The Internet of Things: Evolution or Revolution?

Part 1 in a Series

Forewords by:

Shawn DuBravac, Ph.D.

Chief Economist, Consumer Electronics Association (CEA); New York Times Best-Selling Author, "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate"

Carlo Ratti, Ph.D.

Director, MIT SENSEable City Lab and designer of the Future Food District at the 2015 Milan Expo

AIG

CEA
Consumer Electronics Association

Acknowledgements

The following paper has been made possible thanks to an innovative partnership with the Consumer Electronics Association (CEA)® and its Chief Economist, and *New York Times* Best-Selling Author, Dr. Shawn DuBravac.

We would also like to thank the following subject matter experts from AIG for their valuable contributions to this report:

David Bassi
Lex Baugh
Nicolas Berg
Julien Combeau
Jason Kelly
Erik Nikodem
Garin Pace
Matthew Power
and
Joe Trotti

Table of Contents

Forewords

Dr. Shawn DuBravac
is *Chief Economist at the Consumer Electronics Association* and author of the *New York Times* bestseller "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate."

It's safe to say that we are at the start of another industrial revolution. The rise of the connected objects known as the "Internet of Things" (IoT) will rival past technological marvels, such as the printing press, the steam engine, and electricity. From the developed world to the developing world, every corner of the planet will experience profound economic resurgence. Even more remarkable is the speed with which this change will happen. A decade ago there were about 500 million devices connected to the Internet. Today, there are 10 to 20 billion. In five years, there could be 40 to 50 billion.

Unlike previous industrial revolutions, however, we see this one coming. IoT is not one earth-shattering invention, like the cotton gin. Industries won't be caught unaware by a better mousetrap that renders their manufacturing systems and products obsolete. In fact, every industry and individual company stands to gain and prosper by implementing IoT objects into their business model and, as a consequence, uncover newer and better ways of doing business. Which is not to say there won't be disruption; there will be massive disruption, as new industries spawn and old models fade away. But the phenomenon of IoT is unique because it allows the forward-thinking company to prepare, adapt, and thrive in this new economic age.

The rise of IoT also means we are at the start of a new age of data. Two chief components of an "IoT object" are its ability to capture data via sensors and transmit data via the Internet. As this white paper makes clear, the declining cost of sensors since the start of the new millennium has been a main driver in the rise of IoT. In short, sensors are dirt cheap today. This has had profound implications on our ability to capture data previously out of our reach.

According to the Norwegian research organization SINTEF, 90 percent of the world's data has been generated over the past two years. Every second, over 205,000 new gigabytes are created, which is the equivalent of 150 million books. This is the amount of data created in a world with 10 to 20 billion connected and sensorized objects. The world is producing more data than ever before and, critically, we are moving it around, using it with increasing frequency. Imagine a world with 40 to 50 billion IoT objects.

How well an industry or individual company utilizes the massive influx of data unleashed by IoT objects will greatly determine its competitive advantage and future success. In some form, every organization will have to become data-centric in its approach and outlook. It will be the data that informs a supply-chain manager about inefficiencies or security holes in the supply chain; it will be the data that tells a marketer whether consumers are responding to the latest campaign; and it will be the data that gives businesses a greater insight into its processes and products than ever before.

At the center of this new universe of data will be the insurance industry, which has been using massive amounts of data to understand and mitigate risk. It's only a slight exaggeration to say that insurers invented the idea of Big Data. Naturally, as IoT objects proliferate and permeate all levels of our economy, it will be the insurers who are best placed to analyze this data and extract meaningful and actionable insights – insights that could make our world a safer and more productive place than we could ever have imagined.

Dr. Carlo Ratti
is the Director of the MIT SENSEable *City Lab and designer of the Future Food District at the 2015 Milan Expo.*

For decades we've been dazzled by new and better gadgets. Better computers; better music players; better televisions; and better phones. This trend has made technology seem like one long train of miraculous gizmos that had no antecedent in our lives. One might expect that this will continue; that the next revolutionary technology will come in yet another plastic or metal container. Yet that might not be the case.

Indeed, there is another technological revolution looming, but it's far simpler and at the same time potentially more ground-breaking than any single device. It is a data-driven revolution that could do away with many inefficiencies, hassles, dangers, and unsafe practices of modern life. The global insurance industry promises to play a vital role at the center of this technological revolution.

Call it the "Internet of Things" or "Internet of Everything", the transformation deals with the steady but inexorable rise of connected and sensorized objects – in short the online digitization of our physical world. Autonomous objects can constantly acquire, analyze, and transmit reams of data captured from their surroundings. In turn, economies, cities, businesses, and people will respond to this flow of information - opening an unprecedented array of opportunities.

The Internet of Things is giving rise to pervasive digital networks within the physical space - the networked lifeblood of the "smart city." Not just a network of municipal services, such as electricity and water, truly "smart" cities combine elements from all urban stake-holders, including citizens, government and business. And, once again, a broad spectrum of implementation models is emerging in different parts of the world.

In the United States, the general idea of smart urban space has been central to the current generation of successful start-ups. Design itself has a positive impact on revolutionizing most aspects of urban life – from commuting to energy consumption to personal health. These new initiatives are receiving eager support from venture capital funds.

In South America, Asia, and Europe, all levels of government are identifying the potential benefits of building "smart" cities, and are working to unlock significant investment in that area. Rio de Janeiro is building capacity at its "Smart Operations" center; Singapore is about to embark on an ambitious "Smart Nation" effort; the European Union's Horizon 2020 program has earmarked €15 billion in 2014-2016 – a significant commitment of resources to the idea of smart cities, especially at a time of fiscal constraints.

The future will show how the different models outlined above will play out. In the meanwhile, there is no doubt that the global insurance industry has the potential to play a major role. How will we assess risks associated with the largely uncharted territory of the Internet of Things? How can we understand challenges that could spark fundamental shifts in the responsibility for and management of risks we already know today? That's where insurers can lead – not only for the sake of their industry, but to provide guidance to other industries, governments and, above all, citizens.

Executive Summary

According to industry analysts, there are between 10 to 20 billion things connected to the Internet today. This ecosystem of connected objects forms the foundation of "Internet of Things" (IoT). Even though the technology that comprises IoT has been around for years, we're only in its very earliest stages. The number of connected objects today pales in comparison to how many will be connected in just five years. Estimates vary, but the range of connected objects by 2020 will be 40 to 50 billion, and includes everything from cups and pens to homes, cars, and industrial equipment.

