U.S.-KOREA BUSINESS COUNCIL

IoT Innovation and Deployment: A Blueprint for U.S. and Korean Leadership

Written by Dr. Gwanhoo Lee | American University Kogod School of Business

Executive Summary

The Internet of Things (IoT) is transforming the way we live, work, do business, and meet the needs of the public. This emerging technology will impact virtually all industries and all walks of life. There is little doubt the scale of IoT will grow exponentially. It is estimated that the number of connected devices will grow from 20 to 50 billion units in 2020 and the market size will grow to several trillion dollars by 2025. This report presents several use cases of IoT that demonstrate the benefits of the emerging technology in various industries and settings, including energy, manufacturing, healthcare, auto, supply chain and logistics, and cities.

While IoT has a great potential to contribute to economic growth as well as to social welfare, its success will require thoughtful and strategic government policy-making to drive a pro-innovation environment. IoT faces several technical, social, legal, and policy challenges relating to interoperability, radio spectrum, bandwidth, security, privacy, regulation, protectionism, and skill gaps in the workforce that must be addressed to enable the full breadth and reach of IoT innovation. This report summarizes how the U.S. and South Korean governments have been attempting to craft pro-innovation policies and ease burdensome regulations to promote IoT. This report presents recommendations relating to IoT for the U.S. and South Korean governments in terms of general principles, specific policies, and process and structure. Below is a summary of them.

I. Principles of Policies and Smart Regulations

- Develop a consistent, well-coordinated regulatory framework
- Use a light-touch approach
- Regulate based on evidence, not on speculation
- Maintain technology neutrality
- No country-specific regulations or requirements

II. Policies Accelerating IoT Innovation and Removing Barriers

- Address spectrum requirements and needs
- Invest in 5G and new network infrastructure
- Promote adoption of IPv6
- Encourage development of international standards
- Promote security of IoT systems
- Protect data privacy
- Make public sector data freely accessible
- Ensure free data flow across borders
- Drive demand through public sector adoption
- Increase investment in IoT innovation, education, and training

III. Coordination, Collaboration, and Engagement

- Develop national strategies for IoT
- Ensure inter-agency coordination
- Promote public-private partnership
- Foster international coordination, collaboration, and engagement
- Pass the DIGIT Act

I. Introduction

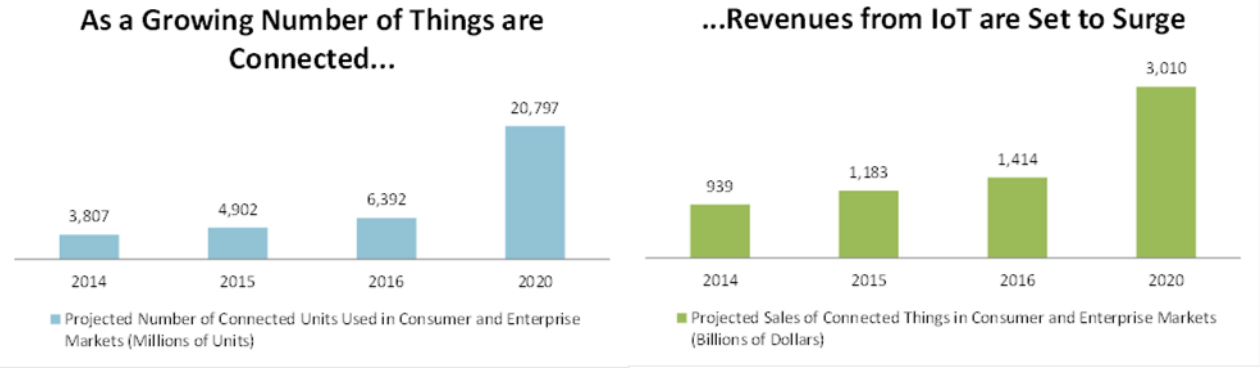
The Internet of Things (IoT) has arrived. It is already transforming the way we live, work, and serve citizens, and will continue to impact virtually all aspects of life. At its simplest, IoT refers to physical "things" connected to the Internet – from thermostats and lamps to cars and machines – that are able to communicate and exchange data without human intervention. These "things" are securely connected through a network to the cloud, from which data can be shared and analyzed to create value[1]. No matter how IoT is defined, it shares a few common principles: ordinary objects include instrumentation such that objects within a network can be addressed individually; the physical objects are interconnected by way of a shared platform; and the devices are "smart" in that they transmit and receive information related to their use, which can lead to the devices performing functions adaptively through cloud-powered machine learning and data analytics[2].

IoT innovation and deployment is being driven by several factors[3] that are combining to accelerate investment in IoT-focused companies and IoT-inspired business models. Sensor prices have dropped to an average of 60 cents from $1.30 in the past decade. The cost of bandwidth has also declined precipitously, by a factor of 40 times over the past decade. Similarly, processing costs have declined by nearly 60 times over the past decade. Smartphones are now personal gateways to IoT, serving as a control hub for the connected home, connected car, or health and fitness devices. With Wi-Fi coverage nearly ubiquitous, wireless connectivity is available for free or at a very low cost. Big data analytics is becoming widely available to analyze hitherto unimaginable amounts of data gathered by IoT devices.

> *"IoT technologies will be a tool in fighting climate change, alleviating poverty, and eliminating large scale hunger. They will increase productivity and efficiencies for small, medium, and large businesses, create new jobs, and contribute to future economic growth."*

There is little doubt the scale of IoT will continue to grow exponentially, and that the potential demand for IoT is significant. Only 0.6 percent of all the things that may one day be potentially connected were connected as of 2013. Exactly how fast the market meets its potential depends on a number of technological, social, and policy factors[4], which may help explain predictions ranging from Gartner's 20 billion connected devices by 2020[5], to Huawei's bolder estimate of 100 billion connected devices by 2025[6].

The IoT market will grow rapidly. Machina Research predicts the total IoT revenue opportunity will grow from $750 billion in 2015 to $3 trillion in 2025[7] and McKinsey estimates that IoT has a potential economic impact of $3.9 to $11.1 trillion by 2025[8]. According to a Cisco study, over the next decade there is $14.4 trillion at stake in IoT for the private sector and $4.6 trillion for the public sector[9]. Interestingly, the Gartner estimates that by 2017, 50 percent of IoT solutions will originate in startups that are less than three years old[10].



Source: Gartner

IoT provides tremendous value to users by offering solutions that not only save time and money, but can also save lives and help governments allocate resources more efficiently. Many connected devices and services have already begun to reshape homes, factories, cities, vehicles, and hospitals. The benefits of increased connectivity will come from two main areas: consumer-facing IoT and industrial IoT. While consumer-facing IoT is what most people think of first, the industrial IoT is expected to account for the lion's share of GDP growth[11] where gains will be derived greater efficiencies in: asset utilization, employee productivity, supply chain and logistics, customer experience, and innovation[12].

While IoT's potential to contribute to economic growth and social welfare is indisputable, its success is not guaranteed without thoughtful strategies to drive a pro-innovation environment. IoT faces several technical, social, legal, and policy challenges, ranging from interoperability and spectrum availability to cybersecurity and privacy. These challenges can and should be addressed by the joint efforts of a wide range of stakeholders from the public and private sector. In particular, the potential benefits of IoT are likely to flow to those nations whose policymakers best enable the opportunities and help address challenges associated with it. The U.S. and South Korean governments should work together to foster IoT innovation and deployment by creating effective policies and a pro-innovation regulatory environment.

This report illustrates several use cases of IoT that demonstrate the benefits of the emerging technology. It then discusses some of the important challenges that need to be addressed to fully realize the promise of IoT, while providing an overview of recent U.S. and South Korean policies and regulations relating to IoT. It presents policy and regulatory recommendations for the U.S. and South Korean governments that will help make IoT technologies ubiquitous.

II. IoT in Action

IoT have the potential to transform virtually all industries and sectors. IoT technologies will be a tool in fighting climate change, alleviating poverty, and eliminating large scale hunger. They will increase productivity and efficiencies for small, medium, and large businesses, create new jobs, and contribute to future economic growth. Due to space constraints, this report highlights three use cases that show a

glimpse of the promising future that IoT brings, with more use cases presented in the Appendix.

Smart Cities: The world's population is increasingly migrating to cities. Fifty-four percent of the world's people live in urban areas and the World Health Organization estimates that by 2050, more than two-thirds of the global population will be city dwellers[13]. IoT technology can transform cities to smart ones. Connected sensors combined with advanced analytics enable cities to better understand and plan for growth, increase efficiency, and assist residents. They can identify open parking spaces and direct drivers to them. Smart streetlights equipped with motion sensors save cities energy and money. Technology can aid public safety by detecting gunfire in troubled areas, and, with real-time data analysis, pinpoint the location of shots, and notify emergency dispatchers to send police officers to the area[14]. Both the U.S. and South Korea have initiated smart cities projects and have become global leaders in the space. Leveraging their technology and experience, the two nations have tremendous bilateral opportunities in helping build smart cities around the world.

