19] Without such crucial discussion, the IoT will arrive and affect our lives in highly intricate ways without regard for important considerations such as privacy, security, and trust.

RESEARCH QUESTIONS

The focus of this research was to first and foremost uncover existing perceptions and beliefs around the IoT, disruptive technology, and information ethics. The following questions guided research pertaining to the literature review:

- What is known about the IoT?
- What is known about the IoT's technological implications to this point in time?
- What perceptions exist surrounding the IoT?
  - What level of awareness exists surrounding IoT as a rapidly developing disruptive technology?
- How do people perceive information ethics in terms of the IoT?

Upon review of the literature, four constructs of interest were chosen for further investigation via design and distribution of a survey: privacy, security, trust, and convenience. These four constructs appeared more than once across the literature with special focus provided by an IoT Expert Group in the European Union.[8, 19]

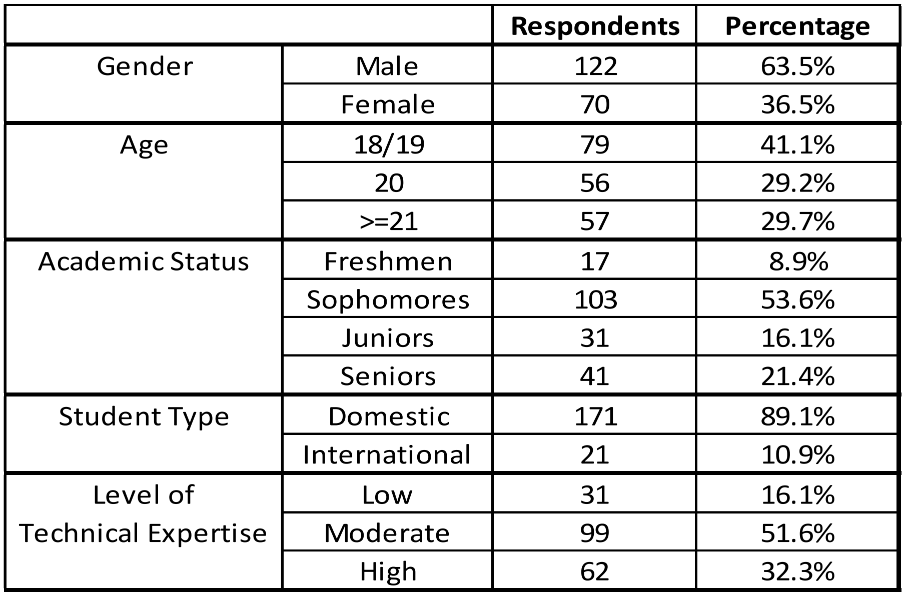
METHODOLOGY

A thorough review of available literature relating to the three bodies of interest—the Internet of Things, disruptive technology, and information ethics—was conducted with special focus on implications for the Internet of Things. An exploratory study was then developed based on the literature review via a survey tool. The chosen methodologies for analysis of the survey data included average of the means and analysis of variance (ANOVA).

Data Collection

An electronic survey powered by QuestionPro was distributed to university students enrolled in an undergraduate business program at a private university in the Northeast United States. The survey instrument had been previously presented to three students as a test for ease of use and ambiguity. These students made some suggestions leading to revised questions that included more positive-looking statements to ease question understanding, and also led to the removal of a section of miscellaneous questions of interest relating to some specific IoT applications including smart refrigerators, self-driving vehicles, and perceptions around data mining. This preliminary survey feasibility test resulted in a more concise instrument which reduced the time to complete the survey by up to five minutes. These three collections of data were not included in the final dataset. The survey instrument in its distributed form is included in the Appendix.

A total of 192 usable responses were received. The profile of the respondents is summarized in Table 1. Of the sample, 63.5% were male. The majority of the respondents were between 19 and 21 years old (81.2%). About half (53.6%) were sophomores at the university. Most respondents were also domestic U.S. students (89.1%). About half of the respondents indicated a moderate level of technical expertise with computer technology (51.3%) with an additional one-third (32.3%) reporting a higher level of expertise.



		Respondents	Percentage
Gender	Male	122	63.5%
	Female	70	36.5%
Age	18/19	79	41.1%
	20	56	29.2%
	>=21	57	29.7%
Academic Status	Freshmen	17	8.9%
	Sophomores	103	53.6%
	Juniors	31	16.1%
	Seniors	41	21.4%
Student Type	Domestic	171	89.1%
	International	21	10.9%
Level of Technical Expertise	Low	31	16.1%
	Moderate	99	51.6%
	High	62	32.3%

Table 1 – Demographic profile of the respondents

Data Analysis and Results

The survey administered contained six vignettes selected to represent important application of the IoT. The vignette scenarios included applications of the following:

1. A remote home management and security system accessed remotely via mobile device
2. An placed order and remote notification by a smart refrigerator performing automatic shopping for its owner
3. Remote smart grid technology coupled with a home energy management system
4. A smart car interacting in real-time with its traffic-related surroundings while on the road
5. Automated issuance and notification of a speeding ticket by a freeway speed sensor
6. Targeted contextual advertising via smartphone based on the TV show currently being watched

Respondents were asked to rank on a scale of one (1) to seven (7) their agreement with five questions for each of the vignettes. The first four questions each corresponded to one of the four constructs: privacy, security, trust, and convenience.

Figure 16 displays the respective averages of the four key constructs across all six vignettes. The results indicate that the average of the respondents rating on each of the four constructs hovered around a response of four (Neither Agree Nor Disagree) on the seven-point scale, . This suggests that on average respondents tended not to have extreme positions among the four constructs.