IoT presents startling new opportunities for businesses, many of which remain obscure to the non-expert. The media chooses to focus its attention on the consumer side of IoT, such as the wearables market. There is little doubt that these products hold a prominent place in the IoT universe, but they remain a niche. Businesses that aren't in the consumer market might mistakenly believe that IoT has nothing to offer. Yet the implications that IoT will have on all levels of business operations, no matter the industry, will range from the mundane to the profound. Problems that have dogged businesses for centuries will dramatically diminish and, in many cases, disappear all together. Matched with other technological developments such as cloud computing, smart grids, nanotechnology and robotics, the world of IoT that we are about to enter presents one giant stride toward an economy of greater efficiency, productivity, safety, and profits.

According to a RAND Europe study, by 2020 upper estimates of IoT's annual global economic potential across all affected sectors range from $1.4 trillion (about €1.09 trillion) to $14.4 trillion (about €11.2 trillion) – or, roughly, the current GDP of the European Union. Indeed, by then IoT will not be so much an isolated IT segment as the driving force behind much of the world's economic activity. Rare will be the industry in five years that will not be changed by IoT. Even today few industries have zero to gain from using IoT objects in their processes or products. There remain, however, several trailblazing industries where IoT has become indispensable to operations. As we'll see, these industries help shine a light on the promise of IoT in the years to come.

All opportunity, however, comes with some level of risk and with IoT the risks are just as important as the rewards. From cyber breaches to shifting questions of property and products liability, businesses cannot afford to enter this new technological world unprepared. For example, every object that connects with the Internet is another entry point through which the cyber-criminals can enter a business' enterprise system. Equally dangerous, in a world where machines replace humans as the decision-makers and sensors are continually capturing data, serious questions of liability, resulting physical damage and privacy arise. It is the purpose of this white paper series to inform readers of the opportunities as well as the potential risks of IoT. Even if we can't say for certain what awaits businesses five years down the road, we can predict the issues that will become important. An IoT world is one of increasing economic complexity and the framework that industries as well as governments have adopted to foster growth and competition will not prove suitable in the long run. IoT will impact every country and economy on the planet, even in the developing world, which has historically been denied the benefits of technological progress.

As Dr. Shawn DuBravac, the chief economist at the Consumer Electronics Association in Arlington, Va., argues in his best-selling book, "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate":

> This is not what might happen if we choose this road over another. This is what will happen regardless of which road we take.

For businesses to fully realize the great potential of Internet of Things, they will need to be prepared for risks that lie ahead. The insurance industry is particularly well placed to help businesses navigate this new technology world. Indeed, many of the elements that have converged in IoT have long been used by insurers to better understand risk and improve safety. And as insurance helps businesses adapt, so too will it adapt to improve its core processes and functions.

What is the "Internet of Things"?

The term "Internet of Things" is not new. It was coined as early as 1999 by British technology pioneer Kevin Ashton, who was then working as an assistant brand manager at Procter & Gamble. In 2007, Ashton expanded on his phrase in an article:

> "If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count every thing, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling, and whether they were fresh or past their best.
>
> "We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world – without the limitations of human-entered data [i]."

Later, in 2012, Rand Europe would seek to further define the "Internet of Things" in a research report to the European Commission. The report said:

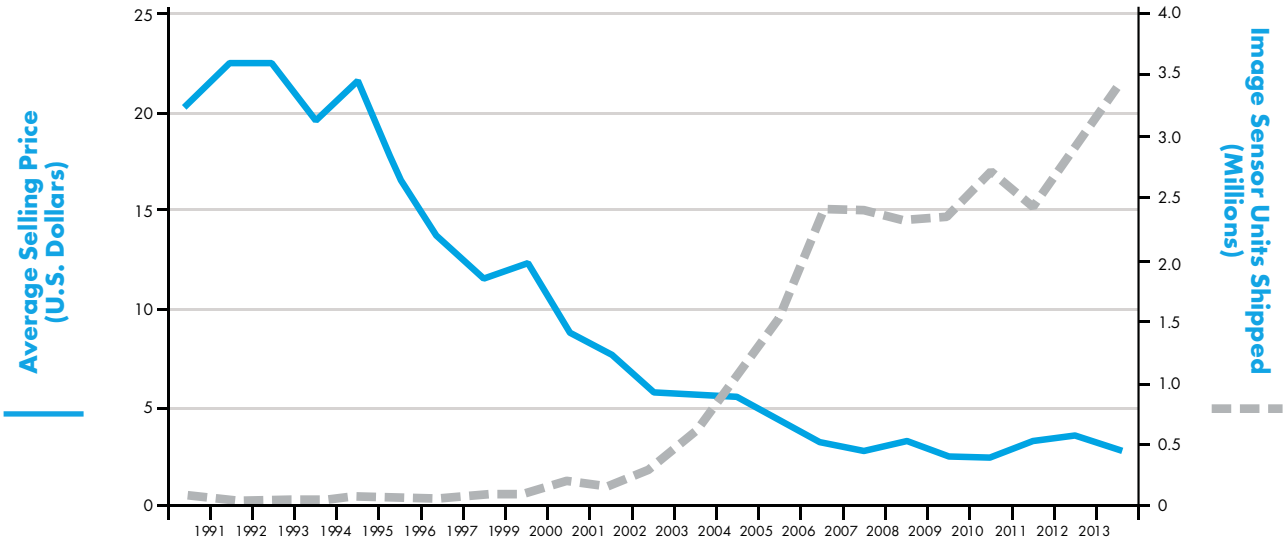
> "The Internet of Things builds out from today's internet by creating a pervasive and self-organising network of connected, identifiable and addressable physical objects enabling application development in and across key vertical sectors through the use of embedded chips, sensors, actuators and low-cost miniaturisation[ii]."

Both Ashton's and RAND's definitions are true. Yet RAND's version takes Ashton's original concept of "empowered computers" and extends it to include "physical objects." In other words, the "Internet of Things" doesn't primarily rely on computers to exist. Rather, every object, even the human body, can become a part of IoT if equipped with certain electronic parts. Those parts certainly vary depending on the function the object is to perform, but they fall into two broad categories: 1.) the object must be able to capture data, usually through sensors; and 2.) the object must be able to transmit that data to someplace else through the Internet. A sensor and a connection, therefore, are the two primary electronic "parts" of an IoT object.