Smart Cities in Action: The city of Songdo, South Korea, is one of the world's first 'smart cities.' Construction began in 2003 and is slated to be completed by 2020. Through public-private cooperation involving both the U.S. and Korean companies, the city is planned and built as a leading international business district in Northeast Asia. It aims to become a business and research hub, which targets to build an environmentally sustainable community by using advanced digital technologies on a large scale[15]. The smart city project is divided into six sectors including transport, crime prevention, facility management, disaster prevention, environment, and citizen interaction.

The city is equipped with ubiquitous wireless networks, pervasive RFID, sensor networks, CCTV, telepresence systems, etc. These technological systems enable Songdo to provide its residents with 'smart services' such as effective traffic management, smart health care or smart home management – i.e., citizens can easily connect to the city government, schools, universities, hospitals and more from their home via telepresence. Numerous sensors are installed throughout the city to monitor air pollution, water pollution, traffic, and city facilities. The data gathered by those sensors are sent to the city's Integrated Operations Command Center[16]. Based on the data, a computer system can detect abnormal situations and communicate that information to relevant agencies and residents.

Connected Cars: Connected cars are equipped with Internet access and a swarm of sensors, including road condition sensors, vehicle distance sensors, forward/side/rear obstacle sensors, GPS sensors, driver monitoring sensors, and speed and acceleration sensors, and more. The data gathered by these sensors will be used not only by the driver but also by carmakers, insurance companies, mechanic shops, or even other connected vehicles to improve safety, performance, convenience, and overall driving experience[17]. Both the U.S. and South Korea have globally competitive companies in industries including automotive, consumer electronics, semiconductor, telecommunication, and mobile applications. Naturally, there will be huge opportunities for these companies in collaborating to realize the promise of connected vehicles.

Connected Cars in Action: Using mobile devices, drivers can unlock their cars, check the status of batteries on electric cars, find the location of the car, or activate the climate control system. Concierge features provided by automakers or apps alert the driver of the time to leave to arrive on time from a

calendar on her smartphone and send text message alerts to friends or business associates to alert them of arrival times[18]. They can also help find parking or gas stations. Standards such as the Cellular Vehicle-to-Everything (C-V2X) and the DSRC (Dedicated Short-Range Communications) will serve as the foundation for the connected vehicle of the future. While most connected cars in the early stages will be a car-to-mobile connection, this network will expand eventually to vehicle-to-vehicle and vehicle-to-infrastructure connections. In addition, an important driver fueling the early demand for connected cars is increasingly more sophisticated infotainment systems that provide digital contents to the driver by connecting with smartphones through such standards as Apple CarPlay and Android Auto.

Supply Chain and Logistics: IoT technology can help companies reimagine their supply chains. This capability allows customers to monitor shipments across road, rail, sea, and air. For example, IoT solutions are able to track and monitor the condition of refrigerated shipping containers with perishable goods as they travel around the world[19]. The solutions also can identify inefficiencies or delays in their shipping and confirm product integrity from plant to retail sale. Both the U.S. and South Korea heavily rely on international trade. As such, they have developed efficient supply chains and enabling digital technologies. Through bilateral cooperation, the two nations can transform the global supply chain and logistics.

Supply Chain and Logistics in Action: Companies like FedEx and Union Pacific gain huge benefits from use of IoT solutions. FedEx expects to save $9 million a year using connected sensors on its trucks that let it schedule dock assignments more efficiently[20]. Union Pacific, the nation's largest railroad company, reduced the number of train derailments caused by failed bearings by 75 percent by doing near real-time analysis of data collected by sensors along its tracks[21]. This IoT solution also can predict certain kinds of derailments days or weeks before they are likely to occur, improving safety and potentially avoiding millions of dollars in damages. The company is pouring millions of R&D dollars into new techniques, such as accelerometers on trains that feel for bumps that suggest a bad track.

III. Challenges for IoT

IoT technologies have the potential to drive economic growth as well as to social welfare. However, the rapid development of new technologies creates new technical, social, legal, and policy challenges. This chapter discusses some of the key challenges for IoT that can be addressed by the joint efforts of stakeholders from the public and private sector.

IoT devices and systems must be interoperable in order to effectively communicate with one another. According to a McKinsey study[22], "Interoperability is necessary to create 40 percent of the potential value that can be generated by IoT in various settings." Similarly, Intel's IoT group senior vice president and general manager said, "IoT is a significant opportunity but one that needs interoperability and scale to fulfill industry predictions of billions of connected devices"[23]. Standards play a crucial role in facilitating interoperability across IoT ecosystem. However, many IoT standards are currently competing so it is a daunting task to get all stakeholders to agree on a single standard[24].

The good news though is that industry standards bodies have already begun the process of developing technical standards for the IoT and many industry standards organizations are starting to come

together to create joint organizations. For example, the Open Connectivity Foundation, which brought together members of the previously competitive Open Interconnect Consortium and the AllSeen Alliance in February 2016, has expanded to hundreds of members across Asia, North America, Europe and other geographies[25]. Further, The Industrial Internet reached an important milestone with the founding of the Industrial Internet Consortium in 2014, charged by its members—coming from Europe, Asia, and the United States—with promoting initiatives to connect and integrate objects with people, processes, and data using common architectures, interoperability, and open standards.

Large volumes of data collected from numerous sensors embedded in connected cars, roads, streetlights, mobile health devices, and home appliances must be able to flow freely over wireless networks. The crucial question is whether the wireless infrastructure can keep up with the demand to support the explosive growth of IoT. The amount of traffic passing through wireless networks today is already overwhelming. The possible surge in demand from IoT devices will add much more demand for more mobile bandwidth. To meet the demand, we must expand the capabilities of wireless networks. Deployment of 5G (the fifth generation of wireless communications technology) will be essential to handle the traffic generated by IoT. The transition from 4G to 5G requires not only substantial investment but also much more spectrum.

> *"More than ever, we will need to work together to promote the advancement of these connected devices while also ensuring they are secure, safeguard our privacy, and remain worthy of our trust."*
> *-the White House*

The security of data collected from IoT devices may face new risks. A recent study by HP revealed that 70 percent of the most commonly used IoT devices contained vulnerabilities ranging from inadequate consumer passwords to more serious issues[26]. The range and number of devices and disparate networks that are being used may expand the number of potential targets for cyber threats.

With IoT applications, cyber risks are transferred to risks in physical systems[27]. Some of IoT use cases have been compromised already due to unanticipated cyber threats, if devices and networks are not properly protected. For example, certain early connected cars and medical devices have been hacked[28] and some low-powered specialized IoT devices may not have the processing power to maintain high levels of security. Considering the risk factors associated with the expansion IoT, it is important to address cyber concerns at the outset.

IoT also may heighten privacy concerns for consumers. It could carry the risk of intrusive monitoring, an unacceptable invasion of privacy, or the misuse of or unauthorized access to intimately personal information. While more information will be collected and transmitted over networks, it may not always be possible for consumers to know how their data is being used. In addition, many IoT devices are too small to have screens or other direct user interfaces. This constraint creates challenges for privacy regimes based on the traditional concepts of "notice and consent". Therefore, it is important to design effective, yet flexible methods and policies to protect consumer privacy.

In addition to the challenges discussed above, there are policy and regulatory decisions that will need

to be made in order to facilitate the adoption of IoT technologies on a broad scale. For example, it is possible that a company making IoT systems is subject to an inconsistent, conflicting patchwork of regulations imposed by multiple government agencies. A lengthy and cumbersome regulatory review process especially for connected medical devices may discourage companies from developing innovative IoT products. The advancement of IoT requires unprecedented coordination among a myriad of government and industry stakeholders.

The importance of inter-governmental coordination cannot be overstated. In efforts to promote 'national champions' some policymakers have created policies that hinder foreign companies from competing in the domestic market, preventing certain technologies from becoming ubiquitous. Some nations want to restrict cross-border data flows, creating costly compliance regimes that deter foreign investment. Roaming is another important issue, since the vast majority of IoT devices and sensors will be mobile and will need to cross over network boundaries. Finally, there will be a growing skills gap to support IoT development. We must train our students and workforce in the skills needed to foster IoT innovation. All of these barriers must be removed to enable IoT to reach its full potential and deliver its transformative societal and economic benefits.

