Internet of Things: Annotated Bibliography

Prepared by Ashley Dennee, Isabelle Savoie and Alex Weintraub

As of June 9, 2016

Contents:

1: The Internet of Things

A Guide to the Internet of Things Infographic (from INTEL): http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

An Executive's Guide to the Internet of Things Infographic (from Forbes): http://www.forbes.com/sites/baininsights/2016/05/19/an-executives-guide-to-the-internet-of-things-infographic/#5b2fccc3f239

Burrus, Daniel, "The Internet of Things is Far Bigger than Anyone Realizes," *Wired Magazine*, at http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/

As IoT begins to make its mark on the tech industry and revolutionize not only consumer goods but virtually every aspect of human life (author suggests things from cars to street lights to seaports will eventually be "smart"), the importance of IoT, or IoE, lies, as the author points out, in the sensors and cloud computing inherent in the technology. While smart devices have the capacity to "talk to" or communicate with other smart devices (M2M), they also have the capacity to gather and monitor data (vis-à-vis sensors) and analyze that data in real-time (vis-à-vis cloud-based software applications). Below is a poignant example provided by the author of the importance of monitoring and analyzing data in real-time through the novelty of a "smart" infrastructure:

> If there's ice on the bridge, the same sensors in the concrete will detect it and communicate the information via the wireless internet to your car. Once your car knows there's a hazard ahead, it will instruct the driver to slow down, and if the driver doesn't, then the car will slow down for him. This is just one of the ways that sensor-to-machine and machine-to-machine communication can take place. Sensors on the bridge connect to machines in the car: we turn information into action.

Chambers, John and Wim Elfrink, "The Future of Cities," *Foreign Affairs* (October 31, 2014), at https://www.foreignaffairs.com/articles/2014-10-31/future-cities

The authors of the article expound that the integration of IoT into daily life, namely into city infrastructure (roads, buildings, waste management systems, etc.) will greatly reduce costs and yield billions of dollars in value. The authors cite the success of Barcelona, Spain and Songdo, South Korea as two "smart" cities which have integrated various IoE devices and projects into multitudes of city infrastructure projects which have cut costs and reduced emissions, saving energy and dollars. The authors appear to be proponents of IoE in managing cities and the benefits that the public and private sectors could yield if IoE devices were integrated on a greater scale.

Heppelmann, James E. and Michael E. Porter, "How Smart, Connected Products are Transforming Competition," *Harvard Business Review* (November 2014), at https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition/ar/1

The IoT as described by the authors is the "third wave" of product revolution due to information technology. The ubiquitous connectivity of smart devices has two unique functions: 1) to allow the product to transmit information wirelessly to outside parties (i.e. the manufacturer, user, other products, etc.); and 2) the product cloud – allowing some of the product to exist outside of the physical instrument. Connected devices, essentially products with built-in computers with wireless connectivity, require manufacturers to develop new technology infrastructures, known as "technology stacks." According to the authors, a stack is comprised of, "modified hardware, software applications, an operating system embedded in the product…network communications to support connectivity, and a product cloud containing the product-data database, a platform for building software applications, a rules engine and analytics platform, and smart product applications that are not embedded in the product."

These smart devices have three purposes, as argued by the authors: 1) **to monitor** the product's condition, external environment, its operation and usage through the use of sensors, and to enable alerts/notify of changes; 2) **to control** and personalize user interaction with the product in novel ways; 3) **to optimize** the product operation and use in order to enhance the product and to allow predictive diagnostics, service, and repair. Combining these three factors of the "smart" device allows **autonomous** product operation, self-coordination of operation with other products and systems, autonomous product enhancement and personalization, and self-diagnosis and service.