Although this technology has existed for more than a decade, two developments in the last twenty years have been the primary drivers behind the emergence of IoT as a paradigm-altering phenomenon. The first is the explosive growth in mobile devices and applications and the broad availability of wireless connectivity.

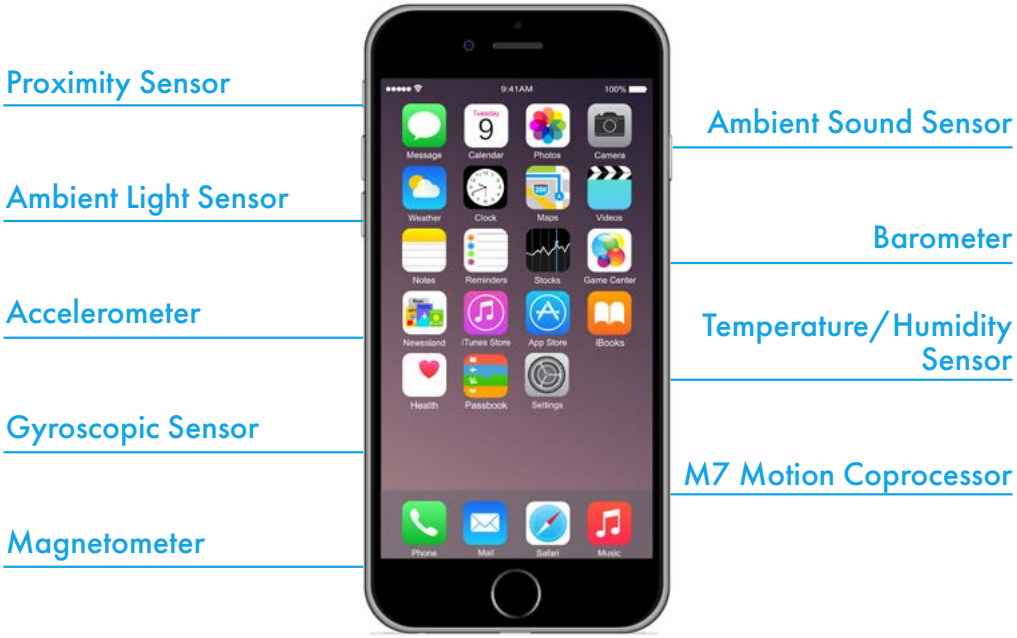
A 2011 report from Cisco noted that there were approximately 500 million devices connected to the Internet in 2003, nearly all personal computers. By dividing the number of connected devices by the world population, then at 6.3 billion, there was less than one (0.08) device for every person on the planet[iii]. By 2010, the smartphone and tablet PC market had exploded, increasing the number of connected devices to 12.5 billion, even as the world's population increased to just 6.8 billion. In just seven years, the number of connected devices per person in the world had increased by 2,250 percent, from 0.08 to 1.8. In Europe, which has one of the highest mobile phone penetrations in the world, there are 1.1 billion mobile subscriptions for a population of roughly 800 million people[iv]. That's about 1.3 mobile subscriptions per capita, or, in plainer terms, there are more mobile subscriptions in Europe than people.

The other development goes back even further than mobile technology: sensors. Yet the high cost of sensors for most of the 20th century limited their use in anything but top-of-the-line products. In the early 1990s, solid state image sensors cost $20 to $25. By the end of the decade they sold for $5. What followed was a huge increase in the digital camera market. Indeed, other sensors, such as those found in your typical smartphone, have followed a similar trajectory in terms of power and cost. In 2007, for example, accelerometers measuring a single axis of motion cost around $7. Today's accelerometers measuring six axis of motion costs less than $0.50.



Source: DuBravac, Shawn. "Digital Destiny." P. 78

Of course today's smartphone would be anything but "smart" if not for the array of sensors embedded in each device. Today's smartphones are equipped with between five and nine sensors, depending on the model. These include:



Fifteen years ago the inclusion of one, much less nine, of these sensors would raise the cost of a product beyond the means of the average consumer. Today, the cost of all these sensors adds up to under $5.00, with the cheapest sensors costing as little as $0.07[v].

Yet sensors do more than enable neat features on our mobile phones. In fact, they are the critical ingredient that "turns on" IoT. By continually capturing data on its surroundings, a sensor replaces the human as the primary way a computer receives data. And because sensors can capture data at speeds and in quantities that no human could ever match, they have led to the phenomenon called Big Data – or the acquisition and analysis of extremely large data sets.

What is this data? It's everything and anything that surrounds us. More practically, the data that today's sensors are able to acquire – that humans cannot – are revolutionizing the economy and business processes. Indeed, car manufacturers all over the world are using sensors not just in their cars, but also in their manufacturing plants, where they assist autonomous machines as well as improve safety among auto workers.

Other factors that have contributed to IoT, particularly in a business and industrial setting, include cost-effective cloud storage and the rise of data analytics which allow organizations to manage and extract information from massive amounts of data[vi]. But we're never too far from the principle players. It is a sensor which captures the data and mobile connectivity which transmits the data to another device or to the cloud.

We must remember that IoT is not simply one, easily definable phenomenon. There are a variety of segments and markets that comprise IoT. For the consumer, IoT means wearable technology and "smart" appliances, such as thermostats and televisions. In the industrial sector, IoT means autonomous machines and sensorized equipment. In the business space, IoT means Big Data and marketing analytics. In short, from the manufacturing to consumer products, IoT is as varied as the global economy itself.

The question then becomes: How can businesses utilize these connected objects to enhance their processes, increase productivity, reduce costs, and avoid risks?

A New Economic Age

To appreciate the opportunities for businesses inherent in IoT, let's first understand its macroeconomic impact. In a policy paper for the European Commission, RAND Europe put upper estimates of the economic potential of IoT between $1.4 trillion per year (about €1.09 trillion) to $14.4 trillion (about €11.2 trillion) across all sectors globally[vii]. Furthermore, the sale of connected devices and services will come to about $2.5 trillion in 2020, while the accumulated investments indicated by the connection of billions of connected devices will reach at least €2 trillion at present prices. For example, the RAND study notes that China has already earmarked €625m ($775m) for IoT investment[viii].

