June 2, 2016

Attn: IOT RFC 2016
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

On behalf of the Center for Data Innovation (datainnovation.org), we are pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comments on the benefits, challenges, and potential roles for the government in fostering advancement of the Internet of Things.[1]

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. With staff in Washington, DC and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation.

[1] https://www.federalregister.gov/articles/2016/04/06/2016-07892/the-benefits-challenges-and-potential-roles-for-the-government-in-fostering-the-advancement-of-the

The Internet of Things offers many opportunities to grow the economy and improve quality of life. Just as the public sector was instrumental in enabling the development and deployment of the Internet, it should play a similar role to ensure the success of the Internet of Things by addressing challenges the private sector alone cannot solve. In this submission, we identify a wide variety of these opportunities and challenges. In addition, we offer recommendations on how the government should support the development of the Internet of Things to ensure that it develops rapidly, securely, and cohesively; that consumers and businesses do not face barriers to adoption; and that both the private and public sector can take full advantage of the coming wave of smart devices.

Please find our responses to the relevant questions in the attached document.

Sincerely,

Daniel Castro
Director
Center for Data Innovation
dcastro@datainnovation.org

Joshua New
Policy Analyst
Center for Data Innovation
jnew@datainnovation.org


CENTER
FOR
DATA
INNOVATION

GENERAL

1. ARE THE CHALLENGES AND OPPORTUNITIES ARISING FROM THE INTERNET OF THINGS (IOT) SIMILAR TO THOSE THAT GOVERNMENTS AND SOCIETIES HAVE PREVIOUSLY ADDRESSED WITH EXISTING TECHNOLOGIES, OR ARE THEY DIFFERENT, AND IF SO, HOW?

Many of the challenges and opportunities associated with the Internet of Things apply to existing technologies to at least some degree, but the unique characteristics of the Internet of Things will reshape some of these issues to the point that new ways of thinking may be necessary.

For example, while many government agencies already use sensors to collect important data, the amount of data that they will collect from these sources in the future will be substantially greater. Better data will unlock new capabilities and new challenges that these organizations will need to manage. The National Oceanic and Atmospheric Administration (NOAA) provides a clear example of this trend. NOAA has long recognized the value of combining data from satellites with data from environmental monitoring stations on the ground and at sea. But now, as it becomes feasible to install and monitor environmental sensors with much higher penetration and granularity across the planet, the resolution and accuracy of weather monitoring and forecasting can increase substantially as well as lead to unprecedented insights into climate change and other environmental challenges.[1] This augmented weather monitoring capacity will likely have a substantial impact on a wide variety of economic and social issues, including resource and environmental management, transportation planning, natural disaster response, and insurance pricing.[2] Thus it is imperative for NOAA, and related federal agencies, to consider how they should reshape their operations to fully capitalize on the potential of data from the Internet of Things.

However, the Internet of Things is still an emerging set of technologies and while industry forecasters and technologists can imagine its potential applications and estimate its impact, there is simply no way to predict all of or even most of the most of the opportunities that the Internet of Things will create as it matures.[3] The Internet of Things will be an enormously disruptive platform for innovation and attempting to define the nature and scope of the issues that will arise in the future would be akin to attempting to predict the full social and economic impact of the Internet shortly after the launch of the World Wide Web in 1991.

A. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

Smart devices can have a number of properties that make them more useful and convenient, but also make them a greater security risk. For example, mobile devices may use low-power processors to conserve battery power, which limits the device's ability to perform computationally complex operations, such as encrypting data.

Many IoT applications will be transmitting large amounts of data across long distances which can present challenges in rural areas without reliable connectivity, such as sensor networks dispersed through miles of farmland to support precision agriculture applications. Similarly, in areas densely populated with transmitting devices, the volume of data being transmitted and sheer number of wireless connections may surpass the capacity of existing spectrum available to the private sector.

B. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?