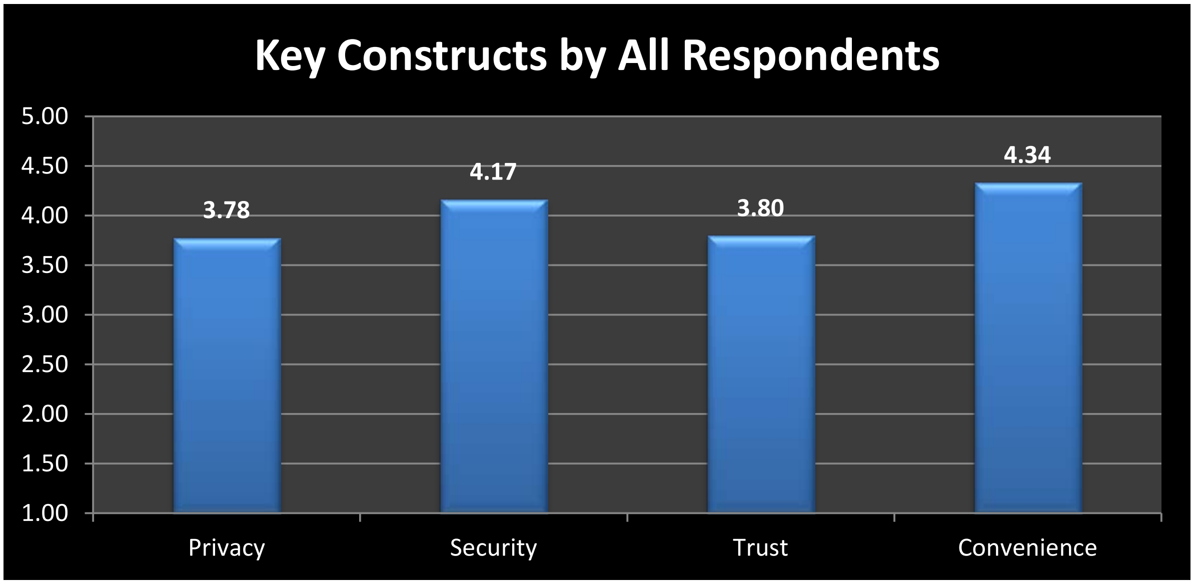


Figure 16 – Key Constructs by All Respondents

When taking into consideration the individual demographic factors of gender (Figure 17), age, (Figure 18), academic status (Figure 19), student type (Figure 20), and computer technology expertise (Figure 21) the comparative means suggest that there were no observable differences within a demographic factor for each the four constructs of privacy, security, trust and convenience.