IV. Current Policies and Regulations in the United States and South Korea

The United States

It is important to first understand the U.S. strategy for innovation in a broader context. President Obama issued the *Strategy for American Innovation* in 2009 and updated it in 2011 and 2015[29]. In this President's Strategy, the Administration has identified policies to sustain the innovation ecosystem that will deliver benefits to American people. The Strategy recognizes the important role of the federal government to invest in the building blocks of innovation, to fuel the engine of private-sector innovation, and to empower a nation of innovators.

One of the initiatives in the Strategy is building smart cities, which is closely tied to deployment of IoT[30]. The initiative will focus on four key strategies: creating test beds for IoT applications and developing new multi-sector collaborative models; collaborating with the civic tech movement and forging intercity collaborations; leveraging existing federal activity; and pursuing international collaborations.[31]

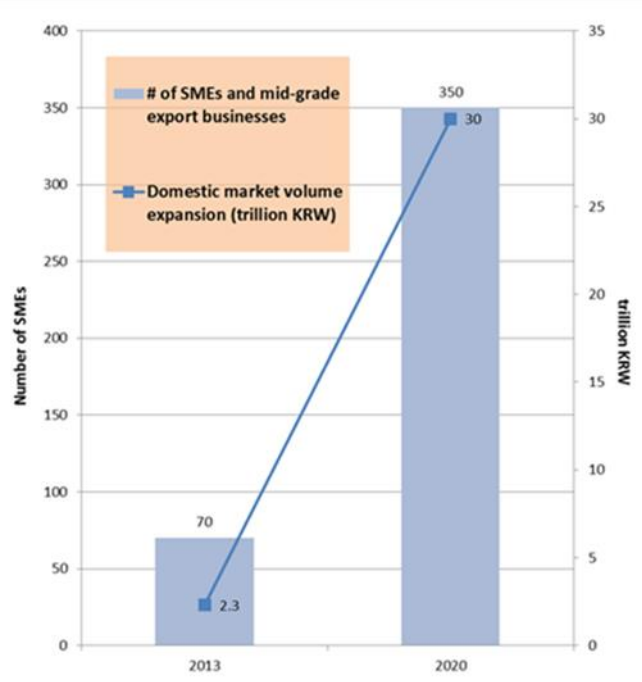
Several agencies have been actively involved in efforts to support IoT. In 2013, the Federal Communications Commission (FCC) held a public forum to get input from industry with respect to policies and regulatory barriers for IoT. In 2014, NIST facilitated the convening of the Public Working Group on Cyber-Physical Systems (CPS) to foster public-private multi-stakeholder discussion on CPS. In May 2016, the Public Working Group released the Framework on Cyber-Physical Systems[32] to provide a comprehensive tool for the analysis and description of connected devices and systems. The US Food and Drug Administration (FDA) has proposed to largely deregulate a long list of Class I and Class II medical devices and no longer require their makers to go through the 510(k) process[33]. The U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) has worked closely with Congress, the FCC, and other government agencies to make significant progress on President Obama's 2010 commitment to make a total of 500 MHz of spectrum available for commercial use by 2020[34]. In June 2016, the NTIA solicited public comments on the benefits,

challenges, and potential roles of the government in fostering the advancement of IoT. Most recently, in September 2016, the Department of Transportation issued guidelines that pave the way for self-driving cars to hit the roads without much red tape[35].

While those government activities are encouraging, their efforts have not been adequately coordinated, as no comprehensive national strategy for IoT exists. To address this issue, the US Senate passed a resolution in March 2015 calling for the development of a national strategy for IoT to promote economic growth and consumer empowerment[36]. It also called for a modern framework around innovation, recognizing the importance of industry-led, consensus-based best practices. The US House passed a similar resolution by a near-unanimous vote in September 2016. Congress has been deliberating on the bill known as the *Developing Innovation and Growing the Internet of Things (DIGIT) Act*, which builds on the Senate resolution.

South Korea

The South Korean government has planned to invest 5 billion dollars through 2020 in IoT systems ranging from wearables to smart cars[37], and has taken a number of steps to foster the growth of IoT since publishing its national master plan in May 2014.



Source: Ministry of Science, ICT & Future Planning

The master plan's strategies include development of open platforms for IoT through strengthening collaboration among companies involved in IoT ecosystem, leveraging the concept of open innovation, and strengthening global collaboration with global companies to co-develop products and services and join forces in entering the global market[38]. The plan targets the commercialization of 5G mobile communications by 2020 and aims for Gigabit Internet to achieve 90 percent national penetration by 2017. It aims to secure over 1 GHz of radio spectrum by 2023 and significantly expand the deployment of IPv6 by 2017[39]. The plan also expresses support for standards intended to facilitate global interoperability.

In October 2014, the Ministry of Science, ICT, and Future Planning released a roadmap for IoT to guide government actions to develop cybersecurity standards and best practices[40]. Its strategy centers on strengthening cybersecurity policy, technology, and industry. The Ministry aims to promote the concept of "security by design," develop test beds to validate security measures and capabilities, build a collaborative network with the U.S., Japan, and EU to share information, and promptly respond to security incidents or new cyber threats. In June 2015, the Ministry launched IoT Security Alliance, which is a public-private joint council[41]. Furthermore, the Ministry opened an IoT-ISAC (Information

Sharing and Analysis Center) in 2015 and plans to launch an IoT-CERT (Computer Emergency Response Team) in 2016.

In May 2016, the South Korean government announced plans to ease regulations on the ICT sector as part of its aggressive deregulation drive[42]. It focuses on lowering the barrier for companies to launch businesses in IoT sector and prompting an early establishment of nationwide networks dedicated to IoT. The launch of new businesses based on location information services will be changed to a report-based system from the current permission-based one. The government also plans to lift a series of regulations covering cloud computing, drones, the biotech industry, autonomous vehicles, and other areas as part of a broader deregulatory campaign aimed at boosting economic growth[43]. With the lifting of those regulations, the government will approve all drone-related businesses except for those that may undermine the safety of citizens or national security. Test operations of self-driving cars, which had previously been allowed only in limited regions, can now be conducted across the entire nation. And in an emergency, 3D printers now can be used to make medical devices under the direction of doctors.

In order to boost the use of big data, the Korean government plans to ease rules on the protection of private information, which has been cited as a major roadblock to the development of big data applications. Rules on the use of satellite-based location data will be relaxed to a certain extent to support related businesses. The government will also set up guidelines on the extent to which wearable smart gadgets can collect information on the body. It decided against regulating Samsung phones with a mobile health component as medical devices[44]. The government's Telecommunications Strategy Council has been given responsibility to adapt existing laws and regulations to ensure a liberal and competitive industrial environment for IoT[45]. Where the Council finds regulations that hinder ICT convergence, it can request related ministries to improve these regulations.

V. Recommendations for the Role of the U.S. and South Korean Governments

IoT offers unprecedented opportunities to grow the economy and solve various social problems. However, its potential benefits depend in part on how policymakers respond to the opportunities and challenges associated with it. Unnecessary, excessive or poorly-designed regulations can significantly slow the growth of IoT. Historically, smart policies and regulations that proactively support innovation or avoid doing harm have been integral to the success of major technological developments such as the Internet and global positioning systems[46]. Similarly, smart policies can foster the growth of IoT. In what follows, this report presents a set of principles that can guide U.S. and South Korean policymakers in their efforts to build an effective policy framework. It then recommends specific policies that help accelerate IoT innovation and remove adoption barriers. Finally, this report makes recommendations for processes and structures that the U.S. and South Korean governments should establish to accomplish their policy goals.

5.1 Principles of Policies and Smart Regulations

Develop a consistent, well-coordinated regulatory framework: The early years of the IoT have shown that multiple agencies and ministries are eager to assert jurisdiction over IoT products and services. A

multitude of uncoordinated efforts of federal, state, municipal, and local governments to regulate IoT can create an uncertain and inconsistent regulatory environment. Consequently, companies can face the prospect of multiple regulators creating a confusing and disjointed patchwork of regulations. For example, a company developing connected devices for cars could be subject to overlapping or inconsistent federal oversight from a consumer protection regulator (Federal Trade Commission), a transportation safety regulator (National Highway Traffic Safety Administration), and a spectrum regulator (Federal Communication Commission), among others. Rather than govern IoT piecemeal, government should harmonize existing regulatory structures. Sector-specific regulation can cause fragmentation that threatens deployment of IoT, as it impedes the interoperability of devices and the aggregation of data across platforms[47]. Except for some specific matters germane to a particular industry, government should develop a holistic and consistent regulatory framework that is neutral across industries.

Furthermore, a lengthy and cumbersome regulatory review process increases the time to market for connected devices and thus discourages companies from developing new IoT products. For example, it takes on average over two and a half years for the U.S. Food and Drug Administration (FDA) to approve a low-risk medical device, compared to an average of seven months in Europe[48]. Due to a more efficient regulation process of the EU, many mobile health companies enter the EU market first and then secure US FDA approval later. Government can help IoT sector by working to streamline the regulatory process and pave the path for innovators.