The private sector is capable of effectively developing most technologies on its own, but the Internet of Things is subject to an array of market failures–challenges the private sector acting alone cannot overcome quickly or effectively–that could limit these incentives and thus slow progress toward a fully connected world. These market failures include: externalities, particularly network and competitiveness externalities; "chicken-and-egg" dynamics; risk and uncertainty; interoperability; and public goods (resources that the private sector cannot supply in sufficient quantities on its own, namely spectrum, human capital, and R&D funding).[4]

Additionally, many existing regulatory frameworks and approaches are not well suited to governing the Internet of Things and will make deploying these technologies more expensive and less valuable. For example, in the past, a company making a device for a car may have worked with a single government agency, but now a company developing connected devices for cars could very well be subject to confusing, overlapping, or inconsistent frameworks from a consumer protection regulator, a transportation safety regulator, and a spectrum regulator, among others.[5] Similarly, many consumer protection regulations, particularly as they relate to privacy, make little sense to apply to the Internet of Things for a variety of reasons. For example, much of the data collected by IoT applications will be benign and many devices will not have user interfaces, making current notification and consent requirements designed for browsing the Internet cumbersome and obsolete.[6]

Furthermore, the Internet of Things can be a valuable tool to help meet the needs of underserved populations, but without appropriate public policies such as ensuring that

smart city technologies serve all cities and neighborhoods rather than just affluent ones, adoption will be uneven. Failure to achieve equitable adoption rates across all demographics will limit the value of such systems as a whole because of the network effects that widespread deployments generate. For example, smart city technology that police departments use to reduce crime would be substantially less effective if they could only analyze data from certain neighborhoods. As the world increasingly relies on data to improve services such as health care, education, and finance, the potential harm of being underrepresented or excluded in the data that drives this decision-making also increases.[7] The Internet of Things offers a valuable opportunity to close this divide. Low-cost sensor technologies and networked services empower underserved populations to more easily provide data that is useful for improving their quality of life. However, this can only happen if governments and the private sector invest in and deploy these technologies equitably. If the public sector does not implement policies to encourage equitable deployment, the Internet of Things could exacerbate existing inequalities by providing the benefits of data-driven decision-making only to some, and placing already underserved communities at an even greater disadvantage.[8]

C. What are the most significant new opportunities and/or benefits created by the Internet of Things, be they technological, policy, or economic?

There are countless opportunities for the Internet of Things to deliver substantial economic and social benefits to the public and private sectors alike. It is difficult to rank the value of these opportunities, but they include: improving disaster response efforts by protecting first responders, minimizing damages, and even helping to avoid disasters entirely; making public and private spaces substantially more accessible for people with disabilities; increasing the productivity of the manufacturing sector; improving resource conservation, particularly

energy and water; making supply chains more efficient and transparent; and making government services more effective and efficient.[9]

Overall, the Internet of Things will allow for every aspect of society and the economy to have a digital layer, and the data that these networks will generate will offer unprecedented insight into how the world works. Given that the Internet of Things is still in its infancy, there is likely no telling what the most beneficial applications of the Internet of Things will be until it matures.

2. THE TERM "INTERNET OF THINGS" AND RELATED CONCEPTS HAVE BEEN DEFINED BY MULTIPLE ORGANIZATIONS, INCLUDING PARTS OF THE U.S. GOVERNMENT SUCH AS NIST AND THE FTC, THROUGH POLICY BRIEFS AND REFERENCE ARCHITECTURES. WHAT DEFINITION(S) SHOULD WE USE IN EXAMINING THE IOT LANDSCAPE AND WHY? WHAT IS AT STAKE IN THE DIFFERENCES BETWEEN DEFINITIONS OF IOT? WHAT ARE THE STRENGTHS AND LIMITATIONS, IF ANY, ASSOCIATED WITH THESE DEFINITIONS?

Definitions are important, but they also evolve over time. The Center for Data Innovation uses the following definition: "The Internet of Things is a term used to describe the set of physical objects embedded with sensors or actuators and connected to a network." This definition distinguishes the key characteristics about what makes an object part of the Internet of Things, i.e. it is an object with the ability to communicate (i.e. connected to a network) and collect data (i.e. sensors), act on its environment (i.e. actuators), or both.

3. WITH RESPECT TO CURRENT OR PLANNED LAWS, REGULATIONS, AND/OR POLICIES THAT APPLY TO IOT:

A. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?