To be sure, in five years there is no industry that IoT won't impact directly. The pace of adoption matched with consumer expectations and demands will quickly turn any non-IoT industry, to say nothing of an individual company, into a museum relic. That said, many industries have time to understand IoT and where it might improve their long-term strategic goals. As the first installment in this series, this white paper intends to provide readers with current examples of how certain industries have begun to use IoT. Our hope is that readers will be able to start implementing a strategy for their own business based on the examples we provide below. Because IoT has uses that span the business spectrum, we've divided how each industry is using IoT into four categories:

Safety, Efficiency,
Data-Driven Decision Making,
and Infrastructure.

AUTOMOTIVE

Safety: In 2010, the World Health Organization reported that 1.24 million people worldwide died as a result of a motor-vehicle accident[ix]. Every year, approximately 30,000 people are killed in motor-vehicle accidents in Europe[x]. It's roughly the same in the United States. In Asia, the problem is far worse. In China and India alone, more than 400,000 people die in a motor-vehicle accident every year[xi]. IoT technology, particularly the rise of safety-focused sensors on automobiles, promises to drastically reduce the global death rate from motor-vehicle accidents. Because a vast majority of motor-vehicle accidents are the result of human error, replacing the human decision-making component in driving is the object of autonomous vehicles.

In May 2015, the German-owned, U.S.-based Daimler Trucks North America announced it was ready to test its driverless Freightliner Inspiration Truck on Nevada roadways[xii]. But driverless cars, such as companies like Google[xiii] and Tesla[xiv] are developing, are slowly coming on line. Many of these come in the form of safety sensors that give a motorist a 360-degree view of their car; while others work autonomously, protecting the car without direct driver action. Auto companies also use the data these sensors acquire to help them produce safer, more efficient cars. While these data-collecting devices raise certain privacy concerns, they're the next step in the automobile evolution.

BANKING

Efficiency: The financial sector has helped pioneer the use of mobile technology to make banking easier for the average consumer. One obvious example where IoT and the banking industry intersect is with ATMs, which can be equipped with sensing technology. A user with the right biometric identifiers might one day withdraw money from a sensorized ATM without ever taking out his debit card. Looking ahead, IoT promises to connect a consumer's financial activities with other aspects of his or her life. One example is connecting a user's health monitor with his financial portfolio. As Deloitte has noted, a health crisis, captured by the monitor, could signal the user's bank to automatically rebalance his portfolio to minimize his financial exposure[xv].

In a 2014 report on the "Bank of Things," Accenture noted: "The Bank of Things will anticipate customers' needs and respond to their changing circumstances, offering timely, relevant solutions that assist them to achieve their goals. It will remain a trusted advisor, facilitator and value aggregator for its customers — yet it will do so with an almost intimate understanding of each customer's needs and preferences."[xvi]

MARINE

Safety: Much like the rest of the transportation industry, maritime shipping companies for decades have equipped their fleets with a variety of sensors to monitor critical vessel systems, weather and sea conditions, and cargo. IoT technology now allows these sensors to acquire data that can then be analyzed to improve voyage optimization, safety, and stowage processes.

In one example, open source software uses a ship's sensors to provide real-time vessel movement information to other ships and land-based sea traffic coordination centers. The IoT software "supports collaborative decision making amongst the key stakeholders involved to achieve safer, more efficient, and environmentally friendly maritime operations," as one expert explained[xvii].

Data-Driven Decision Making: At International CES 2015, Swedish-based Ericsson unveiled an enhanced IoT solution for maritime shipping. The cloud-based platform would connect ships at sea with "shore-based operations, maintenance service providers, customer support centers, fleet/transportation partners, port operations and authorities." The solution would allow both sea- and land-based operators to monitor fuel consumption, engine performance, weather, traffic and navigation for improved voyage optimization, track specific cargo location and condition, and through improved communications, entertainment options and telemedicine, even enhance the wellbeing of the ship's crew[xviii].

PROPERTY (REAL ESTATE)

Efficiency: At the property level, there are already "smart" objects, like thermostats and other appliances, that help homeowners improve energy efficiency and lower utility costs. We can expect these products to proliferate as the home becomes more and more "connected." But the real value of IoT in homes will come when these connected appliances and other household objects communicate with each other. So, for example, a home's smart thermostat will know the outside temperature and relay this data to the home's closet system, which will suggest appropriate outfits for the day. Another example is when a home's system, let's pick the closet again, syncs with a user's calendar. The closet then "knows" if the user has a meeting that day and selects the appropriate clothing.

Data-Driven Decision Making: In the real estate industry, an IoT-equipped home can all but take the place of a human agent. It can list itself on the right real-estate listings and schedule showings because it will "know" when the owners will be out of the house[xix]. Some brokerage firms are already experimenting with Apple's iBeacon[xx] technology and "For Sale" signs. The concept is that a prospective homebuyer who passes a house for sale will receive a message on their smartphone from the iBeacon giving instant details on the house. Inside the house, iBeacon technology can be used to provide prospective buyers with floor plans, previous owner video testimonials, and even renovation opportunities – likely in partnership with a home-improvement and hardware store[xxi].

Infrastructure: Floods, fires, structural decay – these are the risks any business must accept. However, IoT technology, particularly sensors embedded in specific risk areas, can help diminish, and in some cases eliminate, these enduring problems. For example, electrical systems can be equipped with sensors that monitor the flow of electricity through a building. When a wire or a connection has failed, or is about to fail, raising the probability of fire, the sensors can immediately warn technicians. Real estate companies can use IoT sensors in their properties to monitor a variety of risk-related incidents, including the presence of dangerous gas, termite infestations, HVAC/boiler malfunction, and general wear-and-tear. Even when a particular structure seems to be in top condition, analysts can pore over the massive amount of data captured by these embedded sensors to identify clues to future problems.

ENERGY

Efficiency: The energy industry already reaps huge rewards from IoT technology. At the consumer level, users are able to use advanced appliances and "smart" devices to cut energy usage and costs. Businesses as well can utilize these technologies, but at a much more advanced level. An office building with multiple tenants, for example, can capture and monitor energy usages from each floor. Analyzing the data, the building can identify areas of wasteful energy use and cut costs.