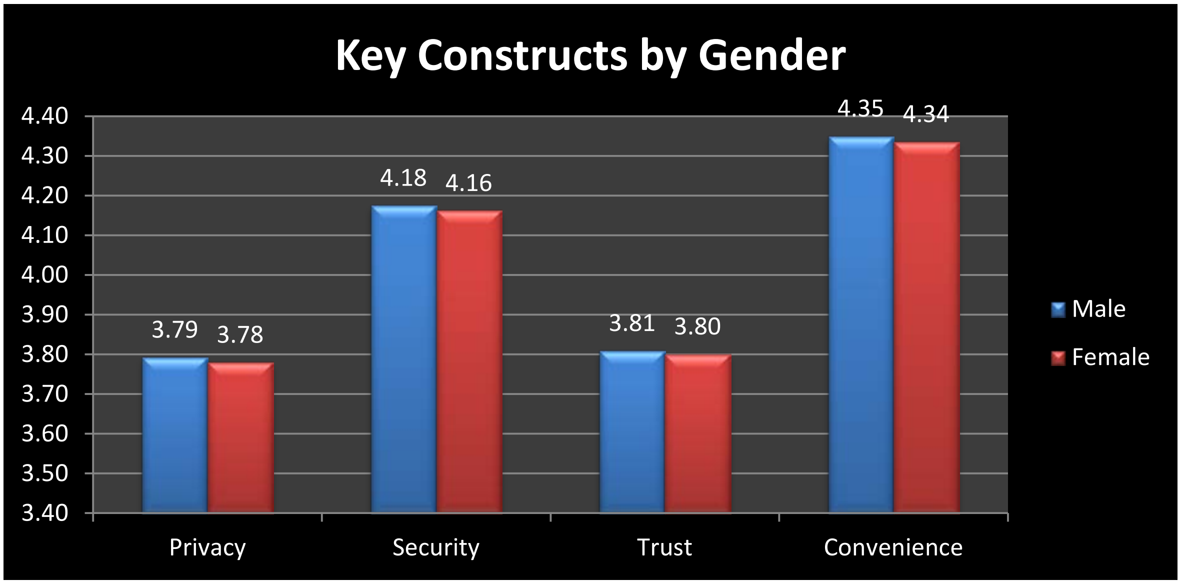


Figure 17 – Key Constructs by Gender

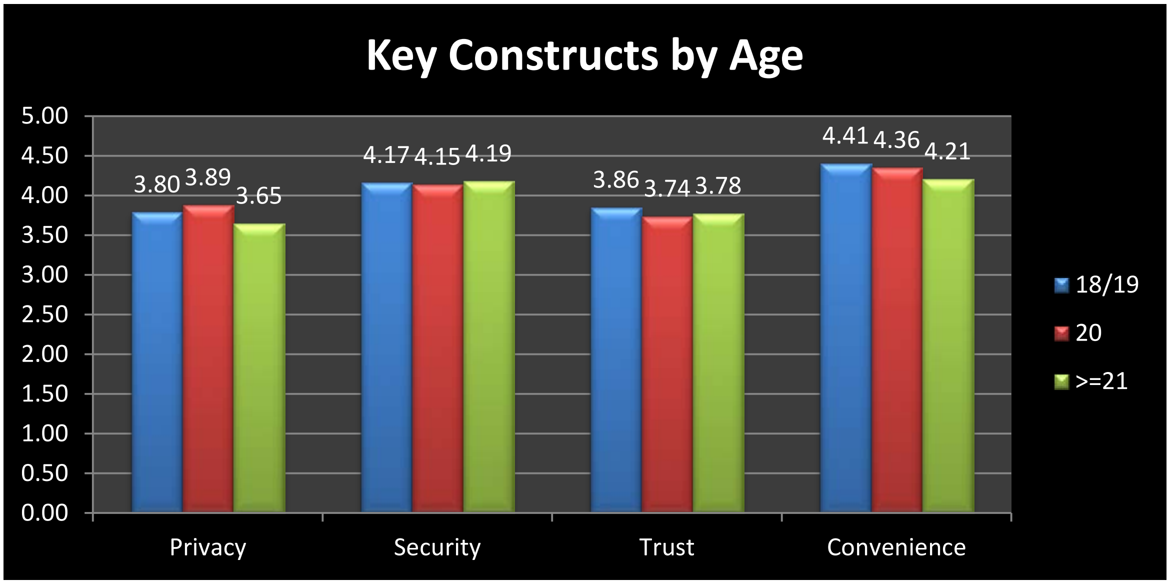


Figure 18 – Key Constructs by Age

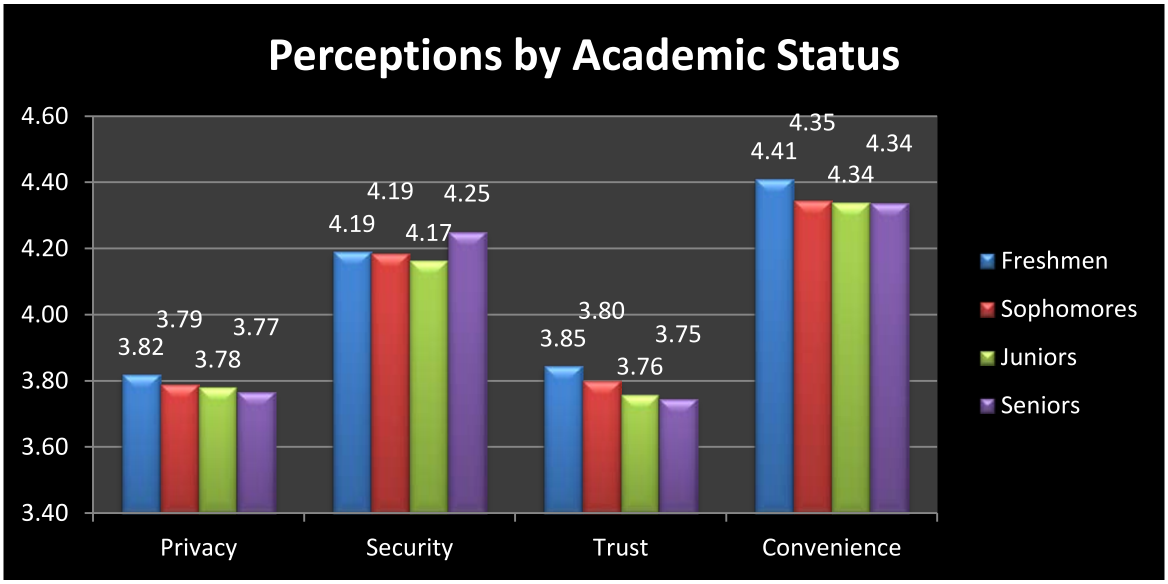


Figure 19 – Perceptions by Academic Status

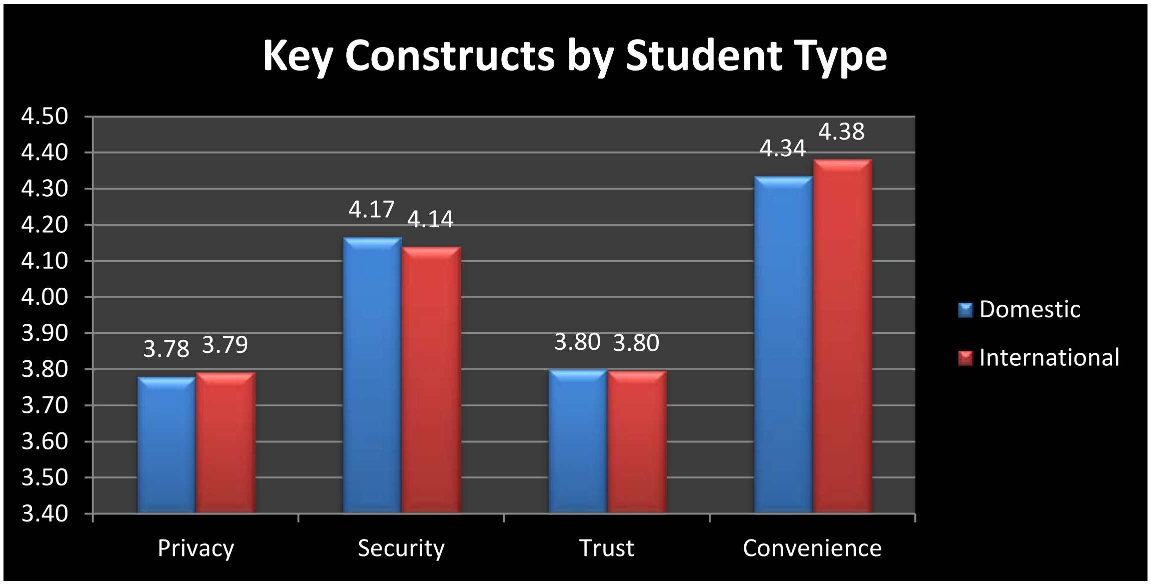


Figure 20 – Key Constructs by Student Type

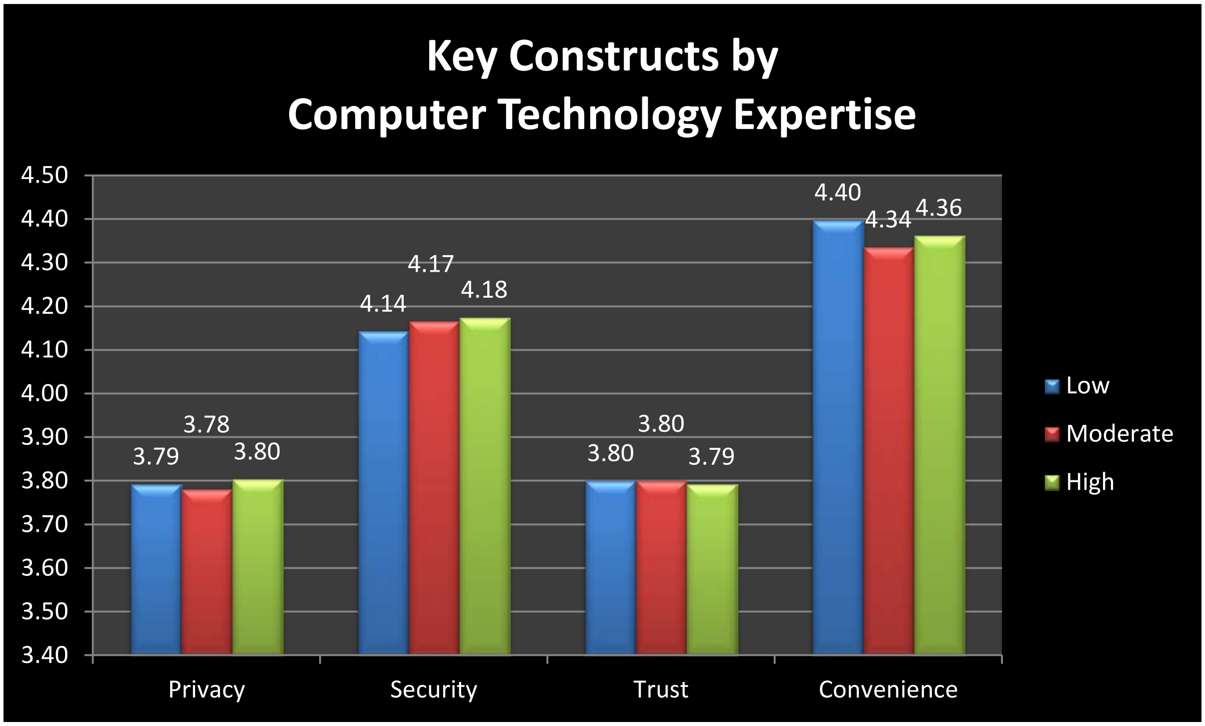


Figure 21 – Key Constructs by Computer Technology Expertise

In analyzing the means across the four constructs by vignette scenario, the results indicated an inverse relationship between privacy and convenience. Furthermore, the inverse relationship changes direction dramatically for scenarios five and six compared to the first four scenarios. Privacy concerns were markedly lower compared to convenience for the first four vignettes, while the latter two scenarios saw a dynamic switch where privacy was remarkably high while convenience was relatively low. Figure 22 shows these results graphically while Table 2 displays them numerically.