Pierce, David, "The Internet of Things is Everywhere, But it Doesn't Rule Yet," *Wired Magazine* (December 29, 2015), at http://www.wired.com/2015/12/this-year-was-almost-the-year-of-the-internet-of-things/

The article points out that the IoT industry has yet to take off in the mainstream market but is firmly optimistic that its expansion will occur in the near future. The author raises the point that at the present time, IoT companies must still perfect their technology and manage a way to centralize the multitudes of "smart" devices we will likely find ourselves interacting with in the years to come. Another central point the article raises is that in the wake of huge data-hacking scandals like that of Target in 2013, the public and IoT industry leaders must create a dialogue on how private data will be extracted and what will be done with it, and to ensure government transparency in the exchange of information that IoT, as described by the author as a "tidal wave," will bring.

Sarma, Sanjay, "The Internet of Things: Roadmap to a Connected World," *MIT Technology Review* (March 11, 2016), at https://www.technologyreview.com/s/601013/the-internet-of-things-roadmap-to-a-connected-world/

The author at once explains the evolution of the Internet of Things and discusses potential downfalls of the technology. He asserts that the IoT will eventually influence everything, both in industrial and personal spheres, and that the main underlying problem with this is the lack of any clear or universally agreed-upon architectures for building connected systems. Given this main issue and others that IoT expansion will undoubtedly cause, he elaborates upon three main suggestions that he feels would assist in "controlling the chaos." These are **1)** establishing an agreement on system architecture; **2)** developing open standards reflecting the best architectural choices, and **3)** creating a "test bed" where best practices can be designed and perfected.

2: Security of the Internet of Things

Barcena, Mario Ballano and Candid Wueest, "Insecurity in the Internet of Things," *Symantec Security Response* (March 12, 2015), at http://magasinet.f5.dk/wp-content/uploads/2015/08/insecurity-in-the-internet-of-things-2.pdf

This report claims that many household "smart" devices are found to be lacking in critical security apparatuses, leaving them vulnerable to third party manipulation/hacking. Through analyzing 50 common smart devices, the report's authors aim to show that weaknesses to IoT systems are well known to both the security industry and manufacturers and should be fixed in the future prior to the release of any IoT device. Some of the report's findings are:

- None of the tested devices utilized strong passwords, used mutual authentication, or protected user accounts against "brute-force" attacks.
- Some of the IoT cloud interfaces did not support two-factor authentication.
- Most of the IoT services did not provide signed or encrypted firmware updates, if updates were provided at all.

It can be deduced from the report that the methods in which smart devices "connect" wirelessly (most frequently through Wi-Fi, but also through other radio protocols such as Bluetooth 4.0), leave devices unprotected. The authors conclude that IoT devices must start using methods of "mutual authentication and encryption."

Bevan, Kate, "The Internet of Things Makes Strange — and Worrying — Connections," *Financial Times* (January 24, 2016), at http://www.ft.com/cms/s/2/7b880aa2-b616-11e5-b147-e5e5bba42e51.html

The author touches on the explosive impact that the IoT has, and will have, in the coming years on the tech industry. However, the author brings to light some of the security risks associated with IoT devices: last year, Chrysler recalled 1.4 million cars after a Jeep's transmission, air conditioning and radio were all hacked while the car was in use. However, the author cites various reports by firms such as Juniper and Gartner that expect IoT devices to number >20.8 billion devices by 2020. As more and more devices become "smart," the author fears not enough security measures are being taken to insure the reliability and safety of users in the upcoming IoT world. Moreover, the author correctly points out that information gathered and transmitted between devices, known as Machine to Machine (M2M) communication, is not currently protected under data protection laws; user privacy in the new age of IoT is not guaranteed. In 2014, HP reported in a survey of IoT devices that 90% collected "at least one piece of personal information."

Fishenden, Jerry, "Internet of Thieves - Government Must Take a Lead in Internet of Things Security," *CIO* (February 8, 2016), at http://www.cio.co.uk/blogs/political-debate/internet-of-thieves-3634688/

Fishenden notes the need for government intervention in the fight for user data privacy, and he sees the IoT as the next fundamental resource in which private data will be mined. The author seems to focus not on hacking as an avenue in which private data will be "thieved," but rather on big corporations, ad agencies, and even governments themselves as the agents of data heist by lax privacy laws in the emerging IoT market.