In January 2015 FDA issued draft guidance exempting low risk devices from regulatory oversight in certain conditions.[10] For example, connected devices that collect health data, such as a fitness tracker, will not be subject to regulatory scrutiny provided that they only function to promote healthy behavior, and not diagnose or treat a specific disease.[11] Additionally, in February 2015, FDA finalized guidance exempting medical device data systems–connected devices that store, transfer, display, or convert medical data—from regulatory oversight.[12]

The FCC has undertaken a number of proceedings to make additional wireless spectrum available for commercial use. While these efforts are not specifically aimed at the Internet of Things, additional spectrum, including licensed, unlicensed, and blended access models, will facilitate cheaper, more abundant connectivity that will support a broad array of connected technologies. The 2015 AWS-3 auction made $44.9 billion of licensed, flexible-use spectrum bands available to wireless network operators; FCC is working to improve rules governing access to the 5 gigahertz (GHz) band and made considerable in progress to ease access to an additional 100 megahertz (MHz) of unlicensed spectrum; FCC is experimenting with new model of spectrum access for the 3.5 GHz band to better coordinate licensed and unlicensed users, the ongoing 600 MHz incentive auction will allow television broadcasters to sell their rights to these spectrum bands to wireless providers, and FCC is exploring how to free up more high-band spectrum above 24 GHz, which is expected to be an important component for next generation 5G networks.[13]

B. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

There are both existing and planned regulatory actions, particularly related to consumer protection issues, that will substantially hinder the growth of the Internet of Things.

The FTC has expressed support for requiring the practice of data minimization for data generated by the Internet of Things—limiting the collection and retention of data so it can only fulfill specific, predefined purposes.[14] Applying such rules to the Internet of Things would be damaging as there may be one primary reason to collect data, but innumerable other ways to use the same data beneficially beyond its initial purpose. And, with so many new opportunities to collect data from billions of new connected devices, the value of the data at stake is proportionately large. Furthermore, mandating data minimization practices can preclude opportunities for de-identification, which can protect sensitive information without unnecessarily sacrificing its value.[15] Similarly, applying existing notification and consent rules to devices that gather consumer data on the Internet to the Internet of Things would be damaging because many connected devices will have limited, if any, user interfaces.[16] Outdated notification requirements will prove particularly frustrating given that the vast majority of applications on the Internet of Things pose no real threat to consumer welfare and most data collection would likely be routine and insignificant. Any costs incurred by adhering to these regulations would be passed on to consumers and ultimately serve to make consumers less likely to adopt connected devices.

Overall, federal regulators appear far more concerned with minimizing the potential harms of the Internet of Things rather than maximizing the benefits of the technology. For example, in 2012, the FTC filed suit against Nomi Technologies, a company that develops retail IoT applications, despite no evidence that any consumers were harmed by Nomi's

actions (failure to provide an in-store method for shoppers to opt-out of its anonymous tracking technology, even though Nomi did provide an opt-out method on its website).[17] Nomi was in the wrong, but FTC's decision failed to weigh the tangible economic and consumer-empowering benefits of the company's technology against the hypothetical harm it caused.[18] And in 2015, FTC released a report on the Internet of Things that called for broad-based privacy legislation and endorsed data minimization, but failed to acknowledge the need to carefully weigh the benefits of IoT when shaping regulation.[19] This approach substantially limits the growth of the Internet of Things as private companies will be less willing to experiment with the technology if they fear they could be punished without evidence they actually harmed consumers.

4. ARE THERE WAYS TO DIVIDE OR CLASSIFY THE IOT LANDSCAPE TO IMPROVE THE PRECISION WITH WHICH PUBLIC POLICY ISSUES ARE DISCUSSED? IF SO, WHAT ARE THEY, AND WHAT ARE THE BENEFITS OR LIMITATIONS OF USING SUCH CLASSIFICATIONS? EXAMPLES OF POSSIBLE CLASSIFICATIONS OF IOT COULD INCLUDE: CONSUMER VS. INDUSTRIAL; PUBLIC VS. PRIVATE; DEVICE-TO-DEVICE VS. HUMAN INTERFACING.

There is a need to provide broad government support for the Internet of Things through a comprehensive national strategy.[20] However, there are also some unique policy issues that affect particular IoT applications for consumers, municipal governments, the agricultural industry, the military, and so on. Thus, it is not productive to treat every concern as universally relevant. Regardless of the merits of different classification schema, they should support narrow, targeted approaches to regulation to avoid unnecessarily restricting the growth of the technology as a whole.

5. PLEASE PROVIDE INFORMATION ON ANY CURRENT (OR CONCLUDED) INITIATIVES OR RESEARCH OF SIGNIFICANCE THAT HAVE EXAMINED OR MADE IMPORTANT STRIDES IN

UNDERSTANDING THE IOT POLICY LANDSCAPE. WHY DO YOU FIND THIS WORK TO BE SIGNIFICANT?

There are a number of concluded and ongoing initiatives that have advanced understanding of the technical, security, and connectivity considerations of the Internet of Things, which will help provide policymakers with the knowledge necessary to craft regulations and legislation regarding the Internet of Things.