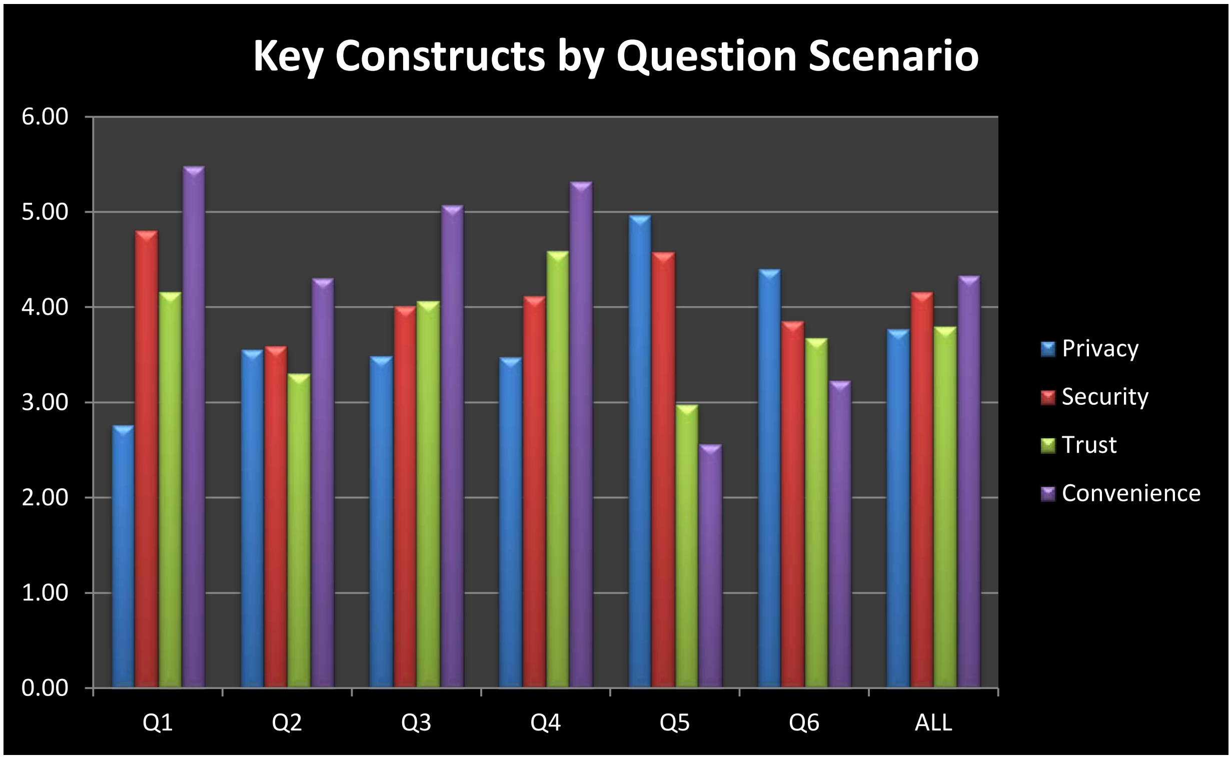


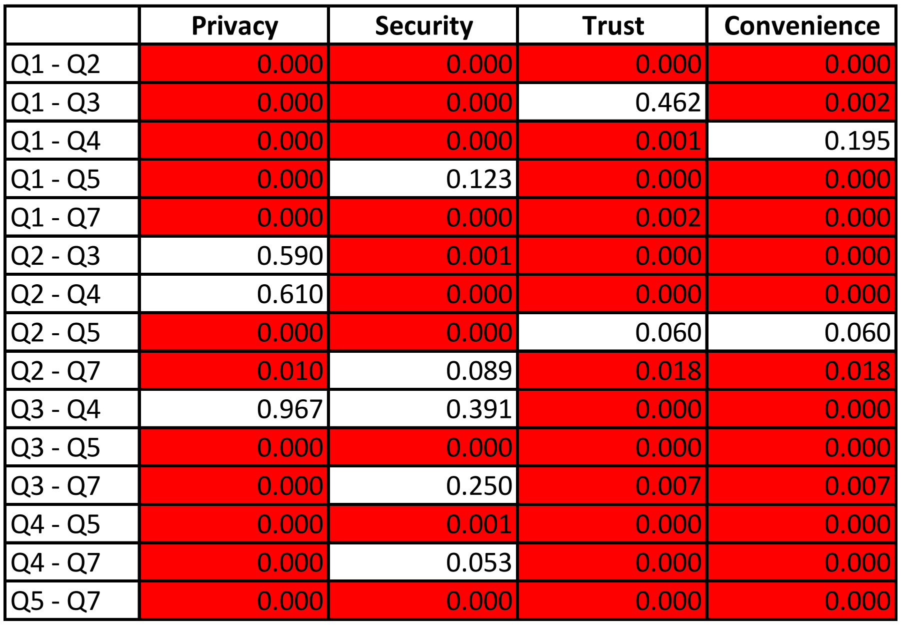
Figure 22 – Key Constructs by Question Scenario

Comparison of Means

	Privacy	Security	Trust	Convenience
Q1	2.77	4.81	4.16	5.49
Q2	3.56	3.60	3.31	4.32
Q3	3.49	4.02	4.07	5.08
Q4	3.48	4.13	4.60	5.32
Q5	4.98	4.58	2.99	2.57
Q6	4.41	3.86	3.68	3.23
ALL	3.78	4.17	3.80	4.34

Table 2 – Key Constructs by Question Scenario

Additionally, Table 3 shows the results of one-way ANOVA between each scenario by construct. As expected due to the different kinds of constructs investigated in the differing types of vignettes posed, the large majority of the questions asked were found to be significant.



	Privacy	Security	Trust	Convenience
Q1 - Q2	0.000	0.000	0.000	0.000
Q1 - Q3	0.000	0.000	0.462	0.002
Q1 - Q4	0.000	0.000	0.001	0.195
Q1 - Q5	0.000	0.123	0.000	0.000
Q1 - Q7	0.000	0.000	0.002	0.000
Q2 - Q3	0.590	0.001	0.000	0.000
Q2 - Q4	0.610	0.000	0.000	0.000
Q2 - Q5	0.000	0.000	0.060	0.060
Q2 - Q7	0.010	0.089	0.018	0.018
Q3 - Q4	0.967	0.391	0.000	0.000
Q3 - Q5	0.000	0.000	0.000	0.000
Q3 - Q7	0.000	0.250	0.007	0.007
Q4 - Q5	0.000	0.001	0.000	0.000
Q4 - Q7	0.000	0.053	0.000	0.000
Q5 - Q7	0.000	0.000	0.000	0.000

(Highlighted results are significant at the .05 level)

Table 3 - Results of One-Way ANOVA Between Individual Question Items

DISCUSSION AND IMPLICATIONS

An exploratory study was conducted to investigate university students' perceptions of the IoT. Four constructs were considered including privacy, security, trust and convenience. Previous research has identified these four constructs as major issues for the effective adoption of the IoT. College students were selected for the survey because they will be entering the workforce just as applications of the IoT become more readily available. Graduated student acceptance of the technology will be important for successful adoption.

Students were most concerned about convenience of the technology (m=4.34) followed by security issues (m=4.17), trust (m=3.80) and privacy (m=3.78). In general, the mean responses of all students varied between 3.78 and 4.34 with standard deviations for each individual question that did not exceed 1.8. This suggests that student perceptions on average were not extreme. The fact that students do not have strong opinions about the IoT with respect to privacy, security, trust and convenience may be the result of their being unfamiliar with the IoT and the likelihood that they do not have personal experience using the technology due to its relative immaturity.

The largest difference was between privacy and convenience. Convenience would appear to be a more important factor for students than privacy concerns. At face value, this result may be expected for this age group; however, there was a very interesting and notable relationship between these two constructs. Privacy concerns have the lowest means and convenience concerns have the highest means for the first four scenarios. However, for the last two scenarios the two constructs reverse the relationship with privacy having the highest mean and convenience having the lowest for the last two scenarios. This is a striking reversal in student perceptions. This result appears to be related to the type of scenarios that the students were presented with. The first four scenarios deal with situations that appear to be less personal than the last two. These four scenarios have the IoT perform a service that efficiently manages familiar functions and reduces the effort of the individual to manage these functions. For example, scenario one describes how an IoT application can automatically manage a home security system and control heating; scenario two automatically checks your groceries and reorders them; scenario three monitors your energy expenditures at home and efficiently controls them; and scenario four has the IoT reduce your time stuck in traffic. The last two scenarios are of a much more personal nature. In scenario five, the IoT monitors your individual driving patterns and automatically issues you a ticket for speeding. This scenario is perceived to be more of a privacy concern than all others. The last scenario has the IoT monitoring your individual television viewing patterns and sending ads for new products to your smartphone that are specifically targeted to your profile.

