https://doi.org/10.48009/4_iis_2015_194-201

Issues in Information Systems
Volume 16, Issue IV, pp. 194-201, 2015

THE IMPACT OF DISRUPTIVE TECHNOLOGY: THE INTERNET OF THINGS

Kyle Ebersold, The Hartford, Bryant University, kyle.ebersold@gmail.com
Richard Glass, Bryant University, rglass@bryant.edu

ABSTRACT

The Internet of Things (IoT) employs radio tags to uniquely identify and create computerized inventories of all types of objects and persons. Considered by many to be the next evolution in Internet technology, the IoT connects virtual and physical worlds in highly unified and increasingly useful ways. The world is currently poised to experience widespread use of this potentially disruptive technology, which will facilitate human-to-human (H2H), human-to-thing (H2T), and thing-to-thing (T2T), also referred to machine-to-machine (M2M) interactions. This paper provides an overview of the IoT, discusses its potential as a disruptive technology, and highlights the societal implications of the IoT.

Key Words: The Internet of Things, Internet, Disruptive Technology, RFID

INTRODUCTION

Accredited to Kevin Ashton from the Auto-ID Center at the Massachusetts Institute of Technology, the Internet of Things (IoT) takes advantage of radio-frequency identification (RFID) and sensor technology to integrate extensively with our physical environment [10]. 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, for the entire human population, 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. Control of objects in this highly integrated manner provides for effective uses in numerous applications for the home, personal use, work environments, healthcare 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 is today. 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. 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.

THE INTERNET OF THINGS

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" 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 an Internet-connected IT infrastructure [1, 2]. 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, 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. 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. Figure 1 presents a visual depiction of the anatomy of the Internet of Things.

IoT Applications

The Internet of Things has many applications in business, and as such it 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, 6]. Additionally, the household sector as the juxtaposed market to business would also see related benefits. Figure 2 lists some of the major applications of the IoT that are currently being used.

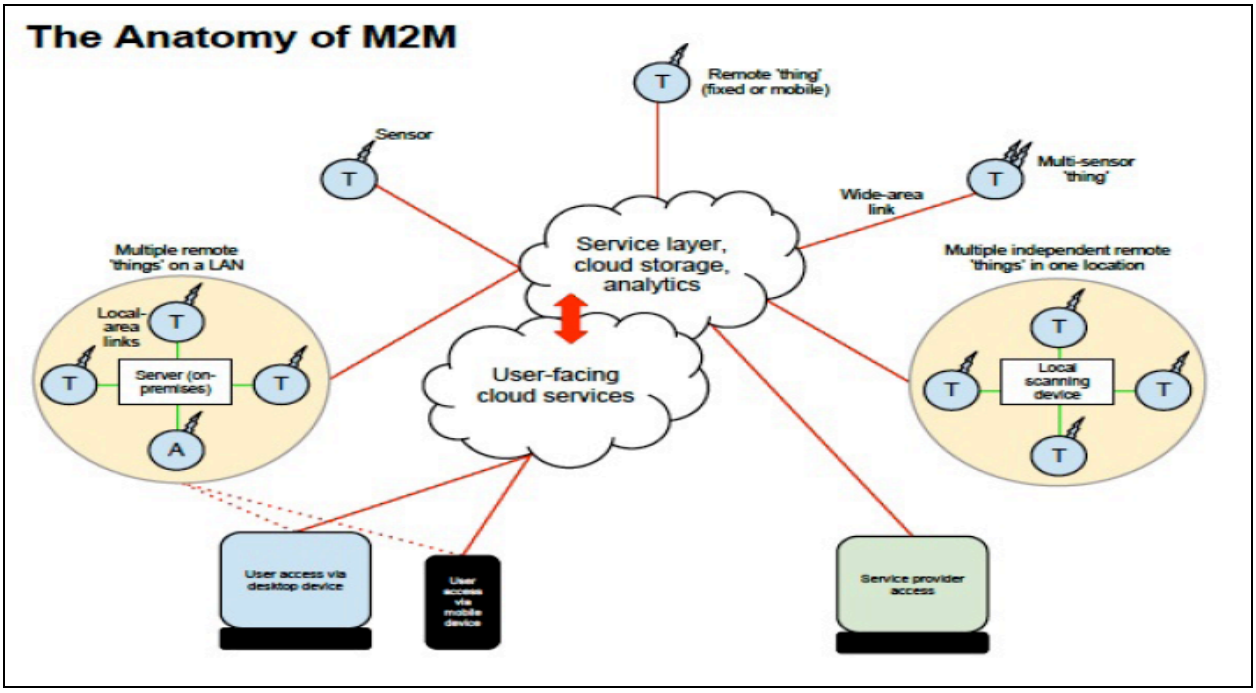

Figure 1. The Anatomy of M2M [1]