Meanwhile, the energy industry has long been at the forefront of IoT technology, primarily with utility companies innovating ways to read energy usage of commercial, industrial, and residential customers remotely. Indeed, according to Ericsson, the number of connected devices being managed by utility companies globally is expected to grow from 485 million in 2013 to 1.53 billion in 2020. In fact, the utility industry is the second largest source of "machine-to-machine" service provider revenue, behind the automotive and transport industries. "These devices can range from meters, grid sensors and actuators to energy boxes and electrical appliances. They are used for applications such as grid monitoring and control, metering, asset management and tracking, and field force communication," says Ericsson[xxii].

AEROSPACE

Safety: "Fly-by-wire" systems have been a staple of the aerospace industry for decades. Put simply, "fly-by-wire" allows a pilot to focus his attention on monitoring the plane while sensors and automated systems take care of the rest. Indeed," fly-by-wire" is becoming so advanced that in many ways airplanes are virtually autonomous vehicles. For example, when Capt. Chesley B. "Sully" Sullenberger made an emergency landing in the Hudson River moments after taking off from New York's LaGuardia Airport, he was flying an Airbus A320, whose earlier models pioneered the use of digital "fly-by-wire" systems. It's no disservice to Capt. Sullenberger to say that the "Miracle on the Hudson" could have ended in tragedy if not for the highly-developed sensors on the aircraft that allowed him to focus on safely landing the plane in the river[xxiii].

Efficiency: On the ground, aerospace companies are employing IoT technology to improve the maintenance and safety measures. For example, General Electric's aircraft engine maintenance business uses onboard sensors in jet engines to capture real-time data on engine performance. The volume of data this process produces allows GE to boost engine efficiency, cut fuel costs, and shorten travel times[xxiv].

HEALTH CARE

Data-Driven Decision Making: There is really no realm of health care that does not or will not employ IoT technology. At the patient level, IoT-enabled wearables allow doctors to capture health data that would be otherwise unknown. Yearly physicals could become obsolete because doctors already have copious amounts of individual patient data that let them know if an in-person check-up is warranted. Likewise, patients with troubling health signs that might not cause symptoms would be detected by the physician before they lead to more severe problems. Clinicians can use this data to not only better understand the health of the individual patient, but also create detailed data sets of patient subgroups, with the objective of treating and preventing humanity's most ancient diseases.

Meanwhile, hospitals, which have always produced and stored tremendous amounts of data, can use IoT technology to find actionable intelligence in the data they collect. For example, many hospitals intentionally overstock inventories to prevent shortages on critical supplies. IoT-enabled scanners give hospital administrators visibility into their stock and know the moment that shortages occur. Also, IoT devices can drastically improve the treatment in hospitals, particularly in emergency situations. A paramedic can use IoT devices to take a patient's vital signs and other statistics, which are then instantly relayed to the ER. Once the patient arrives, no longer will doctors waste valuable time in understanding a patient's condition because they will already know.

MANUFACTURING

Safety: Furthermore, IoT promises to drastically reduce the rate of workplace-related injuries and deaths. Globally, according to the International Labour Organization, 2.3 million people die every year from work-related accidents and diseases[xxv]. According to the European Commission, every year more than three million workers are the victims of serious accidents while on the job and 4,000 die in workplace accidents[xxvi]. IoT can help keep employees safe, especially those working alone in hazardous areas such as construction sites. For example, wearable technology can be equipped with embedded sensors to determine when a worker might be dangerously exerting himself or performing an unsafe maneuver. The sensors can also monitor hazardous environmental conditions, such as extreme temperatures and the presence of toxic substances. Also, behavioral data collected from these wearable sensors can help safety managers understand when a worker is likely to have an accident. This predictive element in IoT – while in many ways still theoretical – is one of its most exciting (as well as potentially exploitative) features.

Data-Driven Decision Making: Companies can also utilize IoT products to ensure the integrity, quality, safety, and security of components in their complex supply chains. Gartner, Inc., an IT research and advisory firm, estimates that "a 30-fold increase in Internet-connected physical devices by 2020 will significantly alter supply chain leader information access and cyber-risk exposure."[xxvii] IoT devices embedded throughout the supply-chain will give managers a deeper insight into their processes than ever before. From in-transit visibility to depot security, IoT objects promise to revolutionize how companies design, secure, and maintain their sensitive supply chains.

FOOD

Efficiency: Delivery companies already offer consumers the ability to track their packaged orders at each processing station, but the technology is far more useful when it's applied to businesses. IoT sensors embedded in the right time and place can help a business track assets in real time. The collected data can allow organizations to identify inefficiencies and bottlenecks in their supply chains. Just as important, sensors in storage facilities, such as on a freezer truck, can warn a company when the cooling mechanism has failed or is about to fail. This takes the onus of monitoring off the driver, who might not check the goods until several hours after the cooling unit has failed, and gives organizations the ability to salvage precious cargo before spoilage.

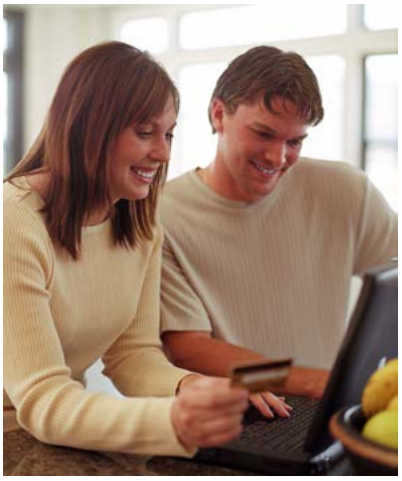
In agriculture, farmers can use IoT technology, embedded in their fields, to monitor critical information like water usage. For example, a sensor can tell a farmer where there are gaps in his sprinkler system or whether he's using too much water on a particular acreage. Particularly when applied to the developing world, the advances IoT will have on food production and distribution promise to be ground-breaking.

IoT Risks

In many ways, IoT's possibilities are limited only by our imaginations. Particularly when we consider all the data that goes unrecorded, all the bits of information that slip through our fingers, and how IoT will allow us to finally capture this data and use it in a way that has eluded humanity for years, it's easy to ignore the dark side of the new IoT world. But businesses cannot afford to invest in their IoT systems without first understanding the major risks inherent in any system that is connected to the Internet. From the day we turned on the first computer, we have known that our reliance on technology can lead to disruption, big and small. This is not to scare companies away from embracing IoT; by far, the opportunities outweigh the risks. Yet every company must understand that for every problem IoT solves, there is another problem it creates. Here are four of the biggest risks that come with IoT:

PRIVACY

When the world's billions of sensors are constantly acquiring data on their surroundings, which includes humans, then privacy concerns are paramount in an IoT world. Most of the developed world has attempted to protect consumers from illegal use of confidential information, but in many cases the laws are not adequate to meet the tremendous number of new ways personal information is being captured and used. The EU's recent attempt to update copyright law (see below) is a symptom of the outmoded nature of many of the developed world's laws.