The fact that students perceive these scenarios differently with respect to privacy has strong implications for the potential adoption of the IoT. While other applications of such technology may prove more convenient and offer less overall concern for privacy, IoT applications on a highly personal level of contact may not be as well-received by people. This is an important finding for IoT architects, businesses, and government especially as it demands a need for limitation in the degrees of invasiveness and informed consent required by the public. Vendors will have to focus their marketing of IoT applications differently depending on how directly the IoT application is perceived by the individual to affect them at a personal level. The scenario with the IoT application issuing a ticket has many similarities to the video systems installed at traffic lights that capture video of automobiles going through red lights and issuing tickets. While it may be argued that these systems improve safety and earn money for cash strapped cities, many cities have removed these systems based on widespread complaints by the public.

Another interesting finding of this research was that there appears to be very little difference among student perceptions across different demographic characteristics. Mean responses for each of the 4 constructs did not vary by academic status (freshman, sophomore, junior, senior), student type (domestic, international) or by the degree of expertise with computer technology. This may be because students are not aware of the IoT, or may be related to the fact that the sample was fairly homogeneous. This finding warrants future research to determine whether the results may be replicated. If, in fact, perceptions across demographics are fairly similar, then this may facilitate the acceptance of the IoT among this group by enabling vendors to create a campaign with a uniform message.

One finding that did demonstrate a difference was the fact that concerns for privacy differed by the age of the respondent. Students in the 21 or older group tended to view privacy as less of an issue. Given that there was little difference by age for security, trust, and convenience this result may be an aberration of the data. Further research may explore whether this finding is significant. If so, it may imply that as students reach the age of graduation and entry into the workforce, privacy issues may decline in importance for adoption of the IoT.

Limitations and Future Research Focus

One of the limitations of this research relates to the sample selected. Survey respondents were undergraduate students enrolled in a private college in the northeast United States. While students of several majors were represented, the bulk of the students were business majors with most students between the ages of 18 and 21. Further variation in the population demographics and inclusion of non-students should be undertaken to determine whether these results are generalizable to a wider population.

The development of additional question scenarios relating to IoT technology may also improve the quality of results generated. This study did not include more scenarios as the survey was distributed during limited class time by professors, and it also strived to maintain a high rate of completion by respondents who may have been less apt to complete the instrument in its entirety if it were longer.

A study that compares perceptions of convenience and privacy relating to the IoT may provide important findings for the introduction of IoT technology given the relationships between these two constructs described above. It would also be interesting to study what characteristics of the IoT are perceived by individuals to be more invasive with respect to privacy and whether these factors vary by demographic.

This research project did not consider other factors that may influence perceptions of privacy, security, trust, and convenience for the IoT. For example, how do personality factors play into the perceptions of the four constructs for different types of scenarios? How does social influence play a role? These questions also indicate areas for future research.

APPENDIX

Survey

You are invited to participate in a Bryant University Honors Program Senior Capstone Project survey about perceptions of the Internet of Things. The Internet of Things refers to uniquely identifiable objects and their virtual representations in an Internet-like structure.

Your participation in this study is completely voluntary. There are no foreseeable risks associated with this project. However, if you feel uncomfortable answering any questions, you can withdraw from the survey at any point. It is very important for us to learn your opinions.

Your survey responses will be strictly confidential and data from this research will be reported only in the aggregate. Your information will be coded and will remain confidential. If you have questions at any time about the survey or the procedures, you may contact Kyle Ebersold at (413) 563-3278 or by email at kebersol@bryant.edu.

Thank you very much for your time and support.

The Internet of Things
Senior Capstone Project for Kyle Ebersold

Please answer the questions below.

1. **How old are you?**
   _____ years old

2. **What is your gender?**
   [ ] Male [ ] Female

3. **What is your academic status?**
   [ ] Freshman
   [ ] Sophomore
   [ ] Junior
   [ ] Senior
   [ ] Graduate Student

4. **What is your major/concentration? Please list all if more than one concentration.**

   ____

   ____

5. **Are you an international student?**
   [ ] Yes [ ] No

6. **How would you rate your level of expertise with computer technology?**
   [ ] Very Little
   [ ] Some
   [ ] Moderate
   [ ] High
   [ ] Expert

Please rate your level of agreement with each of the statements following the scenarios described below.

You arrive at work, and your GPS location is automatically transmitted by your smartphone to your home management system. Your home security system recognizes that you have arrived at work and sends you a notification on your smartphone that your home's security system has automatically armed itself, your house doors have automatically been locked, and the heat in the house has been turned off and will turn on again at exactly 4:45pm.

	Disagree strongly			**Neither agree nor disagree**			**Agree strongly**
This automated home security system is an invasion of privacy.	1	2	3	4	5	6	7
I would be concerned that a hacker could potentially break into my home management system.	1	2	3	4	5	6	7
I would trust an Internet-capable electronic door lock and security system to effectively secure my home.	1	2	3	4	5	6	7
I would find it convenient for my home security system to lock/unlock doors and set my alarm system and heat automatically via my smartphone or other mobile device.	1	2	3	4	5	6	7
I would not be worried about an Internet-generated breach into my home via the home security system.	1	2	3	4	5	6	7

While at work, your smartphone buzzes with a notification that your smart refrigerator has automatically placed an order for milk, bread, and deli meat. The system determined that you were running low on these items and would need them for the next day according to your recent dietary choices. The notification also informs you that these items have been paid for automatically by debiting your checking account and that the items will be available after 4pm for you to pick up at the supermarket closest to your usual route home from work.