Fleishman, Glenn, "An Internet of Treacherous Things," *MIT Technology Review* (January 13, 2015), at https://www.technologyreview.com/s/534196/an-internet-of-treacherous-things/

The author draws a parallel between the insecurity of home networking products (namely consumer-based routers) and the actual and potential insecurity of IoT devices. These devices lack many of the same security measures as routers for a multitude of reasons: **1)** "low price drives buying habits, and features are unevenly included across cheaper hardware, even from major vendors"; **2)** user impatience in creating unique

username/password combinations and two-factor authentication; **3)** devices simply do not receive required upgrades from manufacturers. The author explains that:

> Manufacturers discontinue support to keep costs down; [they] go under or exit the business; and customers may be ill-equipped to handle the technical operation of upgrading firmware, which can involve downloading a patch, and uploading one via an administrative interface in a Web browser.

Higgins, Kelly Jackson, "New Internet of Things Security-Certification Program Launched," *Dark Reading* (May 25, 2016) at http://www.darkreading.com/iot/new-internet-of-things-security-certification-program-launched/d/d-id/1325676

On May 25, 2016 ICSA Labs, an independent division of Verizon, launched a security testing program for IoT products in the hopes of nudging vendors to adopt better security practices for their devices. This follows in the footsteps of Underwriters Laboratories' (UL) launched its Cybersecurity Assurance Program in April (UL CAP), which created a new set of standards for IoT and critical infrastructure vendors to use in evaluating weaknesses and vulnerabilities in their products. The author notes that though a device may seem secure when tested in isolation, vulnerabilities could appear when it is exposed to its operating "ecosystem." An ICSA Labs certification would signify that a product had recently undergone a testing program and that any existing vulnerabilities were fixed. However, even technologies that have the certification must be subject to ongoing testing, as new security risks may appear.

Lomas, Natasha, "The Internet of Things is a Security Nightmare, Warns EFF," *Tech Crunch* (May 9, 2016) at http://techcrunch.com/2016/05/09/the-internet-of-things-is-security-nightmare-warns-eff/

A panel discussion geared at finding a balance between security and privacy at Disrupt New York 2016 tackled important topics such as strategies for securing consumer data and risks associated with an expansion of the IoT. There is a trend in the private sector, especially with messaging companies such as Whatsapp, of increasingly viewing the government as an oppositional force. It is clear that data must be protected, and some experts suggest that one way of doing it is simply not to store the information at all – a zero knowledge model.

The contention between privacy and security has increased dramatically in the past few years given the large shift in volume and type of data being put online. This shift has incentivized hackers to search for and exploit an ever-growing list of vulnerabilities. Nate Cardozo, a senior staff attorney at the Electronic Frontier Foundation, highlights the human risk factor in securing the IoT and worries about how the lack of knowledge or consensus in securing data could impact embedded systems, such as medical devices.

Metz, Rachel, "Finding Insecurity in the Internet of Things," *MIT Technology Review* (January 25, 2016), at http://www.technologyreview.com/news/545661/finding-insecurity-in-the-internet-of-things/

The author suggests that the IoT is an insecure system which has the potential to be manipulated and hacked. Two ways in which the IoT can be made more secure are discussed. The first is to monitor smart devices and their connected networks (things like from where data is being sent, where it's being sent to, and how much of it is actually being sent) and to block suspicious activity. The second, and to which Phil Levis at Stanford's Secure Internet of Things Project promotes, is for software developers of IoT devices to write smarter and more secure code before releasing the products. This is an argument made in other articles mentioned in this list: the IoT will inherently be insecure so long as manufacturers neglect to employ proper security measures in connected, smart devices.