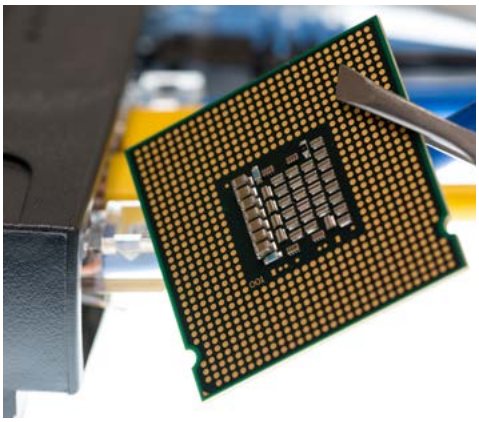
At an earlier stage of the Internet, consumers became familiar, if not entirely comfortable, with tracking software, otherwise known as cookies. Because there was no specific law restricting a web site's use of cookies to track a user's browsing behavior, many companies simply adopted the practice without much forethought on user concerns. In fact, it was the browsers that responded to consumer anxiety with tools to restrict the use of cookies and eliminate them after a browsing session. Legislation in the EU now regulates how cookies are used and what type of data they are allowed to collect on users[xxviii], but with the rise of mobile technology, which doesn't need cookies to track user behavior, many of these laws are swiftly becoming outdated and inadequate in an IoT world.

Likewise, the United States also relies on older regulatory models for new IoT devices and systems. But there is no single federal law that governs the collection and use of personal data. Rather, the U.S. relies on a patchwork of existing federal and state laws to protect consumer privacy. Public outcry at the federal government, particularly the National Security Agency, for "data-mining" activities related to law-enforcement and counter-terrorism presage the public policy debates to come.

The U.S. Federal Trade Commission released a report in January 2015 that surveyed the state of IoT in the U.S. and suggested "best practices" for companies to follow when it comes to consumer data and security. The FTC report, however, continues the federal government "light touch" when it comes to Internet, and thus IoT, regulation. For instance, the report concludes "that any Internet of Things-specific legislation would be premature at this point in time given the rapidly evolving nature of the technology. The report, however, reiterates the Commission's repeated call for strong data security and breach notification legislation."[xxix]

Privacy concerns extend to the workplace as well. There are lots of programs on the market that enable an employer to track worker behavior, usually via the worker's PC. But IoT allows employers to embed sensors in virtually any corner of the office to monitor employee habits. For example, a former sales executive in California has filed a lawsuit against her employer, alleging she was forced to download a tracking app to her smartphone which the employer used to monitor her whereabouts both during and after work hours[xxx]. IoT's ability to track and capture human action raises multiple ethical questions that haven't as yet been fully answered, such as:

- Can a worker be punished because of data collected from an IoT object?
- Must an employer inform his workforce about sensors tracking their behavior?



CYBERSECURITY

Cyber breaches are a major threat to businesses today. According to one estimate, cyber crime costs businesses $400 billion every year[xxxi]. What's most troubling from an IoT perspective is that the cyber-criminals are breaching ostensibly secure systems with multiple layers of protection in place. The complexity of ensuring the security of IoT devices is an area of improvement for business, especially in preparation for the day the "IoT ecosystem" comes to life where billions of objects are connected to the Internet and each other.

We must remember that any device with an Internet connection is a potential gateway for a hacker. For example, in 2014 a hacker was able to break into a baby monitor to harass a two-year-old girl. Follow-up research on the product, which was produced by the China-based company Focsam, discovered that 40,000 out of 46,000 devices had not been updated with a security measure that would have prevented the breach.[xxxii]

We must also remember that the more we automate and connect certain systems, particularly industrial systems, the more open those systems are to hacking. A city that builds a smartgrid for electricity might realize great cost savings in the way the system streamlines troubleshooting. At the same time, the very system also gives a potential hacker an easy way to shut down an entire city's electrical supply from his computer.

In yet another example, the U.S. Government Accountability Office issued a report in April 2015 that discussed the threats that come with the increased interconnectedness between airplanes and ground systems. "This interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems," the report warned[xxxiii]. In other words, a hacker-terrorist could use the system to gain control of the aircraft.

Because of the networked nature of IoT – i.e., that each connected object uses data from other connected objects – there is also the risk that a malfunction could lead to catastrophic system failure. A malfunctioning object potentially could feed incorrect data to another device that's functioning normally. Yet as the bad data inches its way up the system, it begins to infect more and more systems. If we consider a natural disaster, such as flooding, malfunctioning sensors might monitor the integrity of dams and levees and could lead to massive property damage or even loss of life.

Examples like these underscore the new risks many businesses will face when it comes to IoT cybersecurity. While we can expect that the manufacturers of these devices will improve their security measures in time, the sheer number of connected things is growing exponentially.

LIABILITY

When it comes to autonomous vehicles, like driverless cars, we are faced with an obvious ethical dilemma: In the seconds before an accident, should an autonomous vehicle do anything it can to protect the passengers, even if it means harming other motorists or pedestrians? When humans are behind the wheel, collateral damage, as terrible as it is, doesn't pose much of an ethical problem. A human being in danger can't be faulted when its survival instincts make it swerve its car into a pedestrian. But when machines are the decision-makers, does a pedestrian harmed in accident have a case against the car manufacturer? Does a driver have a case against a car manufacturer following an accident in which he or she was injured? As European Commission report on the ethical dilemmas inherent in IoT technology stated, "People are not used to objects having an identity or acting on their own, especially if they act in unexpected ways."[xxxiv]

Other questions of liability emerge when we consider data ownership. With billions of devices collecting data, the lines get blurred on who is responsible for what data. IoT objects function autonomously and in conjunction with multiple other objects. Data is quickly shared, processed, reshared, and reprocessed before it might be seen by human eyes. In other words, it's too simple to associate one device with one piece of data, since so much of IoT's potential lies in the seamless transfer of this data between objects. For instance, an IoT heart monitor won't just monitor a patient's heart looking for warning signs of an impending heart attack. It might also access data from another object that tracks the patient's fitness routine, which in turn takes data from a device that monitors food intake. If the patient has a heart attack, who's responsible?