Use a light-touch approach: When multiple agencies are trying to regulate IoT, there is also a risk of over-regulation. Some policymakers might believe that preemptive regulations will increase consumer trust and therefore increase adoption. However, heavy-handed regulations would likely limit innovation, impose costs, and thus slow down adoption[49]. For example, in South Korea, the use of cloud computing in the healthcare industry is severely constrained due to the regulation that mandates health-related data to reside in the hospital. In addition, telemedicine is not allowed in South Korea. Policymakers should adopt a “do no harm” or a “wait and see” approach because IoT market is still nascent. With this light-touch approach, policymakers should allow room for industry-led, market-based solutions to address emerging issues. Such industry-led solutions are often more flexible and able to successfully deal with rapidly evolving technology innovation. Policymakers should avoid premature regulations that could have harmful unintended consequences. Policymakers should step in only if market forces fail to address a persistent issue.

Policymakers should try to avoid adopting new regulations designed specifically for IoT products and services. Although IoT technology is revolutionary in certain aspects, it is still fundamentally an extension of existing technology. Many sound frameworks are already in place to address most of the policy issues relating to IoT and the existing regulatory framework should serve as the starting point when considering creating new regulations just for IoT context. For example, the FTC recently concluded that there was not yet a compelling need to regulate consumer-facing IoT privacy[50]. Policymakers should permit IoT ecosystems to be developed by technology companies in an environment without additional IoT-specific regulations layered atop the regulatory safeguards that already protect consumers[51].

Regulate based on evidence, not on speculation: Creating restrictive regulations for an emerging technology such as IoT, without clear evidence of concrete consumer harm, can have the unintended consequence of limiting innovation. Before reacting reflexively and prematurely to anecdotes or purely speculative concerns, policymakers should ground decisions and recommendations in rigorous economic and empirical analysis. Policymakers should perform a proper cost-benefit analysis before proposing new regulations. An economic and evidence-based approach is more likely to result in smart regulation that protects and enhances consumer welfare. When policymakers need to intervene to address specific persistent problems, they should ensure that their rulemaking targets specific, demonstrated damages rather than creates general, sweeping regulations that could unnecessarily limit deployment of the IoT.

Maintain technology neutrality: Policymakers should not favor or advantage any particular technology. They should not pick technology winners or losers. Historically, technology-neutral policies helped the Internet technologies realize their greatest potential. Similarly, policymakers should maintain the concept of technology neutrality to facilitate the virtuous cycle of IoT innovation[52]. Much is unknown about the future uses of IoT, including the business structures, distribution and supply chains, and the uses and flows of data that future IoT devices, applications, and services will create. For this reason, policymakers should let any innovative technologies be freely developed[53]. Prescriptive regulation that dictates particular equipment or technology is not only unnecessary but also counterproductive.

No country-specific regulations or requirements: Some policymakers view IoT as an opening to create export opportunities for their domestic firms. These policymakers may endorse policies that hinder foreign companies from competing in the domestic market[54]. Such policies are anti-competitive and create fragmented IoT markets. It is concerning that country-specific measures and barriers are rising. Some countries have implemented legislation and licensing rules that require country-specific device identifiers, or require providers to locate data within a particular country. For example, Singapore has established a requirement that every device number be registered with the government. India is also considering imposing a similar registration requirement. Other countries have imposed or are considering government mandates relating to privacy and cybersecurity requirements, technical standards, and interoperability. Continued adoption of those country-specific requirements will undermine providers' abilities to deliver consistent global offerings in a cost effective manner[55]. By contrast, technologies built on global standards combined with globally consistent regulations can boost innovation and competition, ultimately improving consumer welfare.

5.2 Policies Accelerating IoT Innovation and Removing Barriers

Address spectrum requirements and needs: IoT innovation and deployment depend heavily on spectrum availability. There is no question that more spectrum is needed to support the over one hundred billion IoT devices that will be in use in 2025[56]. Most IoT applications currently operate on unlicensed frequencies, using standards such as Wi-Fi, Bluetooth, ZigBee, and Z-Wave. Although unlicensed spectrum will continue to play a vital role, the big data generated by IoT will need to make use of both licensed and unlicensed spectrum because the data will ultimately be sent to the cloud via a cellular network[57].

5G will become the backbone communications and computing technology of IoT. The transition from 4G to 5G requires substantially more spectrum for commercial use. The U.S. and South Korean governments should develop policies that promote flexible and creative uses of spectrum. For example, they should consider encouraging spectrum sharing among government and commercial operators and using 4G LTE in unlicensed spectrum (LTE-U).

Invest in 5G and new network infrastructure: Connectivity is arguably the most important prerequisite for IoT deployment. IoT requires not only increased spectrum for commercial use but also deployment of the underlying core network infrastructure necessary to support use of that spectrum. Due to the increased number of connected devices, network traffic will be 22 times greater in 2018 than 2013[58]. 5G will offer speeds measured in multiple gigabits per second, latency in the single milliseconds and the capacity to handle 1,000 times more consumption than current network technologies[59]. 5G requires a dense network of small cell receivers and wireless networks increasingly integrate smaller antenna technologies. The government can promote the investment in such infrastructure by expediting tower and small cell siting on government land.

U.S. and South Korean policymakers should implement policies that promote investment in new wireless network infrastructure that is scalable and is capable of handling a broad range of IoT applications' communication needs in terms of mobility, speed, latency, battery-life, and reliability. For example, in July 2016, SK Telecom, South Korea's largest mobile operator, has completed the nationwide rollout of a low-power wide area network based on LoRa technology that is optimized for small IoT devices that require transmission of small amounts of data over a long distance at a very low cost[60].

Promote adoption of IPv6: IPv6 will be the Internet protocol for IoT. However, the transition from

> *"Connectivity is arguably the most important prerequisite for IoT deployment."*

IPv4 to IPv6 is taking longer than expected. With only 4.3 billion possible addresses, IPv4 cannot cope with the explosive demand of connected devices. In fact, many devices are already sharing IP addresses by network address translation (NAT) and carrier-grade network translation (CGNAT) methods that allow multiple devices to share one IP address[61]. This sharing solution creates interoperability issues with applications and devices and increases maintenance costs for IP addresses. To resolve these issues, U.S. and South Korean policymakers need to accelerate IPv6 adoption in networks and devices and promote more IPv6 enabled content. To this end, as the National Telecommunications and Information Administration (NTIA) recommends[62], the government could support certain types of research and development activities, act as a consumer of IPv6 products and services, and act as an educator.

Encourage development of international standards: Interoperability is another critical success factor for IoT and without it more than 40 percent of the benefits of IoT may not be realized.[63] For example, the benefits of connected cars will be greatly reduced if cars, traffic lights, road sensors, and parking sensors use different communication standards, thus not being able to communicate with each other. Therefore, it is crucial that international IoT standards are developed and adopted because standards

provide the basis for interoperability and increase economies of scale.

Standards range from overarching guidelines to specific technical protocol criteria[64]. They should be open, voluntary, private-sector-led, consensus-based, and globally relevant[65]. Such standards can promote innovation and ensure integration of new IoT systems and legacy systems. The U.S. and South Korean governments should support global industry efforts to develop IoT standards. But the governments should be careful not to try to pick winners. The main roles of the governments in standards setting activities should be a promoter, a convener, a trusted expert, and a major implementer of standards. The governments need to ensure that standards-setting activities are industry-led, open, and transparent and that standards are accessible to prospective implementers. Historically, this industry-led approach has proven most effective. For example, the global standardization efforts conducted through the 3GPP organization for 4G LTE have been very successful in enabling the commercialization of new technologies without governmental intervention. The U.S. and South Korean governments should replicate this approach for IoT standardization.

Promote security of IoT systems: IoT may open up new cybersecurity vulnerabilities, if not protected properly. Certain IoT products are often created by consumer goods manufacturers rather than IT firms. As a result, these IoT products may not always be designed with the best cybersecurity practices. In order for IoT to be widely adopted, customers must trust that their data is being securely transmitted. A well-designed and secure device and network is crucial for protecting the vitality of IoT[66]. However, cybersecurity risks are constantly evolving and the cyber threat landscape is rapidly changing. Government and industry must work together to effectively cope with cybersecurity challenges for IoT. However, top-down, pre-defined, prescriptive regulation is generally unnecessary, premature and unwise, especially at this early stage of IoT development as regulation could quickly become obsolete[67]. The policy environment should enable cybersecurity solutions to evolve at the pace of the market, not at the pace of policymakers' decisions.