	Disagree strongly			**Neither agree nor disagree**			**Agree strongly**
I would not trust a smart refrigerator to perform grocery shopping for me.	1	2	3	4	5	6	7
I would be concerned about an Internet-generated break in to my smart refrigerator.	1	2	3	4	5	6	7
I would trust an Internet-capable smart refrigerator to pay for my groceries.	1	2	3	4	5	6	7
I would be concerned about my privacy in using a smart refrigerator.	1	2	3	4	5	6	7
I would find it convenient to have a smart refrigerator automatically order food for me.	1	2	3	4	5	6	7

In the early afternoon of a blisteringly hot summer day, your home energy management system sends you a message on your smartphone that the electric company has remotely shut off your air conditioning, hot water heating tank, and a home light that you left on by accident this morning because your neighborhood is experiencing a peak grid period which would increase your electric bill. A few hours later, you receive another notification that the peak period has ended and power has been restored to these electrical devices.

	Disagree strongly			**Neither agree nor disagree**			**Agree strongly**
I would find it convenient to have a home energy management system make real-time decisions to efficiently manage my home energy use.	1	2	3	4	5	6	7
I would be concerned that a hacker could potentially break into a home energy management system.	1	2	3	4	5	6	7
I trust my electric company to appropriately monitor the specifics of my home energy use down to the appliance-level and communicate with my home energy management system.	1	2	3	4	5	6	7
I would be opposed to a home energy management system that communicated automatically with my electric company.	1	2	3	4	5	6	7
I would not trust my electric company to appropriately monitor the specifics of my home energy use down to the appliance-level.	1	2	3	4	5	6	7
This home energy management system is an invasion of privacy.	1	2	3	4	5	6	7

On your way back from work, you hop in your "smart car" equipped with a state-of-the-art on-board computer. After easing through several green stoplights on your way to the freeway, you recall a time just a few years ago, where you used to get stuck in long car lines at those intersections before smart vehicles like yours began to "talk" with intersection stoplights to ease traffic patterns in real-time.

	Disagree strongly			**Neither agree nor disagree**			**Agree strongly**
I would find it convenient to have traffic and transportation authorities monitor drivers on the road via sensors and advanced monitoring technology.	1	2	3	4	5	6	7
I do not trust sensor/monitoring technology in use by traffic and transportation authorities.	1	2	3	4	5	6	7
I trust sensor/monitoring technology in use by traffic and transportation authorities.	1	2	3	4	5	6	7
Having traffic and transportation authorities monitor drivers on the road via sensors and advanced monitoring technology is an invasion of privacy.	1	2	3	4	5	6	7
I would be concerned that a hacker may potentially break into traffic monitoring systems.	1	2	3	4	5	6	7

While on the freeway, your car's on-board computer notifies you that you have been issued a speeding ticket by the local police authority based on a highway sensor that flagged your car traveling over the freeway's speed limit.

	Disagree strongly			**Neither agree nor disagree**			**Agree strongly**
I would find it convenient to have police enforcement of traffic regulations via sensors and advanced monitoring technology.	1	2	3	4	5	6	7
I think sensor technology that monitors traffic is an invasion of privacy by law enforcement.	1	2	3	4	5	6	7
I do not think sensor technology like the one described above is an invasion of privacy by law enforcement.	1	2	3	4	5	6	7
I trust sensor/monitoring technology in use by law enforcement authorities.	1	2	3	4	5	6	7
I would be concerned that a hacker may potentially break into police sensors/monitoring systems.	1	2	3	4	5	6	7

While watching TV, an ad pops up on your smartphone about a new product/service specifically targeted for people in the demographic that usually watch this show.

	Disagree strongly			**Neither agree nor disagree**			**Agree strongly**
I would find it convenient to have my smartphone personalize ads to me for a new product/service based on what I am currently watching.	1	2	3	4	5	6	7
I would not find it convenient to have my smartphone personalize ads to me for a new product/service based on what I am currently watching.	1	2	3	4	5	6	7
I would be concerned about my privacy in receiving personalized ads on my smartphone.	1	2	3	4	5	6	7
I would be concerned that a hacker may potentially break into my smartphone-TV communication.	1	2	3	4	5	6	7
I trust this type of smartphone-TV communication to remain private.	1	2	3	4	5	6	7

REFERENCES

[1] "The Executive's Guide to the Internet of Things." TechRepublic. CBS Interactive, Jan. 2013. Web. 22 Apr. 2014. <http://www.techrepublic.com/resource-library/downloads/the-executive-s-guide-to-the-internet-of-things/>.

[2] "Tapping M2M: The Internet of Things." ZDNet. CBS Interactive, n.d. Web. 22 Apr. 2014. <http://www.zdnet.com/topic-tapping-m2m-the-internet-of-things/>.

[3] "Intro: Tapping M2M, The Internet of Things." ZDNet. CBS Interactive, 14 Dec. 2012. Web. 22 Apr. 2014. <http://www.zdnet.com/video/intro-tapping-m2m-the-internet-of-things-10110629/>.

[4] Detwiler, Bill. "71 Percent Say M2M Is about Developing New Business Opportunities." ZDNet. CBS Interactive, 4 Apr. 2013. Web. 22 Apr. 2014. <http://www.zdnet.com/71-percent-say-m2m-is-about-developing-new-business-opportunities-7000009304/>.

[5] Rouse, Margaret. "Disruptive Technology." What Is ? TechTarget, Aug. 2011. Web. 22 Apr. 2014. <http://whatis.techtarget.com/definition/disruptive-technology>.