IoT devices also raise troubling questions when it comes to device malfunction. Sensors can be embedded in critical infrastructure like dams, bridges, and roadways to monitor structural integrity as well as environmental conditions that could undermine structural integrity. A road near a flood area could be embedded with sensors that know the moment rainfall has exceeded a point that gives engineers advanced warning of flooding. Indeed, protecting infrastructure is one of the most exciting aspects of IoT. Yet when we turn more and more of our critical infrastructure and security systems over to IoT objects, we run the risk of a catastrophe if and when those objects fail.

We can apply this to the private sector as well. To cite a non-lethal example, in April 2015 several American Airlines flights were delayed when a software malfunction rendered pilots' tablets, which they use for navigational purposes, useless[xxxv]. Although the malfunction was easily fixed with a software update, these examples show just how exposed we already are because of our connected devices. When they fail, will we be prepared?

The State of Play of IoT in Europe, the United States and Asia

EUROPE

With its high mobile penetration rates, Europe is uniquely suited to capitalize on the coming IoT revolution. But despite the inevitability of IoT, there remain obstacles for individual economies to overcome to realize the full potential of IoT. One obstacle is simple competition. For example, in March 2015, during a conference in Brussels of the European Commission, representatives of European heavy industry, car manufacturers, appliance makers, telecoms, and legislators met to discuss how to improve the continent's competiveness in IoT, particularly when U.S. companies, like Apple and Google, seem to be making the most headway.

The result of the conference was a new EU-backed alliance of European industry, including top companies such as Phillips, Bosch, Orange, Alcatel, Nokia, Siemens, Telefonica and Volvo, to spur IoT innovation. As Anne Lauvergeon, chairwoman of French networking startup Sigfox and a board member of the new IoT alliance, said: "Creating an ecosystem for IoT innovation is fundamental to face international competition."[xxxvi]

At the same time, the EU is working toward a single digital market by revisiting existing telecom laws. The goal of the new legislation is to remove impediments to data transfers "by breaking down national silos in areas like e-commerce and copyright law," according to the Wall Street Journal.[xxxvii] This need to overhaul the regulatory environment speaks to the changing nature of the new IoT economy, where the ability to quickly and easily transfer and exchange massive amounts of data will become a hallmark of a region's success.

Beyond updating legislation, the new IoT economy will also require significant investment in technology infrastructure. In March 2015, the European Investment Bank (EIB) held a conference in Berlin on the topic "Momentum for Europe—Innovation and Competitiveness."[xxxviii] During his keynote address, Jeremy Rifkin, President of the Foundation on Economic Trends and a policy advisor to France, Germany, and the EU, spoke of how the scale-up and build-out of IoT will help a "Digital Europe" enter a "Third Industrial Revolution."[xxxix]

However, Rifkin noted that European investment in "outmoded" technology platforms totaled $741 billion in 2012. If 25 percent of these funds were redirected in every region of the European Union toward IoT infrastructure, the full benefits of "Digital Europe" could be realized by 2040.[xl] That is to say, in one expert's opinion, too many euros are going toward buttressing an older economic model at the expense of the future.

UNITED STATES

In 2014, venture capitalists invested nearly $11.9 billion in Internet-specific companies, the highest since 2000 and the cusp of the "Dot Com" bubble.[xli] While not all of this capital went into IoT-specific devices, the excitement surrounding IoT in the United States is certainly at an all-time high. In March 2015, for example, IBM announced it would invest $3 billion in a new "Internet-of-Things division."[xlii]

Indeed, the private sector is trying to keep the U.S. at the forefront of the IoT revolution. In 2014, software and tech giants, including AT&T, Cisco, General Electric, IBM and Intel, announced the Industrial Internet Consortium to create engineering standards surrounding IoT objects. The White House and other government bodies are also involved in the non-binding body.[xliii] Even though the FTC has suggested that the federal government avoid IoT regulation for now, government agencies have started to work alongside private enterprises to produce public applications for IoT technology. For instance, in 2014, representatives from the Defense Advanced Research Projects Agency (DARPA), the Transportation Department and the Veterans Health Administration met in Washington to discuss public-sector IoT technology.[xliv]

However, the United States lags behind other developed nations, particularly Asia, when it comes to broadband access and speeds. According to the digital traffic company Akamai, the U.S. ranks 14th in broadband speed.[xlv] While overall connectivity in the U.S. is one of the highest in the world, aging infrastructure, local regulatory hurdles, and the high-cost of broadband access limit how far the U.S. can lead on IoT adoption and innovation.

ASIA

According to RAND Europe, China is putting considerable resources behind IoT investment. In 2012, it earmarked €625m ($775m) for IoT investment while China's Ministry of Information and Technology set up a fund of $775m to support IoT build over the next five years. These investments will go toward the building of ten IoT industrial parks in more than 100 core enterprises across the country by 2015. Indeed, more than any other nation, China's investment in IoT infrastructure over the past few years has outpaced its European and U.S. competition[xlvi].

While China is certainly the biggest player in the IoT market, the entire Asia Pacific region stands to gain tremendously from recent IoT technology. The research firm IDC estimates that the Internet of Things market size in Asia Pacific excluding Japan will grow from $250 billion in 2013 to $583 billion in 2020. Meanwhile, the number of things connected to the Internet in the Asia Pacific market will grow from 2.59 billion in 2013 to 8.98 billion in 2020.[xlvii]

Although IDC forecasts that by 2020 one out of every five objects connected to the Internet will be in China, it warns that market size is not the same as market maturity. "While the market opportunity in China dwarfs the other leading countries like South Korea, India, Indonesia and Australia in terms of dollar value, that doesn't mean it is the most mature," said Charles Reed Anderson, Associate VP, Head of Mobility and Internet of Things at IDC Asia/Pacific Anderson. "To assess the maturity of a market, we compare the total number of things connected to the overall population to get a connections per capita figure. Based on this calculation, we discovered the top three most mature markets were South Korea, Australia and New Zealand, with China coming in sixth out of the 13 APeJ Countries."[xlviii]

Nevertheless, as the manufacturing hub of the world, Asia stands to reap tremendous gains from an IoT economy.