An effective approach to address IoT cybersecurity challenges is through industry-led voluntary risk management, public-private partnerships, multi-stakeholder collaboration, and information sharing[68]. The US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[69] can serve as a good model for multi-stakeholder government-industry efforts to promote cybersecurity. The framework is effective and well received by industry because NIST, in collaboration with industry, identified a flexible set of standards, guidance, and best practices that companies can voluntarily choose to use. In addition, the FTC published guidance on what companies should consider when they design and market IoT products[70]. The FTC has initiated a program called "start with security" to promote the principle of "security by design". Importantly, U.S. and South Korean policymakers should not create new cybersecurity regulations specific to IoT. Instead, they should work with the existing policy frameworks, focusing on managing newly identified risks associated with IoT technologies as opposed to regulating IoT technologies themselves.

Protect data privacy: IoT has the potential to heighten consumers' data privacy concerns. IoT manufacturers are advised to adopt a "privacy by design" approach that aims to build privacy safeguards in products upfront.[71] Emphasis should be given to technical innovation in privacy-enhancing technologies to enable individuals to manage and control their personal data more

intuitively and effectively[72]. It is unclear exactly how nascent IoT markets would affect consumers' privacy concerns. Therefore, regulators should not rush to craft premature regulations. Instead, they should allow IoT to develop within the current policy framework with some possible modifications[73].

One possible modification pertains to the traditional "notice and consent" framework. The framework may not make sense to certain IoT devices such as some sensors and actuators with no or limited user interfaces. It will not always be possible to provide users with privacy-related information and check-box options. In fact, the vast majority of IoT applications are likely to pose no real threat to consumer privacy and most data collection would likely be routine and insignificant. In such use cases, consumers do not benefit from being inundated with notices. Regulations requiring consumers to give consent manually to data collection would impose costs on companies and such costs will ultimately be passed on to consumers. These concepts can be modernized for IoT space, though. Policies and solutions must focus on outcomes such as transparency and user control rather than requiring a specific type of check-the-box consent. Companies involved in IoT should look for innovative ways to be forthcoming about the data they collect and how they will use it. For example, IoT devices can use online dashboards, apps, or customer support to increase transparency about data practices.

Make public sector data freely accessible: Government can foster IoT innovation and increase consumer welfare by opening up public sector data collected by IoT devices. Government will increasingly integrate connected devices into public infrastructure and government services. The de-identified data it collects should be treated as a public resource and shared with the public accordingly[74]. By making public sector IoT data available to the public through data portals and application program interfaces (APIs), government can create opportunities for citizen welfare, private-sector innovation, and academic research. For example, the city of Chicago has been integrating IoT devices into city infrastructure and services as part of its Array of Things project. It has made over 600 datasets freely available online. With this new resource, citizens have been able to more easily navigate public transit, the city's pest-control agency has reduced the rat population, and the police have created predictive models to fight crime more effectively[75]. Government can also design regulations to free up regulated industry's data, such as energy consumption data. Such data can empower consumers to reduce their energy use and boost the development of new services.

Ensure free data flow across borders: Data flows across national borders are vital for delivering IoT services. However, some nations want to restrict how data can flow across borders. A growing number of countries, including Australia, China, France, India, Russia, and Taiwan, have proposed or adopted obligations to keep data and computing facilities within their country[76]. For example, India requires that gateways and servers that support IoT applications are located inside the country. Although the rationale is to protect national security, these localization requirements are not likely to heighten national security. Such requirements only limit the ability of IoT device manufacturers and service providers to analyze data collected globally and thus impede the provision of various IoT services. The U.S. and South Korean governments should lead and actively participate in the global dialogue with their counterparts in other countries and should advocate for and enact policies that enable free data flow across borders[77].

Drive demand through public sector adoption: Government can and should play an important role in driving demand for IoT. As many IoT services are subject to network externality, the benefits of these services exponentially increase as the number of connected devices increases. Government can act as an early adopter of IoT to jumpstart the network effect, demonstrate the benefits of the technology, and improve public services, both through pilot programs and in full-scale implementations[78]. Government should develop action plans for the deployment of IoT and make "smart" the default for all new investments and allocate funding for smart city demonstration projects[79]. Government should consider revising procurement and grant policies to promote deployment of IoT devices.

Increase investment in IoT innovation, education, and training: To accelerate IoT innovations, government should engage in various types of funding programs that are open, transparent, competitive and technology-neutral. For example, government can sponsor national challenges with prizes to encourage the development of IoT applications; subsidize connected devices for low-income populations; and establish government-backed venture capital funding for promising technologies[80]. In addition, government may establish a center of innovation to engage in R&D, applications development, standards development, training, and policy development[81].

Government should play a crucial role in educating students and training the workforce. As IoT technologies are advancing quickly, there is a growing skills gap. The World Bank estimates that 200,000 new engineers are required every year from 2014 to 2022 in IoT space[82]. The demand for workers skilled in cybersecurity is particularly strong. If the U.S. and South Korea want to be the leaders of IoT technologies, they must prioritize and allocate significant resources to training and education. Government should partner with universities to develop IoT and data science curricula for high school and higher education, offer training opportunities to businesses, and create scholarship programs focused on STEM education.

5.3 Process and Structure for Coordination, Collaboration, and Engagement

Develop national strategies for IoT: The U.S. and South Korean governments should create comprehensive national strategies for IoT to ensure that the technology develops cohesively, that barriers to IoT adoption are removed, and that both the private and public sector fully realize the potential impact of smart, connected devices[83]. Many opportunities with IoT are closely tied to areas of public sector activity. Moreover, some market failures can be effectively addressed by government efforts and interventions. A well-thought-out national strategy can go a long way. Once created, a national strategy should be updated regularly. Further, national agencies involved in specific sectors should develop action plans. In the United States, for example, the Department of Housing and Urban Development should develop an action plan to promote smart homes, and the Department of Energy should develop a plan to improve energy efficiency with connected devices.

Foster international coordination, collaboration, and engagement: It is critical to ensure coordination among industry and governments around the world in order to fully realize the promises of IoT technologies. As countries attempt to make their IoT industries more competitive, some countries may resort to protectionism. The U.S. and South Korean governments must be vigilant, and guard against such protectionism that endangers the open, consensus-based, private sector-led development of IoT

standards and technologies. They should continue their dialogue with their counterpart agencies in other countries. As the global leaders in IoT space, the U.S. and South Korean governments should establish a bilateral working group to coordinate on issues like industry-led standards, pro-competitive policies, and international harmonization of spectrum. In that process, the working group should seek industry input.

Ensure interagency coordination: If poorly coordinated, government policies and regulations pertaining to IoT can confuse and frustrate businesses as well as consumers, thus slowing down IoT deployment. Due to the convergence of multiple industries that are traditionally unrelated, the same IoT technology might be subject to conflicting regulations imposed by different agencies and ministries. Therefore, it is important to ensure smooth and effective coordination among government agencies. One possible solution is to create an interagency task force that coordinates all relevant agencies on IoT-related issues.

Promote public-private partnership: Strong public-private partnership is essential for the success of IoT. Many IoT projects can benefit from public-private partnership. For example, the city of Mumbai, India partnered with a smart metering company to help with its failing water infrastructure. For the same amount of money the government would have spent patching new leaks without ever improving the overall integrity of the system, the partnership with the metering company cut the water loss in half. For productive partnership with the private sector, government should keep up with technological development by engaging in continuous dialogues with companies and attending high-tech trade shows. Furthermore, government should consider creating a nonpartisan National IoT Advisory Board of policymakers, agency representatives, industry leaders, think tanks, academia, and leaders of IoT-focused consortia[84]. A government and industry standing body can coordinate, collaborate and leverage industry IoT consortia[85]. A good example can be found in the convening of the Public Working Group on Cyber-Physical Systems formed under the sponsorship of NIST. This open public forum has fostered stakeholder discussion to define and shape key characteristics of CPS[86].

Pass the DIGIT Act: The U.S. Congress is considering a bipartisan bill known as the *Developing Innovation and Growing the Internet of Things (DIGIT) Act*. This bill builds upon the resolutions that passed the Senate in March 2015[87]. In the resolution, the U.S. Senate supported a national IoT strategy in order to maintain U.S. global competitiveness in the digital age. It also called for a modern framework around innovation, recognizing the importance of industry-led, consensus-based best practices and the need for innovators to drive the future development of IoT. The resolution calls on the U.S. to develop a national strategy that would incentivize the development of IoT, prioritize accelerating its development and deployment, and ensure it responsibly protects against misuse. Once passed by Congress, the Act will pave the way for America's global leadership in the rapidly evolving IoT marketplace by bringing together stakeholders in government and industry to ensure that the United States realizes the full economic potential of IoT. Therefore, it is crucial that the DIGIT Act is passed by the U.S. Congress in the near future. The Act will have profound impacts not only on the U.S. but also on South Korea. Government and industry should work together to help pass the Act in Congress.