[6] Manyika, James, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy." McKinsey & Company. McKinsey & Company, May 2013. Web. 22 Apr. 2014. <http://www.mckinsey.com/insights/business_technology/disruptive_technologies>.

[7] Downes, Larry. "The Five Most Disruptive Technologies at CES 2013." Forbes. Forbes Magazine, 12 Jan. 2013. Web. 22 Apr. 2014. <http://www.forbes.com/sites/larrydownes/2013/01/12/the-five-most-disruptive-technologies-at-ces-2013/2/>.

[8] Wachtel, Tom. "IoT Expert Group Final Meeting Report." European Commission. European Commission, 14 Nov. 2012. Web. 22 Apr. 2014. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=1747>.

[9] "Value Sensitive Design." Dub. University of Washington, n.d. Web. 22 Apr. 2014. <http://dub.washington.edu/projects/value-sensitive-design>.

[10] Van Den Hoven, Jeroen. "Ethics and The Internet of Things." European Commission. Delft University of Technology, n.d. Web. 22 Apr. 2014. <http%3A%2F%2Fec.europa.eu%2Ftransparency%2Fregexpert%2Findex.cfm%3Fdo%3DgroupDetail.groupDetailDoc%26id%3D7607%26no%3D4>.

[11] Frohmann, Bernd. "Subjectivity and Information Ethics." Journal of the American Society for Information Science and Technology 59.2 (2008): 267. ProQuest. Web. 22 Apr. 2014.

[12] [Journal of Future Studies article] (DLed “R01.pdf)

[13] Burk, Dan L. "Information Ethics and the Law of Data Representations." Ethics and Information Technology 10.2-3 (2008): 135-47. ProQuest. Web. 22 Apr. 2014.

[14] Jin, K. G., Ron Drozdenko, and Rick Bassett. "Information Technology Professionals' Perceived Organizational Values and Managerial Ethics: An Empirical Study." Journal of Business Ethics 71.2 (2007): 149-59. ProQuest. Web. 22 Apr. 2014.

[15] Freeman, Lee, and Graham Peace A. "Information Ethics: Privacy and Intellectual Property." Information Management Spring 2005: 17,17,31. ProQuest. Web. 22 Apr. 2014 .

[16] Siponen, Mikko. "A Pragmatic Evaluation of the Theory of Information Ethics." Ethics and Information Technology 6.4 (2004): 279. ProQuest. Web. 22 Apr. 2014.

[17] Levine, Peter. "Information Technology and the Social Construction of Information Privacy: Comment." Journal of Accounting and Public Policy 22.3 (2003): 281-85. Web. 22 Apr. 2014.

[18] "Internet of Things Demands Rethinking of Business Ethics." SmartPlanet. CBS Interactive, n.d. Web. 22 Apr. 2014. <http%3A%2F%2Fwww.smartplanet.com%2Fblog%2Fbusiness-brains%2Finternet-of-8216things-demands-rethink-of-business-ethics%2F11435>.

[19] Van Den Hoven, Jeroen. "Fact Sheet - Ethics Subgroup IoT - Version 4.0." European Commission. Delft University of Technology, n.d. Web. 22 Apr. 2014. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDwQFjAA&url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fnewsroom%2Fcf%2Fdae%2Fdocument.cfm%3Fdoc_id%3D1751&ei=30lUUqnkMcep4APxwIGwDA&usg=AFQjCNG_VgeaUP_DIJVwSiPIww3bC9Ug_w&sig2=DEVquzOFpQWwjhMud5bXIg&bvm=bv.53537100,d.dmg>.

ADDITIONAL RESOURCES

Committee on Forecasting Future. Persistent Forecasting of Disruptive Technologies. Washington, D.C.: National Academies, 2010. Print.

Griffith, Eric. "Home Smart Home." PC Magazine (2012): 165-176. Academic Search Premier. Web. 10 Apr. 2013.

Himma, Kenneth Einar., and Herman T. Tavani. The Handbook of Information and Computer Ethics. Hoboken, NJ: Wiley, 2008. Print.

Hwang, Kai, Geoffrey C. Fox and Jack J. Dongarra. Distributed and Cloud Computing. Waltham, MA: Elsevier, Inc., 2012. Print.

Journal of Business Ethics (2010-2013). Web.

Lin, Patrick. "The Ethics of Saving Lives With Autonomous Cars Is Far Murkier Than You Think." Wired.com. Conde Nast Digital, 30 Aug. 0013. Web. 23 Apr. 2014. <http://www.wired.com/opinion/2013/07/the-surprising-ethics-of-robot-cars/>.

Lohman, Tim. "The Business Benefits of Machine to Machine." ZDNet. CBS Interactive, 10 Jan. 2013. Web. 22 Apr. 2014. <http://www.zdnet.com/the-business-benefits-of-machine-to-machine-7000008924/>.

Martin, Kirsten. "Managing Disruptive Technologies - Kirsten Martin." YouTube. Institute for Corporate Ethics, 11 Oct. 2011. Web. 23 Apr. 2014. <http://www.youtube.com/watch?v=ds0p7MqqfUQ>.

Reynolds, George. Ethics in Information Technology. Canada: Thomson Learning, Inc., 2011. Print.

Satava, Richard M., Achille Gaspari, and Nicola Di Lorenzo. Emerging Technologies in Surgery. Berlin: Springer, 2007. Print.

Spinello, Richard. Cyberethics: Morality and Law in Cyberspace. Jones & Bartlett Publishers, 2010. Print.

van Kranenburg, Rob. The Internet of Things: A critique of ambient technology and the all-seeing network of RFID. Amsterdam: Institute of Network Cultures, 2008. Web Document.

Vander Ark, Tom. Getting Smart. San Francisco, CA: John Wiley & Sons, Inc., 2012. Print.