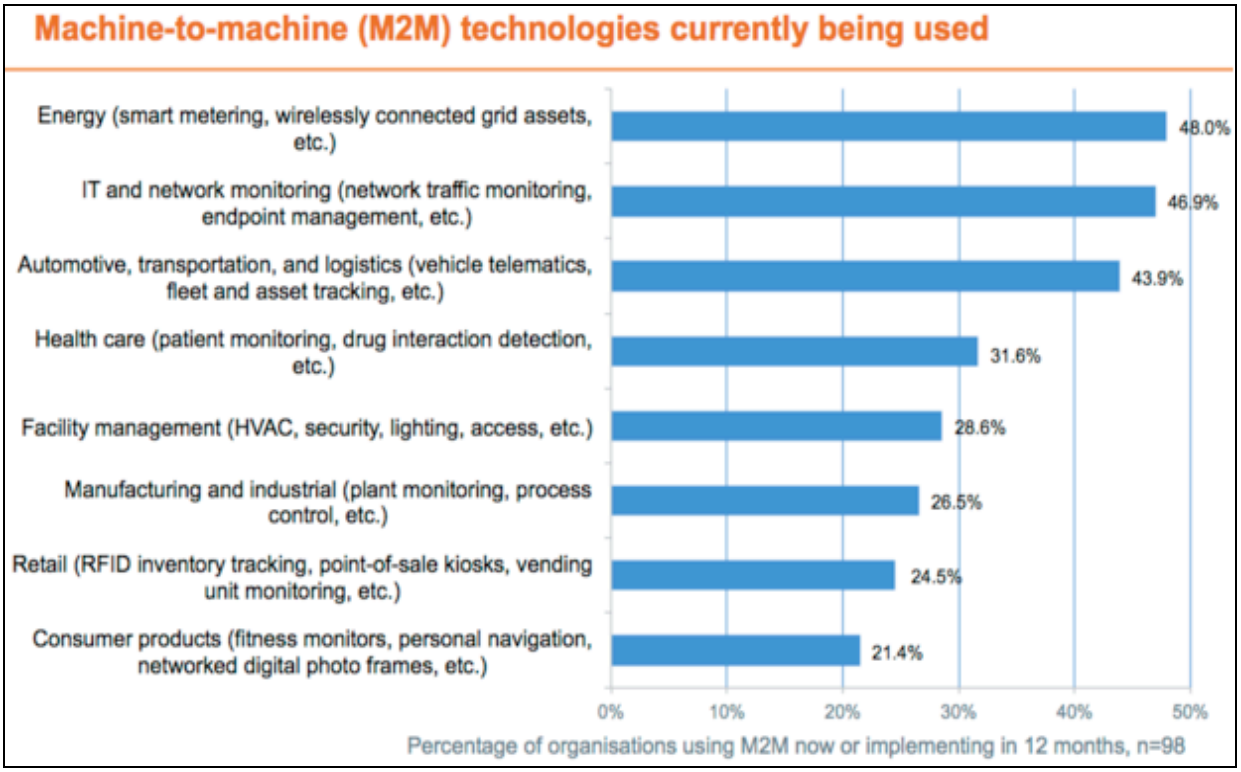

Figure 2. M2M Technologies Currently Being Used [6]

Detwiler [6] found that the key driving forces for business to adopt IoT listed in order of importance are; new business opportunities, faster response time, enhancements of existing products and services, cost savings, expanded cellular coverage, regulatory compliance, and risk mitigation. He also found that the key roadblocks to implementation of this technology in businesses in order of importance are; an immature IoT market, no clear business need, data security and privacy, implementation and maintenance costs, and complexity of implementation.