VI. Conclusions

IoT is here now to transform all aspects of life. But we are only beginning to see a glimpse of the promising future that IoT can bring. As the global leaders in many industries including automotive, consumer electronics, semiconductor, telecommunication, mobile devices, and software, the U.S. and South Korea are facing huge bilateral opportunities to boost the global economy through IoT innovation and deployment. In order to fully realize the great impact of IoT on economic growth and social welfare, the private and public sector should collaborate to foster innovation and remove roadblocks. U.S. and South Korean policymakers must make sure to shape pro-innovation policies and regulations that are evidence-based, consistent, light-handed, and technologically neutral to help their nations be global leaders in IoT space. A bilateral working group involving governments and the private sector from the U.S. and South Korea needs to be established to promote IoT and coordinate on issues such as interoperability, cross-border data flow, security, and privacy. With concerted efforts of government and the private sector both domestically and internationally, IoT will live up to its promise to make the world a better place.

Appendix: Additional Use Cases of IoT

Smart Cities in Action: The City of San Antonio is leveraging a fiber-optic network backbone and wireless mesh network that extends connectivity, the city has developed a variety of IoT-based systems, including a networked traffic-light system that allowed it to recoup $2 billion that was lost due to longer commutes, higher fuel expenses, safety issues, and other factors. Similarly, Kansas City, Missouri partnered with leading IoT companies to design a smart city platform that would enhance Internet connectivity, enable efficiencies in management of public infrastructure, introduce new revenue streams, and improve the citizen experience[88]. The city's smart lighting ensures safer streets and more efficient management of roads, bridges, and city assets through use of data and analytics gathered from sensors placed in the downtown area. To explore all the potential benefits from the smart, connected devices, the city also opened a Living Lab where new uses for the data can be proposed and validated. The City of Cincinnati reduced residential waste volume by 17 percent and increased recycling volume by 49 percent through use of a "pay as you throw" program that used IoT technology to monitor those who exceed waste limits. Cincinnati also partnered with Qualcomm to develop an integrated water connectivity solution that collects actionable information from its water system to improve water quality and facilitate the management of its water resources[89].

Supply Chain and Logistics in Action: Rockwell Automation, an industrial automation firm, uses IoT systems to automate the collection and analysis of data from remote installations across its customer's petroleum supply chain[90]. Its IoT systems have transformed its customer's entire oil and gas supply chain. From the ocean floor to the gas pump on the corner, IoT system is used to light up traditional pump, transport, and meter equipment with connected sensors, and harness data that provides new insight. With this real-time view of the operation of machinery in far-flung and isolated regions, oil and gas companies now can remotely monitor assets across the supply chain and even predict potential problems and costly failures before they happen.

Healthcare in Action: Connected sensors combined with data analytics capabilities have a great potential to revolutionize costly, inefficient healthcare systems and improve consumer wellness. Data generated from wearable devices such as fitness trackers allow consumers to monitor daily activities and a broad range of biometric data. This data can generate new insights into consumers' health and may be shared with their trusted circle as well as their doctors. By so doing, consumers may even earn lower health insurance premiums in exchange for demonstrably healthy behavior. IoT technology can help caregivers and patients bridge the gap between a clinical setting and the home through accurate measurement and transparent data sharing. Remote care management solutions can help people with chronic health conditions live more independently by using IoT devices to collect patient data through motion sensors installed in a residence or care facility.

Verizon and AMC Health jointly developed a mobile patient monitoring solution. With this solution, an active pregnant woman who needs to track her blood sugar can use a mobile device such as a smartphone or tablet to communicate readings from her glucometer at any time and any place she chooses and the information is stored securely in the cloud[91]. Her care provider has 24/7 access to her information and can determine whether she, her baby, or both are at risk. Using this information, the

woman's healthcare provider can provide more timely and appropriate care.

GlowCap is a pill container cap with wireless capabilities to remind a patient to take pills as prescribed. It sends notifications to the patient via light and sound. The patient receives weekly emails showing which days she did, or didn't, take a medication as well as a printed monthly progress report in the mail. Moreover, the patient can send refill requests to her local pharmacy by pressing a button at the base of the GlowCap lid. A study found that GlowCap service raised medication adherence rates 27 percent, resulting in 98 percent adherence[92].

Dexcom's mobile CGM (Continuous Glucose Monitoring) system provides accurate, real-time glucose readings every five minutes for people with type 1 or type 2 diabetes[93]. CGM is a small wearable device that tracks the patient's glucose throughout the day and night, notifying her of highs and lows so she can take action. Dynamic glucose data can be accessed and shared safely and conveniently anywhere, anytime via smartphone or tablet. Family members or caregivers may have access to the patient's glucose data. With much richer, continuous glucose data, CGM helps to minimize the guesswork that comes from making decisions based solely on a number from a blood glucose meter reading. Vital Smith, a Korean startup, has developed an IoT solution called 'b bless' that can help infertile women check their ovulation by using their saliva and smartphone application[94].

Energy in Action: IoT technologies applied to the energy sector will increase efficiencies across the energy spectrum, from oil and gas to renewables like wind and solar. IoT systems are able to automate the collection and analysis of data from remote installations from the ocean floor to the gas pump on the corner. Real-time views of the operation of machinery in far-flung and isolated regions, energy companies can remotely monitor assets across the supply chain and even predict potential problems and costly failures before they happen. Upstream, midstream and downstream companies will be able to extract, refine and market more efficiently, and windfalls will be passed on to their customers. Data analytics will allow solar panels to be deployed more strategically than ever before, and real-time monitoring of assets – as we see in the following example – can be applied not only to wind turbines, but to utility companies who generate power from hydro, solar, wind, nuclear and fossil inputs.

Situated about 100 miles northwest of Los Angeles, California, the Tehachapi Pass in Kern County of the Tehachapi Mountains boasts the largest wind farm in the United States and the second largest in the world. The Alta Wind Energy Center, also known as Mojave Wind Farm, has 600 high-capacity wind turbines, generating 1,548 megawatts, which is enough electricity to power 250,000 homes. Engineers have worked hard to improve the mechanical efficiency of wind turbines as the turbines are quite expensive and a substantial sum of money needs to be invested (a typical wind turbine generating 1.5 MW costs about 2 million dollars). However, a real breakthrough comes from the use of IoT technology. GE developed a so-called 'Digital Wind Farm' where a dozen sensors attached to a wind turbine monitor everything from wind speed and direction to the speed of the blade tips, and send enormous amounts of data to the server[95].

GE also developed a software platform to use the data to optimize the operations of wind turbines on a real-time basis. Furthermore, turbines are connected with one another to communicate, coordinate, and adapt to changing conditions. Turbines are not dumb or isolated machines anymore. They are now smart and connected. Optimizing operations based on the immense data coming from turbine

sensors can increase power generation by 10 percent. Yet another 10 percent increase in power generation is achieved by using a simulation tool that allows the engineers to figure out the best configuration of each wind turbine for a given landscape and climate on the site.

Smart Manufacturing in Action: Smart, connected factories represent an estimated value of up to $1.95 trillion derived from increased productivity, energy savings, equipment maintenance, and inventory optimization[96]. For example, factories can use connected devices to reduce downtime as they constantly monitor machine performance to address issues before they become problematic.

Stanley Black & Decker, the world's largest tool manufacturer, has installed wireless network infrastructure to connect the factory floor in Mexico via an IoT system for increasing visibility and productivity and reducing manufacturing complexity. The results were more than anticipated: equipment effectiveness on the router production line rose 24 percent; immediate notification of issues made for faster decision making; labeling defects fell by 16 percent; and throughput increased by around 10 percent[97].

ThyssenKrupp Elevator created a connected, intelligent line of sensors that monitor millions of elevators around the world in real time, allowing the company to improve maintenance and building efficiency[98]. The King's Hawaiian company, which produces sweet dinner rolls, installed eleven new IoT connected machines. This capability enabled King's Hawaiian to put out an additional 180,000 pounds of bread every day. The machines were linked to manufacturing software that lets the company's employees have remote access to both historical and real-time data and features production dashboards that provide a comprehensive picture of the whole system so they can monitor performance. The new technology has increased efficiency, improved asset utilization, and lowered maintenance costs[99].

Smart Homes in Action: Some of the first IoT applications can be found in homes. Connected sensors enable people to easily monitor and control lamps, thermostats, ceiling fans, coffee makers, speakers, door locks, garage doors, ovens, etc. The data collected from those sensors can be analyzed to improve efficiency and ultimately quality of life.