Conclusion

It is not an overstatement to say that IoT will usher in a new economic era for the entire globe. The promises IoT holds are not simply improvements over existing processes and economic models; rather, they are transformational in scope. The IoT economy will revolutionize the way businesses produce, function, and perform. And the change is happening faster than any previous industrial revolution.

At the same time, IoT will present significant challenges across all sectors and for all industries. As it solves problems that have plagued businesses for decades, if not centuries, it will also create entirely new dilemmas, both procedural and ethical. Concerns over privacy, cybersecurity, and property and products liability will quickly become just as robust as the opportunities IoT presents. While businesses must begin to implement IoT technology if they hope to survive over the long term, they also must implement strategies that account for the many risks associated with IoT.

In the next installment in this series, we will further investigate these risks and provide practical steps for businesses to avoid or minimize them. We will also introduce how the insurance industry will be poised to help businesses navigate this new IoT world. In many ways, the insurance industry stands to gain the most from embedded sensors that produce massive amounts of data, which will provide deeper insights into minimizing risks to customers. Long at the center of data-driven analytics and risk mitigation, the insurance industry will be ready to help maximize businesses' IoT opportunities and minimize their exposure.

Citations

i http://www.rfidjournal.com/articles/view?4986

ii RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, 2012

iii CISCO: The Internet of Things How the Next Evolution of the Internet Is Changing Everything, 2011

iv http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-europe.pdf

v Dubravac, Shawn. "Digital Destiny." P. 68

vi HBR-Verizon INTERNET OF THINGS: SCIENCE FICTION OR BUSINESS FACT?, 2014

vii RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, 2012 p. 14

viii ibid

ix http://www.who.int/gho/road_safety/mortality/en/

x http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm

xi http://morth.nic.in/writereaddata/mainlinkFile/File1465.pdf and http://www.chinadaily.com.cn/china/2011-01/07/content_11808453.htm

xii http://www.forbes.com/sites/dougnewcomb/2015/05/08/daimler-autonomous-truck-has-huge-commercial-implications/

xiii © 2012 Google Inc. All rights reserved. Google and the Google Logo are registered trademarks of Google Inc.

xiv Copyright 2002-2015 Tesla Motors, Inc. All Rights Reserved.

xv http://www2.deloitte.com/us/en/pages/finance/articles/internet-of-things-financial-services-industry.html

xvi http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Bank-of-Things.pdf

xvii http://osdelivers.blackducksoftware.com/2015/02/11/industrial-internet-of-things-in-the-maritime-industry/

xviii http://www.rcrwireless.com/20150106/featured/ericsson-maritime-platform-targets-shipping-connectivity-tag2

xix http://www.inman.com/2014/07/08/internet-of-things-could-be-most-disruptive-to-real-estate/

xx iBeacon is a trademark of Apple Inc., registered in the U.S. and other countries.

xxi http://realtormag.realtor.org/technology/feature/article/2015/03/real-estate-and-internet-things

xxii http://www.ericsson.com/res/docs/2014/gtwp-op-transforming-industries-aw-print.pdf p. 4

xxiii http://www.cnn.com/2009/OPINION/11/18/langewiesche.miracle.hudson.flight/index.html?iref=24hours

xxiv http://www.forbes.com/sites/ptc/2014/06/23/will-the-internet-of-things-revolutionize-the-aircraft-industry/

[xxv] http://www.ilo.org/global/topics/safety-and-health-at-work/lang--en/index.htm

[xxvi] http://www.euractiv.com/sections/social-europe-jobs/commission-publishes-health-and-safety-strategy-eu-workers-302665

[xxvii] http://www.gartner.com/newsroom/id/2688717

[xxviii] http://ec.europa.eu/ipg/basics/legal/data_protection/index_en.htm

[xxix] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

[xxx] http://www.techweekeurope.co.uk/mobility/lawsuit-tracking-app-168043

[xxxi] http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

[xxxii] http://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/

[xxxiii] http://www.gao.gov/products/GAO-15-370

[xxxiv] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752

[xxxv] http://www.nytimes.com/2015/04/30/business/several-american-airlines-flights-are-delayed-by-an-app-malfunction.html?_r=0

[xxxvi] http://blogs.wsj.com/digits/2015/03/25/europe-wants-to-bring-its-industry-online-before-google-apple-make-it-obsolete/

[xxxvii] http://www.wsj.com/articles/eu-considers-new-telecom-rules-to-level-the-playing-field-1427295277

[xxxviii] http://www.eib.org/infocentre/events/all/momentum-for-europe.htm

[xxxix] http://www.automatedtrader.net/headlines/153295/digital-europe-the-rise-of-the-internet-of-things-and-the--transition-to-a-third-industrial-revolution

[xl] ibid

[xli] http://nvca.org/pressreleases/annual-venture-capital-investment-tops-48-billion-2014-reaching-highest-level-decade-according-moneytree-report/

[xlii] http://www.theglobeandmail.com/report-on-business/international-business/us-business/ibm-to-invest-3-billion-in-new-internet-of-things-unit/article23722378/

[xliii] http://bits.blogs.nytimes.com/2014/03/27/consortium-wants-standards-for-internet-of-things/?_php=true&_type=blogs&_r=1

[xliv] http://www.washingtonpost.com/business/on-it/dot-va-reps-discuss-how-the-federal-government-could-use-internet-of-things/2014/08/06/d9ac6410-1d84-11e4-ae54-0cfe1f974f8a_story.html

[xlv] http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf?WT.mc_id=soti_Q114

[xlvi] HBR-Verizon INTERNET OF THINGS: SCIENCE FICTION OR BUSINESS FACT?, 2014 p. 7

[xlvii] http://www.idc.com/getdoc.jsp?containerId=prHK25553415

[xlviii] ibid

The Consumer Electronics Association (CEA) is the technology trade association representing the $286 billion U.S. consumer electronics industry. More than 2,000 companies enjoy the benefits of CEA membership, including legislative and regulatory advocacy, market research, technical training and education, industry promotion, standards development and the fostering of business and strategic relationships. CEA also owns and produces CES – The Global Stage for Innovation. All profits from CES are reinvested into CEA's industry services. Find CEA online at CE.org, InnovationMovement.com and through social media at ce.org/social.

American International Group, Inc. (AIG) is a leading global insurance organization serving customers in more than 100 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds. The content contained herein is intended for general informational purposes only, and should not be viewed as a substitute for legal, regulatory, accounting or other advice on any particular issue or for any particular reason.

AIG

Bring on tomorrow