In healthcare, patients can be monitored twenty four hours a day. Sensors in mobile devices such as cell phones or in devices attached to individuals' clothing or embedded within their bodies will be able to transmit information to the Internet cloud which in turn may be electronically analyzed to identify health issues and take action which may range from automatic adjustment of devices such as pace makers, requesting ambulance assistance, and notifying monitoring agencies and physicians. Accumulated sensory information about an individual may also help in diagnosis and treatment of illness as well as aid in preventative health care activities [5]. The integration of device data collected from inpatient, outpatient, home or mobile-based applications will become a healthcare priority for the near future with as much as 40% of the global economic impact of the IoT occurring in healthcare [4]. The considerable cost savings through lowered hospital costs, insurance costs, and health care provider costs will be the driving force with the added benefit of improving the quality of care for individuals.

Mobile gadgets that are capable of acting as a sensor and provide real-time data transmission are being developed in increasing numbers. These devices are being used in applications that support individual users as well as providing social value such as aggregating the data to identify commuting patterns or traffic patterns that could be better understood, and even shaped in real time. Individuals may use real-time data to actively manage their time more flexibly by receiving traffic updates, viewing the whereabouts of friends and colleagues through geo-tagging devices, changing meeting times and locations based on real time information or to monitor air quality, weather and other urban environmental concerns. Individuals are now using IoT gadgets to inform themselves, particularly in the area of monitoring one's physical indicators for personal health. This Quantified Self movement is not solely supported by mobile devices such as smartphones, and is increasingly likely to be enabled through a variety of wearable technology, such as smart watches, bracelets, and necklaces. These are among a wider variety of new

mobile technologies that are rapidly being developed. Wearables continue 24/7 updates of a person or status— what they are up to, or what they are thinking' [7].

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, and the device could also make dish recommendations based on current contents while maintaining 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 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 via less frequent 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 performers 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].

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 now being offered by multiple vendors. Specific applications include PC/mobile phone apps such as DIRECTV Scheduler; CPI Security which allows for the remote control over home or business monitoring systems including remote arm/disarm, energy source controls, email/text notifications, and current status/recent activity views; and PlotWatt, a free service to connect 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 and EV charging.

Standards

An important consideration in the 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 was established as 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 that 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, whereas Gartner estimates there will be a total of 30 billion devices. 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 critical 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 and are 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" [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 [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 the M2M uptake in business may be rather slow until that proof surfaces.

IoT: A DISRUPTIVE TECHNOLOGY

The term, disruptive technology, was first proposed by Professor Clayton M. Christensen at the 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 on the other hand, lacks refinement, often has performance problems because it is new, appeals to a limited audience, and may not yet have a proven practical application. Disruptive technologies typically involve a high rate of technology change, broad potential scope of impact, large economic value that could be affected, and substantial potential for disruptive economic impact [8]. Examples of disruptive technology include the motor vehicle and Alexander Graham Bell's "electrical speech machine" known today as the telephone.

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. Organizations, however, face difficulty capitalizing on potential efficiencies, cost-savings, or new marketing venues offered by disruptive technologies. They also more frequently dismiss disruptive technology value only to be blindsided later when the technology matures, gains audience and market share, and threatens the market and social status quo [6].

In a McKinsey Global Institute analysis, twelve potentially disruptive technologies were evaluated based on their speed, scope, and economic value at stake. The IoT ranked highest on all three measures. With regard to speed or rate of technology improvement and diffusion, McKinsey Global Institute reported an increase of 300 percent in connected machine to machine devices in the last 5 years with as much as a 90% reduction in the price of IoT sensors. They rated the scope or number of products that could be impacted as greater than one billion across industries and more than 100 million devices connected across business sectors. The economic value that could be impacted by the IoT was projected to be more than $38 trillion USD of operating cost of key affected industries [8]. Figure 3 provides a summary of the IoT's disruptive impacts across several applications. This explosion of sensor-driven devices will potentially create a disruptive ripple effect across organizations large and small, public and private.

The McKinsey Global Institute report concludes that leaders need to focus on technologies with potential impact that is near enough at hand to be meaningfully anticipated and prepared for [8]. 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.