Samsung SmartThings enables one mobile app and one hub to connect a wide range of smart devices manufactured by different companies. This capability allows the user to monitor and control all smart devices that are installed in her home without having to use multiple mobile apps[100]. Similarly, Amazon Echo and Google Home – voice-activated speakers that can also function as a digital assistant, playing music, answering questions, or checking your calendar – are becoming hubs that connect and control smart home devices[101].

Agricultural IoT in Action: IoT is changing how farming is managed. Farmers are now using connected sensors that will provide updates on soil composition, temperature, and water levels, ensuring efficient use of resources. For example, smart sensors that are embedded in the soil can measure moisture and PH levels. These sensors connected to irrigation and fertilizer systems can then apply just the right amount of fertilizer and water to ensure optimal conditions for the crops to grow. In addition, connected sensors will enable farmers to better monitor pest populations[102]. In the event a pest

population is reaching points where it is detrimental to crop yields, farmers can remotely release pheromones to control the pest population without using synthetic pesticides.

Hahn Family Wines uses sensor data and analytics to conserve resources by adding precision to watering and fertilizing at the company's 1,000-acre California vineyard[103]. An IoT gateway continuously monitors data from the various sensors in the vineyard and transmits it over a wireless network. Hahn can use this data to time and target its use of fungicide sprays to prevent disease and rotting, and can assess the need for watering, fertilizer, or other interventions.

Endnotes

[1] TESTIMONY OF INTEL CORP., June 28, 2016, Before the U.S. SENATE CMTE. ON COMMERCE, SCIENCE & TRANSPORTATION, SUBCMTE. ON SURFACE TRANSPORTATION AND MERCHANT MARINE INFRASTRUCTURE, SAFETY AND SECURITY, Hearing on "How the Internet of Things Can Bring U.S. Transportation Infrastructure into the 21st Century," available at https://www.commerce.senate.gov/public/_cache/files/46c728ce-377e-4060-9cac-55db2230ddf8/17D163EB418271C1D3BBC8D572D589EE.doug-davis-testimony.pdf.
[2] The President's National Security Telecommunications Advisory Committee, "NSTAC Report to the President on the Internet of Things," Nov. 19, 2014
[3] Goldman Sachs Global Investment Research, "The Internet of Things: Making sense of the next mega-trend," September 2014, available at http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf
[4] https://iot-analytics.com/iot-market-forecasts-overview/
[5] http://www.gartner.com/newsroom/id/3165317
[6] Quentin Hardy, "The Sensor-Rich, Data-Scooping Future," NYTIMES.COM, Apr. 26, 2015, available at http://bits.blogs.nytimes.com/2015/04/26/envisioning-a-future-when-sensors-are-scooping-up-data-on-everything/?_r=0.
[7] Emma Buckland, Margaret Ranken, Matt Arnott, and Pierce Owen, "IoT Global Forecast & Analysis 2015-25," Machina Research, August 2016
[8] James Manyika et al., "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, June 2015
[9] Joseph Bradley et al., "Internet of Everything: A $4.6 Trillion Public-Sector Opportunity," Cisco White Paper, 2013, available at http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf
[10] http://www.gartner.com/newsroom/id/2869521
[11] COMMENTS OF US CHAMBER OF COMMERCE, June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[12] Cisco, "Internet of Everything (IoE): Value at Stake in the IoE Economy," 2013, available at http://www.slideshare.net/fullscreen/CiscoIBSG/internet-of-everything-ioe-economy/1
[13] World Health Organization, "Hidden Cities: Unmasking and Overcoming Health Inequities in Urban Settings," The WHO Centre for Health Development, Kobe, and United Nations Human Settlements Programme (UN-HABITAT), 2010
[14] VERIZON'S COMMENTS, June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[15] Olesya Benedikt, "The Valuable Citizens of Smart Cities: The Case of Songdo City," Graduate Journal of Social Science, Vol. 12, Issue 2, pp. 17-36.
[16] http://www.ifez.go.kr/frt/biz/contents/CTS_0000000000000217/getContents.do
[17] IoT also has significant application in commercial fleet management, helping fleet operators comply with regulations requiring them to track driving behavior and hours. It enables companies to track, monitor, and manage their fleets efficiently and effectively through features such as onboard vehicle diagnostics, GPS tracking, and roadside assistance.
[18] http://www.autoconnectedcar.com/2016/03/bmw-connected-na-available-for-iphone-apple-watch-calculates-departure-time-texts-friends-finds-gasparking/
[19] AT&T, "Maersk Teams with AT&T to Track and Monitor Cold Shipping Containers," Press Release, September 29, 2015, available at http://about.att.com/story/maersk_teams_with_att_to_track_cold_shipping_containers.html
[20] Chris Murphy, "Internet Of Things: What's Holding Us Back," InformationWeek, May 5, 2014
[21] Michael Hickins, "Union Pacific Using Predictive Software to Reduce Train Derailments," The Wall Street Journal, Mar 30, 2012
[22] Manyika, James, et. al, "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey Global Institute, June 2015
[23] CommsWire Newsletters, No. 150701, 1 July 2015
[24] For instance, in September 2016, the 3GPP (The 3rd Generation Partnership Project) announced the completion of the initial Cellular Vehicle-to-Everything (C-V2X) standard. C-V2X will serve as the foundation for the connected vehicle of the future, giving vehicles the ability to communicate with each other, with pedestrians' devices, with roadside infrastructure and with the cellular network. How C-V2X will compete against the DSRC (Dedicated Short-Range Communications) standard remains to be seen as DSRC is likely to become mandated in the US for all light vehicles starting in 2020 model year.
[25] Open Connectivity Foundation, "Open Connectivity Foundation Brings Massive Scale to the IoT Ecosystem," Press Release, Feb. 19, 2016, available at https://openconnectivity.org/news/open-connectivity-foundation-brings-massive-scale-to-iot-ecosystem.
[26] http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VrLfonJf2Gk
[27] Ministry of Science, ICT, and Future Planning, South Korea, "IoT Information Security Roadmap," October 2014
[28] For connected car hacking, see https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, for medical device hacking, see http://www.medpagetoday.com/practicemanagement/informationtechnology/56566
[29] National Economic Council and Office of Science and Technology Policy, "A Strategy for American Innovation," October 2015
[30] https://www.whitehouse.gov/the-press-office/2016/09/26/fact-sheet-announcing-over-80-million-new-federal-investment-and
[31] In September 2015, the White House officially launched its Smart Cities Initiative, which encapsulates the U.S. government's efforts to support IoT and outlines $160 million in new and ongoing R&D funding. In September 2016, the White House updated and expanded its Smart Cities Initiative, with over $80 million in new Federal investments and a doubling of the number of participating cities and communities, exceeding 70 in total. These new investments and collaborations will help cities of all sizes, including in the key areas such as climate, transportation, public safety, and city services.