Metzger, Robert, "Reconciling Risk and Value for the Internet of Things," *Federal Times* (February 10, 2016), at http://www.federaltimes.com/story/government/solutions-ideas/2016/02/04/reconciling-risk-and-value-internet-things/79826836/

The author describes the way IoT devices operate and interact with each other, and proceeds to explain the vulnerability of interconnected devices to malicious attacks and the impact such an attack can have on a very broad system (an example the author employs is if a "smart" electrical generator were to be corrupted, countless other generators could be degraded or disabled along an entire grid, simply because of how each generator, in this case, interacts with one another). In his own words:

> The IoT likely will proliferate devices and systems at risk of discrete attacks – an "attack once, impact many" paradigm. This exposure results where devices and dependent systems possess common vulnerabilities and suffer circulation of common injury, and where corruption spread among linked applications affects numerous connected systems.

Metzger suggests that the U.S. government has the ability to curb the impact and frequency of IoT and outlines five "recommendations" he believes will accomplish this: **1)** Create market and tax incentives to encourage defense industrial base and other private sector critical infrastructure participants to self-assess for cyber/physical and IoT vulnerabilities and act to eliminate them; **2)** Promote continuing development of scalable IoT and cyber/physical norms, standards and best practices, while taking care to avoid both prescriptive solutions or the potential chaos of competing and conflicting norms; **3)** Develop and validate methods of authentication and authorization, as may rely (for example) upon embedded, tamper-proof and cryptographically secure chips, in order to enhance transaction security among IoT applications, devices and core systems; **4)** Cause federal agencies responsible for critical systems and infrastructure to assess vulnerability of present and planned systems to cyber/physical threats, and to implement protection plans; **5)** Begin to develop regulations to require defense primes and critical infrastructure contractors to adopt systems to anticipate and avoid cyber/physical vulnerabilities and to monitor and report on cyber/physical attacks. In addition, Metzger highlights the importance of "reaction, recovery, reporting, and information exchange after attack" to bolster security measures, suggesting a codified national strategy for responsible IoT security as essential.

Morgan, Steve, "IoT Security: $1-per-Thing to Protect Connected Devices," *Dark Reading* (January 14, 2016), at http://www.darkreading.com/vulnerabilities---threats/iot-security-$1-per-thing-to-protect-connected-devices/a/d-id/1323921

By comparing the amount of smart devices set to be "connected" by 2020 with the growth of the IoT security industry, Morgan has reached the conclusion that it will cost device manufacturers approximately one dollar per device to ensure the integrity of their security. The author draws a parallel to the need of protecting laptops and PCs to that of protecting current and future IoT devices. Morgan cites an FBI Public Service Announcement which states that difficulty in patching IoT devices has left personal information and physical safety at risk of hackers exploiting IoT security flaws to gain access to home and commercial networks. In the emerging IoT industry, security must be a top priority for every manufacturer and producer.

Thielman, Sam, "The Internet of Things: How Your TV, Car and Toys Could Spy on You," *The Guardian* (February 10, 2015), at http://www.theguardian.com/world/2016/feb/10/internet-of-things-surveillance-smart-tv-cars-toys

The article attempts to explain Director for National Intelligence James Clapper's statement that the IoT will provide law enforcement and intelligence agencies unprecedented surveillance access through the advent of new "smart" devices. While the public dialogue surrounding end-to-end encryption has served as a cornerstone for privacy advocates, government officials, hackers, and potential thieves have a new outlet to monitor user activity, both online and off, through the technological innovations the IoT will bring. Sensors in some devices will be able to provide eavesdroppers audio and visual surveillance to unsuspecting individuals, allowing access for intelligence agencies to "snoop" on targets, provided they possess a lawful warrant to do so. Clapper's statements seem to

contradict efforts being made in the private sector to strengthen the security of IoT devices to protect user privacy. The article points out that some smart devices, such as cars, can provide a "surveillance suite all by themselves." Other devices transmit data and receive instruction from a database or server. The article points out that communication to this database from the device, as well as the database itself, are often insecure and liable for unlawful penetration vis-à-vis third parties. The data stored on these servers, which in effect act as "collection" hubs, can contain information as personal as which items you keep in your refrigerator.