In 2015, the National Institute of Standards and Technology (NIST) published its draft Framework for Cyber-Physical Systems, which provides comprehensive technical information, definitions, and taxonomies related to five categories of issues related to the Internet of Things: reference architecture, cybersecurity and privacy, timing and synchronization, data interoperability, and use cases.[21] Once NIST incorporates public feedback on the draft framework, it will use the framework to help guide action plans to solve a variety of technical challenges associated with the Internet of Things.[22] For cybersecurity specifically, NIST also published its Framework for Improving Critical Infrastructure Cybersecurity in early 2014.[23] Though its focus is far broader than just the Internet of Things, it provides valuable recommendations and cybersecurity best practices that apply to all connected technologies. In May 2016, NIST released the second draft of its Systems Security Engineering, which provides additional technical guidance for securing connected technologies.[24] For sector-specific issues, NIST published extensive guidelines for smart grid cybersecurity in 2014, and the Federal Communication Commission (FCC) published a whitepaper in December 2015 detailing the technical considerations of cybersecurity for consumer IoT devices.[25]

To promote interoperability, in September 2015, NIST published its Big Data Interoperability Framework, which provides exhaustive technical and taxonomical information as well as

standards information for data technologies, particularly the Internet of Things.[26] NIST has also published the third iteration of its Framework and Roadmap for Smart Grid Interoperability Standards, and is currently developing its IoT-Enabled Smart City Framework.[27] Additionally, the Department of Transportation's Intelligent Transportation Systems (ITS) Standards Program, which focuses heavily on connected vehicles and infrastructure, is conducting a variety of activities to support interoperable ITS standards and architectures, including testing, providing technical assistance to local and state stakeholders, and developing deployment guidance.[28]

There are several ongoing initiatives that will help advance understanding on the policy implications of IoT specifically.

In early 2016, the U.S. House of Representatives and U.S. Senate introduced the bipartisan Developing Innovation and Growing the Internet of Things (DIGIT) Act, which would direct the Secretary of Commerce to establish a working group of government, industry, consumer, and civil society stakeholders to report on policies and practices that hinder IoT development, propose policies to improve federal agency coordination on IoT issues, and identify opportunities for federal agencies to make better use of the Internet of Things.[29] Additionally, the DIGIT Act would direct the FCC to report on the current and future spectrum needs of the Internet of Things and provide recommendations to overcome any relevant regulatory barriers.[30] The DIGIT Act was introduced following 2015 House and Senate resolutions that acknowledged the potential benefits of the Internet of Things and called for the development of a national strategy to support the technology.[31]

In early 2015, bipartisan members of the House of Representatives launched the Congressional Internet of Things Caucus to study the Internet of Things and educate members of Congress on its policy implications.[32] Similarly, in May 2016, 19 members of the House Energy and Commerce Committee formed a working group on the Internet of Things that will also focus on member education, as well as investigate the ideal role the government should play to advance the development of the technology, and will report on their findings by the end of 2016.[33]

The DIGIT Act and Congressional efforts to study IoT and promote member education are very important steps towards ensuring the government proactively works to accelerate the growth of the technology. As many of the opportunities presented by IoT are unprecedented, educating policymakers about these opportunities, defining the appropriate level of government involvement and determining the specific actions government should take will be instrumental in ensuring the Internet of Things grows rapidly, that the private sector does not face barriers to deployment, and that the United States can fully capture the social and economic benefits generated by the technology.

The Center for Data Innovation has also published several reports that examine the unique policy considerations of the Internet of Things and provide recommendations for policymakers focused on maximizing the benefits of the technology. These reports detail the need for a national IoT strategy, offer a set of policy principles to promote IoT adoption, and providing an overview of the impact of the technology across multiple sectors.[34] The Center will soon publish two additional reports on IoT later this summer: one assessing the extent to which the federal government is adopting IoT and one looking at the opportunity to use IoT to improve accessibility for people with disabilities.

TECHNOLOGY

6. WHAT TECHNOLOGICAL ISSUES MAY HINDER THE DEVELOPMENT OF IOT, IF ANY?

A. Examples of possible technical issues could include: i. Interoperability; ii. Insufficient/contradictory/proprietary standards/platforms; iii. Spectrum availability and potential congestion/interference; iv. Availability of network infrastructure; v. Other.