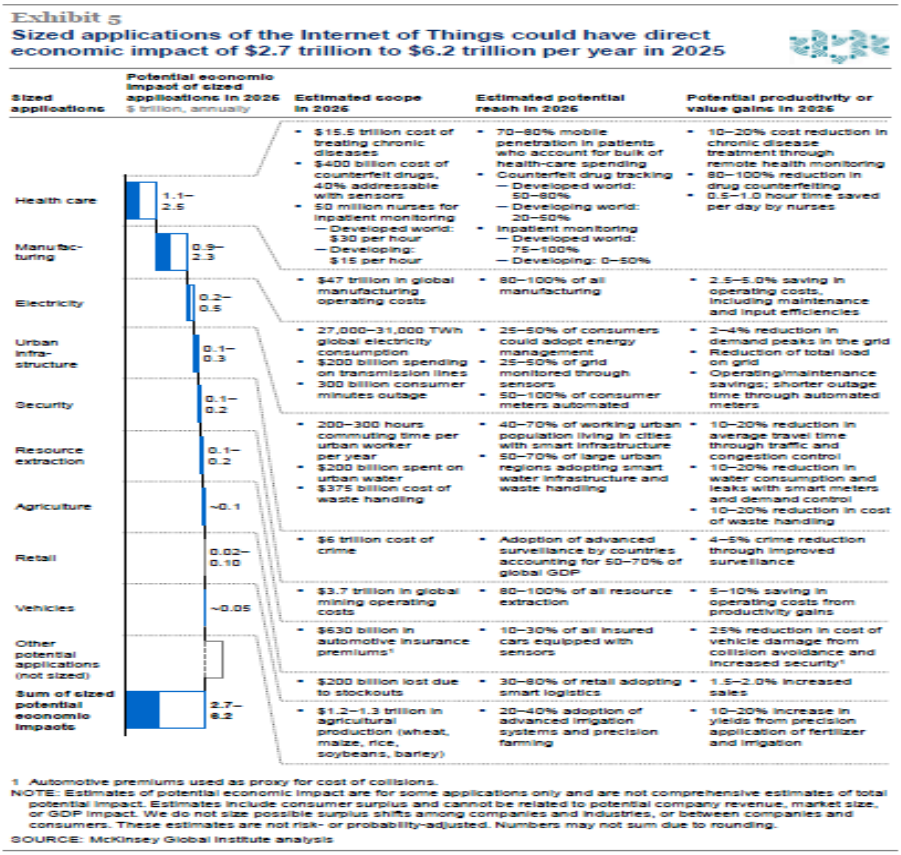

Figure 3. Application-Based Impacts of the Internet of Things [8]

IMPLICATION 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," [8]. 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 degree 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 [8].

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" [8].

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 leaders may ensure that they are in tune with the technological forces in touch with their markets and customers. Firstly, 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," [8]. In order 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," [8]. 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 [8]. The time to plan is not once new technologies begin exerting their influence, but rather right now.

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 also adequately address. 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," [8]. 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 [8]. Many entities including policymakers have the ability to effectively limit adoption or progress of technological advancements through various legislative tools and other influences. IoT technology will begin to disrupt the status quo more and more. The social and economic welfare of citizens demands rigorous evaluation in light of related technological innovations.

REFERENCES

1. The Executive's Guide to the Internet of Things. TechRepublic. CBS Interactive. (2013). Web. 22 Apr. 2014. http://www.techrepublic.com/resource-library/downloads/the-executive-s-guide-to-the-internet-of-things
2. Ajzen, J. (1988). *Attitudes, Personality and Behavior*. Open University Press, Stony Starford.
3. 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
4. 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
5. Big Data at the Center of Disruptive Technologies. Mckinsey Global Institute, May 2013. http://www.mckinsey.com/insights/business_technology/disruptive_technologies.
6. Bui, Nicola and Zorzi, Michele. Health Care Applications: A Solution Based on The Internet of Things. ISABEL' 11, Oct. 26 – 29, Barcelona Spain
7. 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
8. Dutton, W. H., Law, G., Groselj, D., Hangler, F., & Vidan, G. (2014). Mobile Communication Today and Tomorrow. *A Quello Policy Research Paper, Quello Center, Michigan State University*.
9. 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
10. Rouse, Margaret. "Disruptive Technology." What Is ? TechTarget, Aug. 2011. Web. 22 Apr. 2014. http://whatis.techtarget.com/definition/disruptive-technology
11. 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