Zetlin, Minda, "Internet of Hackable Things? Why IoT Devices need Better Security," *The Enterprisers Project* (February 8, 2016), at https://enterprisersproject.com/article/2016/2/internet-hackable-things-why-iot-devices-need-better-security

The article is a transcribed interview with the chief information officer of Prescient Solutions, Jerry Irvine. In the interview, Irvine states that IoT devices do not possess adequate amounts of surface area where more complex processing chips could be installed (chips with installed security measures). Therefore, security measures that manufacturers might package with their device aren't physically included, and management applications that do offer basic security measures (username/password) are quite easy to bypass.

Irvine also notes that the machine-to-machine communication (M2M) that IoT devices champion has actually been around for decades, but that the protocols in which they communicate were not designed to exist in the "open environment" that is the Internet, and that the security of these protocols need to be updated in the age of IoT. Irvine suggests that until this happens, IoT and ICS (Industrial Control Systems) devices should be run on networks separate of the Internet, and that only privileged users and computers should have access to these networks. In terms of the commercial appeal of IoT however, this seems to be a major drawback; household IoT devices are marketed on the basis that users will no longer have to manually oversee the operations that their devices perform.

3: Encryption and the Internet of Things

Benner, Thorsten and Mirko Hohmann, "The Encryption Debate we Need," *Global Public Policy Institute* (May 19, 2016), at http://www.gppi.net/publications/global-internet-politics/article/the-encryption-debate-we-need/

This article discusses the issues that arise in law enforcement with the increasing use of end-to-end encryption in the IoT, specifically in messaging devices. The authors compare the U.S. and Germany's encryption debates, outlining the differences between the two in terms of how each country has approached the situation. In the U.S. there is a war between Washington and Silicon Valley regarding the installation of "back doors" that would allow the government access to encrypted information in exceptional circumstances. James Comey, director of the FBI, has referred to the dangers "going dark" could pose for law enforcement. Civil liberties advocates, on the other hand, argue that installing such backdoors could set a worrying precedent in terms of data privacy.

The German government, unlike that of the U.S., has publicly declared its support for more widespread and effective encryption. However, policymakers in Berlin are beginning to worry about the practical realities of more encryption, especially in light of the recent terrorist attacks in France and Belgium. The author suggests that Germany should take an "encrypted world" as a given and foster discussion in this context, focusing on policy that would allow law enforcement to fulfill its duties in a world of ubiquitous encryption. To do so, they must address legal frameworks, technical capabilities and staffing.

Emery, Vaughan, "End-to-End Encryption is Key for Securing the Internet of Things," *HelpNetSecurity* (September 7, 2015), at https://www.helpnetsecurity.com/2015/09/07/end-to-end-encryption-is-key-for-securing-the-internet-of-things/

The author stresses that smart devices offer back doors to potential malicious activity and that data communicated between machines (information recorded by embedded sensors and the traffic from device to manufacturer database) must have end-to-end encryption as a sure-fire way to detract all potential snoopers. Firewalls, according to the author, will not be able to keep up with the IoT device fragmentation and widespread expansion, therefore encryption must be used to ensure user privacy: "Encrypting everything also complements the traditional focus on network security because even when that initial line of defense fails, the data remain protected." Methods that encrypt and compress data in real time are also less likely to hamper user experience as opposed to IPsec and AES encryption methods which require higher intensity processors which are almost always not found in smart devices:

> Only end-to-end encryption can provide the security necessary to minimize IoT-enabled breaches. However, the encryption technology must be designed for modern use cases and devices, such as by making the most efficient possible use of processors and batteries. Organizations that choose the right encryption solution and then apply it everywhere will be best equipped to address IoT-enabled threats.