For the Internet of Things to develop rapidly, cohesively, and be maximally beneficial for consumers, businesses, and government, several technological challenges will have to be addressed by the public and private sectors. These include interoperability, spectrum availability, and connectivity. For government use of the Internet of Things, agencies may lack a modern technological infrastructure to store and process streaming data which would limit their ability to integrate IoT devices.

B. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

The government can and should work to help mitigate these challenges, most significantly by acting as a convener of private sector stakeholders. For standards and interoperability issues, industry should be allowed to lead development of these standards and reach consensus, but the government can promote communication and collaboration between firms across multiple verticals on the national and international levels to accelerate this process.

The government should also actively push back against the efforts of other countries to establish nation-specific standards for the Internet of Things, as this would fragment and slow the growth of the technology. As a network technology, the value of many Internet of

Things applications increases with scale, so limiting the number of devices in a network based on national borders limits the value of the technology as a whole, thus reducing incentives for investment and adoption.[35]

The FCC has already taken steps to free up additional spectrum and has plans to continue to do so in the future. However, the government should nonetheless actively monitor the spectrum needs of IoT as it develops and work to proactively identify and address bottlenecks before they arise.

ECONOMY

11. SHOULD THE GOVERNMENT QUANTIFY AND MEASURE THE IOT SECTOR? IF SO, HOW?

Measuring the IoT sector would be valuable and should be a priority. Since the Internet of Things includes a broad array of both physical goods and information, any efforts to do so must examine IT use as a whole. For example, a metric that simply indicates the number of connected devices sold does not capture the value of the data these devices generate, the new products build with the resulting data, or the efficiency and productivity gains this data can offer a company. One possible solution would be to expand the Census Bureau's E-Commerce Statistics (E-STATS) program, which is tasked with "measuring the electronic economy," to collect and report data on IT spending, which would include IoT hardware and analytics services, on an enterprise level.[36] Federal agencies should also be asked to report, at least annually, on their use of the Internet of Things.

12. SHOULD THE GOVERNMENT MEASURE THE ECONOMIC IMPACT OF IOT? IF SO, HOW?

B. Does IoT create unique challenges for impact measurement?

Measuring the impact of the Internet of Things is important to understand which areas of the economy are successfully adopting the technology and which ones are not. The U.S. government should consider some of the work done by the European Commission to measure the value-added of data reuse and better understand the "data value chain."

13. WHAT IMPACT WILL THE PROLIFERATION OF IOT HAVE ON INDUSTRIAL PRACTICES, FOR EXAMPLE, ADVANCED MANUFACTURING, SUPPLY CHAINS, OR AGRICULTURE?

A. What will be the benefits, if any?

The Internet of Things will generate data that helps companies make more informed decisions, which in turn improves efficiency, productivity, management, quality control, and essentially every other industrial practice, regardless of the industry. For example, Raytheon operates an advanced manufacturing facility with robotic assembly lines that automatically track every time a screw is turned.[37] Should this system detect an anomaly, it will automatically halt production of that component and warn factory operators, which can prevent distribution of a faulty product or help identify malfunctioning manufacturing equipment, which could then be repaired before it breaks and cause costly downtime.[38] In agriculture, networks of soil moisture sensors can help farmers reduce water consumption by allowing them to target just the areas of their field that need water, environmental sensors can help farmers make more informed planting and harvesting decisions, and sensors that monitor farming equipment performance can warn farmers if they need to perform preventative maintenance rather than pay for expensive repairs should the equipment break down. With more, better, and real-time data about every step of industrial processes, any company in any industry stands to gain substantially.

One particularly interesting impact IoT will have on industry is allowing business model innovation, particularly by allowing products to be sold as a service. For example, rather than just selling a jet engine to an airline, a manufacturer could adopt a product-as-a-service business model so that it sells the engine's function (i.e. providing thrust for flight) as a service, but retains ownership of the engine, billing the customer based on use as indicated by sensors on the engine.[39] Though this entails manufacturers assuming more risk, it can lower the investment barrier for their customers and lead to market expansion.[40] Additionally, connected devices can generate valuable data about their performance and how they are used after they are purchased which, if manufactures can access this data, could allow manufactures to better understand their customers' needs and improve their products.[41]

Supply chains, which all industries rely upon, also stand to benefit substantially from the Internet of Things. Sensors that record every stage of a supply chain, such as the harvesting of raw material, international shipping, and customs inspections, allow for unprecedented insight into the flow of goods and materials. This can promote transparency into international markets, which can reduce costs, streamline regulatory compliance, and allow companies to make better planning decisions, which not only benefits those companies directly but also has secondary benefits for the competitiveness of an economy as a whole.[42]