[32] Cyber Physical Systems Public Working Group, "Framework on Cyber-Physical Systems Release 1.0," May 2015, available at https://pages.nist.gov/cpspwg/
[33] MobileHealthNews, August 1, 2014; While the proposal requires the public comment period and other steps before enacted, the FDA said it would not enforce 510(k) requirements for the devices it listed and it doesn't expect companies making these devices to submit 510(k)s for them in the meantime. These devices include thermometers, smart body scales, stethoscopes, and ophthalmic cameras.
[34] White House, "Presidential Memorandum: Unleashing the Wireless Broadband Revolution," June 2010, available at https://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashingwireless-broadband-revolution
[35] U.S. Department of Transportation, "Federal Automated Vehicles Policy," September 2016, available at https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf
[36] http://www.govtech.com/fs/USSenateBillWouldLendFederalSupporttotheInternetofThings.html, March 2016
[37] Cho Mu-hyun, "South Korea to Invest $5b by 2020 in IoT and Smart Cars," ZDNet, March 25, 2015, available at http://www.zdnet.com/article/south-korea-toinvest-5b-by-2020-in-iot-and-smart-cars/
[38] The plan aims to foster a hyper-connected, digital revolution[38], and sets goals to grow the size of the domestic IoT market from 2 billion dollars in 2013 to about 30 billion dollars in 2020. Further, the plan seeks to increase the number of exporting SMEs from 70 in 2013 to 350 in 2020[38], and grow the number of jobs created from 2,700 in 2013 to 30,000 in 2020.
[39] The South Korean government also plans to raise transmit power for 900 megahertz, the commonly used bandwidth for IoT, from the current 10 megawatts up to 200 megawatts, which would help cut network costs by a third. It will also push for the supply of additional frequencies for IoT.
[40] Ministry of Science, ICT, and Future Planning, South Korea, "IoT Information Security Roadmap," October 2014
[41] Yonhap News, "IoT Security Alliance Launches with 40 Companies Participating," June 18, 2015
[42] Yonhap News, "Regulations on IoT industry will be eased," May 18, 2016; On a macro-level, the Korean government has been trying to remove regulations across all industries and sectors that are obsolete, unnecessary, or counter-productive. According to the Office for Government Policy Coordination, the South Korean government scrapped or improved 3,992 regulatory measures out of a total 14,600 during the period from March 2014 to December 2015.
[43] Yonhap News, "S. Korea decides to ease regulations on drones, biotech, autonomous vehicles," May 18, 2016; The panel on investment in new industries, affiliated with the Office for Government Policy Coordination, had received 151 deregulation recommendations from business associations. The government decided to address 141 of them.
[44] Stewart Eisenhart, "Korean Regulators Waive Registration Requirements for Some Mobile Medical Devices," Emergo Group, March 18, 2014, available at www.emergogroup.com/blog/2014/03/korean-regulators-waive-registration-requirements-some-mobile-medical-devices
[45] Ministry of Science, ICT, and Future Planning, South Korea, "Master Plan for Building the Internet of Things that Leads the Hyper-Connected, Digital Revolution," May 2014, available at http://www.kiot.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf
[46] Peter Singer, "Federally Supported Innovations: 22 Examples of Major Technology Advances That Stem From Federal Research Support," Information Technology and Innovation Foundation, February 2014, available at http://www2.itif.org/2014-federally-supported-innovations.pdf
[47] COMMENTS OF Samsung., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[48] Baltimore Sun, "Medical Device Approval Plagued by Unhealthy Delays," February 24, 2011
[49] Daniel Castro & Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," New Center for Data Innovation, December 4, 2014
[50] Federal Trade Commission, "Staff Report, Internet of Things: Privacy & Security in a Connected World," January 2015
[51] COMMENTS OF Samsung., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[52] For example, in the Joint Explanatory Statement of the US Congress Conference Committee accompanying the 2015 US transportation funding law, the Fixing America's Surface Transportation Act (FAST Act), Congress stated: "The FAST Act ensures that these [Department of Transportation] programs are implemented and Intelligent Transportation Systems (ITS) are deployed in a technology neutral manner. The Act promotes technology neutral policies that accelerate vehicle and transportation safety research, development and deployment by promoting innovation and competitive market-based outcomes, while using federal funds efficiently and leveraging private sector investment across the automotive, transportation and technology sectors."
[53] COMMENTS OF Qualcomm., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[54] Robert Atkinson, "ICT Innovation Policy in China: A Review," Information Technology and Innovation Foundation, July 2014, available at http://www2.itif.org/2014-china-ict.pdf
[55] For example, when mandated IoT identifiers are inconsistent between countries, providers will have to create a country-specific version of each device. As a result, devices will be difficult or expensive to use across geographic regions.
[56] Quentin Hardy, "The Sensor-Rich, Data-Scooping Future," NYTIMES.COM, Apr. 26, 2015
[57] COMMENTS OF CISCO SYSTEMS, INC., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[58] COMMENTS OF CISCO SYSTEMS, INC., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[59] VERIZON'S COMMENTS, June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[60] http://www.mobileworldlive.com/asia/asia-news/skt-unveils-pricing-for-lora-based-iot-services/

[61] Scott Hogg, "ARIN Finally Runs Out of IPv4 Addresses," Network World (Sept. 22, 2015), available at http://www.networkworld.com/article/2985340/ipv6/arin-finally-runs-out-of-ipv4-addresses.html
[62] NTIA, IPv6 Task Force, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)," Jan. 2006, available at https://www.ntia.doc.gov/files/ntia/publications/ipv6final.pdf
[63] James Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey Global Institute, June 2015
[64] Microsoft's Response., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[65] COMMENTS OF Samsung., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[66] Federal Trade Commission, "Staff Report, Internet of Things: Privacy & Security in a Connected World," January 2015, available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[67] COMMENTS OF US CHAMBER OF COMMERCE, June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[68] COMMENTS OF GM, June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[69] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Feb. 12, 2014.
[70] Federal Trade Commission, "Staff Report, Internet of Things: Privacy & Security in a Connected World," January 2015
[71] Brill, Julie, "The Internet of Things: Building Trust and Maximising Benefits Through Consumer Control," 89 Fordham L. Rev. 205, 2014
[72] COMMENTS OF Huawei., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[73] Data privacy also requires cross-border coordination. The U.S. or South Korea cannot act in isolation and must coordinate with its international partners as different countries have different approaches to protecting data privacy. For example, the EU takes a horizontal approach to data protections, whereas the U.S. approach is built around specific verticals involving highly sensitive data. An inconsistent patchwork of global regulations relating to data sovereignty will impede IoT innovation.
[74] Daniel Castro & Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things," New Center for Data Innovation, December 4, 2014
[75] Josh Taylor, "Chicago's smart city: From open data to rat control," ZD Net, October 15, 2014, available at http://www.zdnet.com/chicagos-smart-city-from-open-data-to-rat-control-7000034726/
[76] VERIZON'S COMMENTS, June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[77] Cross-border data flow should be restricted only to the extent necessary to achieve legitimate regulatory objectives.
[78] COMMENTS OF Samsung., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[79] Joshua New & Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015
[80] *Ibid*.
[81] Government of India, Ministry of Communications and Information Technology, "National Telecom M2M Roadmap," May 2015
[82] World Bank, "ICT for Greater Development Impact," June 2012
[83] TESTIMONY OF INTEL CORP., Feb. 11, 2015, Before the U.S. SENATE CMTE. ON COMMERCE, SCIENCE & TRANSPORTATION, Hearing on "The Connected World; Examining the Internet of Things," available at https://www.commerce.senate.gov/public/_cache/files/c88aece5-8769-4afd-8c51-81c69d961cb9/A2366CDD7FCB7ADAB70148A549B3614E.doug-davis---intel---prepared-statement-for-the-record-february-11-2015.pdf
[84] Ibid.
[85] Microsoft's Response., June 2, 2016, Before the NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION DEPARTMENT OF COMMERCE Washington, D.C. 20230, Docket No. 160331306-6306-01, April 2016
[86] In May 2016, the Public Working Group released the Framework on Cyber-Physical Systems[86], which provides a comprehensive tool for the analysis and description of Cyber-Physical Systems to promote exchanging ideas and integrating research across sectors.
[87] http://www.govtech.com/fs/USSenateBillWouldLendFederalSupporttotheInternetofThings.html, March 2016
[88] Kansas City Living Lab, http://kclivinglab.com/
[89] https://www.qualcomm.com/news/releases/2014/06/11/qualcomm-ch2m-hill-and-city-cincinnati-collaborate-integrated-water
[90] Microsoft, "Moving from Insight to Action with Azure IoT Services," available at https://www.microsoft.com/en-us/server-cloud/customer-stories/rockwell-automation.aspx.
[91] Verizon, "State of the Market: Internet of Things 2016," April 2016, available at https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf
[92] Brian Dolan, "Study: GlowCaps Up Adherence to 98 Percent," Mobi Health News, June 23, 2010, available at http://www.mobihealthnews.com/8069/study-glowcaps-up-adherence-to-98-percent
[93] https://www.dexcom.com
[94] http://seoulspace.co.kr/2016/08/24/korean-startup-vital-smith-one-of-four-finalists-of-grants4apps-accelerator-2016/
[95] Stacey Higginbotham, "GE Uses Holograms and the Industrial Internet to Make Wind Farms 20% More Efficient," Fortune, May 19, 2015, available at http://fortune.com/2015/05/19/ge-holograms-wind/

[96] Cisco, “Internet of Everything (IoE): Value at Stake in the IoE Economy,” 2013, available at http://www.slideshare.net/fullscreen/CiscoIBSG/internet-of-everything-ioe-economy/1
[97] http://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-factory/automation/stanley-black-decker.html
[98] Microsoft, “Giving the World’s Cities a Lift with IoT,” available at https://www.microsoft.com/en-us/servercloud/customer-stories/Thyssen-Krupp-Elevator.aspx.
[99] Kylie J. Wakefield, “How The Internet of Things Is Transforming Manufacturing,” Forbes, July 1, 2014, available at http://www.forbes.com/sites/ptc/2014/07/01/how-the-internet-of-things-is-transforming-manufacturing/#1e76c898228e
[100] https://www.smartthings.com/how-it-works
[101] http://www.zdnet.com/article/amazon-echo-and-google-home-where-the-real-battleground-lies/
[102] Neiger, Chris. “The Internet of Things Is Changing How Your Food Is Grown -- and That's a Good Thing,” Motley Fool. December. 12, 2014
[103] Stacey Higginbotham, “Inside Verizon's big plans for the Internet of things,” Fortune, October 28, 2015, available at http://fortune.com/2015/10/28/verizon-internet-of-things/