Perlroth, Nicole, "Defense Secretary Takes Position against a Data 'Back Door'," *The New York Times* (March 2, 2016), at http://www.nytimes.com/2016/03/03/technology/defense-secretary-takes-position-against-a-data-back-door.html?_r=1

Defense Secretary Ashton B. Carter has come out against a government "back door" to encrypted information, stating that he thought such a solution was neither realistic nor technically accurate. In reference to the FBI vs. Apple debate, he that he doesn't "think we ought to let one case drive a single solution" and that policy crafted in anger or grief is unlikely to be effective in the long term. Though he does not take a side in the debate, Carter takes a cue from Silicon Valley and asserts that asking technology companies to create such vulnerability in their systems advocates for a weaker security in a time when they are under constant attack. He encourages cooperation between the public and private sectors, with the creation of a new Defense Innovation Board that would foster collaboration between tech companies, entrepreneurs and the Pentagon in order to create policy that allows law enforcement to continue to do its job, but that does not compromise consumer privacy or security.

4: Data Ownership and Collection in the Internet of Things

"Will the Owner of the Data Please Stand Up?" *InfoBright* (June 18, 2014), at https://infobright.com/blog/will-owner-data-please-stand/

The author points to the Consumer Privacy Bill of Rights as a predecessor and good example of the type of regulatory measures that should be installed when it comes to protecting user data rights in IoT. Users should have the final say as to what is done with data that is collected on their smart devices; the author demonstrates that this is paramount for IoT devices to become ubiquitous in the near-future. The author believes that if companies wish to collect user data generated from IoT, they must prove the "value" of the service rendered from collecting such data.

Akpan, Nsikan, "The Secret Things you Give Away through your Phone Metadata," *PBS Newshour* (June 2, 2016), at http://www.pbs.org/newshour/updates/your-phone-metadata-is-more-revealing-than-you-think/

This article explains just how much personal information is actually stored in easily accessible cell phone metadata, citing a 2014 study from Stanford University. An Android app "MetaPhone" was used to collect metadata from volunteers. Using algorithms to skim online public information, they were able to obtain 82% of the volunteers'

identities. This revelation is troubling despite the shuttering of the NSA's bulk collection program in 2015, as the NSA and FBI can still request access to metadata from the FISA court and the NSA still has access to five years' worth of metadata tied to ongoing legal cases.

Best, Jo, "Who Really Owns your Internet of Things Data?" *ZDNet* (January 11, 2016), at http://www.zdnet.com/article/who-really-owns-your-internet-of-things-data/

There is no exact measure to reference when it comes to data ownership in the IoT. Previous legislation surrounding user data from apps, such as Facebook or Twitter, are outdated and are becoming increasingly irrelevant when it comes to smart, sensor-based devices in the IoT. Within the industry, the topic of data ownership is highly debated and not as clear-cut as many consumers might like. In most instances, it is not clear who owns the data being collected from IoT devices. Often, an app will require users to agree to hand over data being collected by the software company, for storage in a collection database. This is the classic example of targeted-advertising on platforms such as Facebook, Twitter, etc. However, many connected devices do and will gather more types of data: **1) internal data** – data provided to vendor from consumer site detailing how product is being used; **2) external data** – data relevant to customer and/or broader market. An emerging line of thought, as expressed by Eric Harper of ABB, is that the first type of data should be owned by the vendor, since it is used in enhancing the product/service the device delivers. The second type of data, the external, should be used by the consumer however they please; the consumer should own this data. Data ownership in the IoT is a constantly evolving process that needs to be revisited and addressed often as the industry matures.

Guinard, Dominique, "Internet of Things: Businesses Must Overcome Data and Privacy Hurdles," *The Guardian* (June 1, 2015), at http://www.theguardian.com/media-network/2015/jun/01/internet-of-things-businesses-data-privacy

The article points out that data privacy regulations in the IoT are not universal, and are at the discretion of both the user and manufacturer/software developer. The author argues that sensitive data emanating from certain smart devices such as health or finance information should be protected from companies and kept solely in the private domain, but that other types of data, less sensitive in nature, should be communicated and shared with device manufacturers so as to enhance the services provided by the device and to fulfill their functions as connected technology. Ultimately, the author proposes that the final decision of sharing user data should rest with the user, and that universal guidelines be drafted to "address privacy and security concerns while also educating the consumer on where and how their data is being shared."

Waddell, Kaveh, "Who Will Own Your Data if the Tech Bubble Bursts?" *The Atlantic* (May 13, 2016), at http://www.theatlantic.com/technology/archive/2016/05/what-happens-to-your-data-if-the-tech-bubble-bursts/482622/

This article calls into question the notion of data ownership, especially as it concerns failed technology companies and the user data they have collected over the years. People give social media websites like Facebook and Twitter access to large amounts of personal information, assuming that their information will only be used by those companies in non-detrimental ways. However, should one of them go bankrupt, they may resort to selling data in order to salvage themselves - even those companies that have promised not to sell this type of data. Facebook's privacy policy even states that, "if the ownership or control of all or part of [its] Services or [its] assets changes, [it] may transfer [one's] information to the new owner." In the event of a "cyber doomsday," criminal buyers may gain access to millions of users' personal information.

5: Consumer Convenience and the Internet of Things

Tilley, Aaron, "Microsoft, Qualcomm and Intel Start Playing Nice on 'Internet of Things' Standards," *Forbes* (February 19, 2016), at http://www.forbes.com/sites/aarontilley/2016/02/19/microsoft-qualcomm-and-intel-start-collaborating-on-internet-of-things-standardization/#216d2bc51de0

Rival chip makers Intel and Qualcomm have agreed to consolidate their respective standards groups for IoT protocols into one entity, Open Connectivity Foundation (OCF). Industry leaders hope this new group will streamline IoT devices, ensuring that all connected devices will be able to "talk" to each other seamlessly, regardless of the chip manufacturer or operating system of the device. To ensure this, the standards group will define industry regulations regarding communication protocols, software, hardware, and licensing agreements. Microsoft has also played a key role in the formation of OCF; according to a spokesperson, "Despite the opportunity and promise of IoT to connect devices in the home or in businesses, competition between various open standards and closed company protocols have slowed adoption and innovation." Microsoft has a large stake in the future of IoT: Windows 10 will be released for low-powered devices in the near future and will implement the IoT standards defined by the OCF on all of its devices.

"POSCO Looks to Internet of Things for a Safer Workplace," *The Steel Wire* (May 27, 2016) at, http://globalblog.posco.com/posco-looks-to-internet-of-things-iot-for-a-safer-workplace/

POSCO, a multinational steel manufacturing company headquartered in South Korea, is looking to utilize the IoT in order to create a safer work environment for its employees. The company already uses sensors installed on its machines to detect dangerous gases. Now, they are connecting these sensors to employee smart watches in order to increase the speed and efficacy of the safety network. POSCO has also proposed adding smart technology to employees' hard hats and safety vests, giving them increased protection when working alone.

Consumer Protection Infographic (from Consumers International)
https://1.bp.blogspot.com/-91yPgWEDJYA/Vzs0wd-RLLI/AAAAAAAAAX4/RJVr1WgJIoc_A_FOCizp5AuUxPGVesqSwCKgB/s1600/blog2.jpg

Though navigating most daily tasks will be made easier for the average consumer with the expansion of the Internet of Things, many issues may arise concerning consumer protection and rights. Consumers are advised to weigh the pros and cons of technological advancement as it concerns the IoT.