B. What will be the challenges, if any?

For industry to realize any of these benefits, companies need to be able to rapidly deploy and use the Internet of Things and act upon the data generated by smart devices. For example, if consumer protection regulations prevent a consumer IoT manufacturer from

accessing performance data from devices after consumers purchase them, they will be substantially limited in their ability to understand their products' shortcomings or develop improvements for future designs. And farmers will not be willing to invest in IoT applications if they live in areas without reliable connectivity, as connected devices will not be able to transmit and receive data.

There is also a considerable competitiveness externality that substantially affects industries ability to adopt the Internet of Things. Countries home to companies well-positioned to produce billions of new connected devices, develop software to run them, and apply analytics to generate value from the data they generate will have a competitive advantage over other countries. Similarly, given the efficiency and productivity gains the technology can offer the private sector, countries that readily adopt and implement the Internet of Things will gain a competitive edge over those that do not. While business actions can improve an individual firm's competitiveness, everyone, not just the individual firm, shares in the benefits of a national economy that is more competitive overall.[43] But the drawbacks of an uncompetitive economy work the same way: if a country is not well-positioned to develop or adopt the Internet of Things, its national economy will be less competitive overall and individual businesses can be at a relative disadvantage in the global marketplace. For example, an importer that implements connected technologies to improve the efficiency of its international supply chains and reduce overhead costs will increase the overall competitiveness of domestic companies that can purchase imported goods at resulting lower prices.[44] Conversely, companies in a country slower to adopt this technology, through no fault of their own, will find themselves at a competitive disadvantage as a result of comparatively sluggish supply chains.

Additionally, no industry will be able to take advantage of the Internet of Things without employees equipped with the skills necessary to work with the data the Internet of Things generates. By 2018, the United States will face a shortage of up to 190,000 workers well-educated in data science and 1.5 million managers and analysts able to use data to make better decisions.[45] Similarly, a survey of 497 businesses in the China, France, Germany, India, the United Kingdom, and the United States revealed that this shortage of skilled data workers is a universal concern, with only one-third of companies reporting they have the human capital necessary to effectively use new data.[46] While business can and do supply supplementary training for employees, no company can cultivate the necessary amount of human capital necessary to fully capture the benefits of the Internet of Things.

C. What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?

The federal government should actively pursue policies that reduce barriers to IoT adoption and deployment, that support the free flow and exchange of data, and that encourage government to be an early adopter of the Internet of Things to ensure the government does not act as a bottleneck to private sector IoT use. Examples of such policies are described throughout this filing.

14. WHAT IMPACT (POSITIVE OR NEGATIVE) MIGHT THE GROWTH OF IOT HAVE ON THE U.S. WORKFORCE? WHAT ARE THE POTENTIAL BENEFITS OF IOT FOR EMPLOYEES AND/OR EMPLOYERS? WHAT ROLE OR ACTIONS SHOULD THE GOVERNMENT TAKE IN RESPONSE TO WORKFORCE CHALLENGES RAISED BY IOT, IF ANY?

As described in response to question 13-B, there is a pressing need for workers with data skills, and the need will only increase as the Internet of Things proliferates. In order to

ensure that the U.S. workforce remains competitive, the government should support the cultivation of data science skills in high school and higher education.

POLICY ISSUES

15. WHAT ARE THE MAIN POLICY ISSUES THAT AFFECT OR ARE AFFECTED BY IOT? HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO THESE ISSUES?

The main policy issues that affect or are affected by IoT include consumer protection, data access and use, regulatory oversight, education, spectrum and connectivity, competition and trade, and equity. These and other issues, as well as recommendations for the government, are detailed throughout this filing.

16. HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO CYBERSECURITY CONCERNS ABOUT IOT?

C. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

The government should continue to research the cybersecurity implications of IoT and provide guidance, such as NIST's cybersecurity and cyber-physical systems frameworks. And, while the government should work to convene stakeholders to advance adoption of robust cybersecurity standards and best practices, it should allow industry itself to develop these standards.

17. HOW SHOULD THE GOVERNMENT ADDRESS OR RESPOND TO PRIVACY CONCERNS ABOUT IOT?

A. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

Though the Internet of Things allows for the collection of unprecedented amounts of data, this does not necessarily mean it poses novel or alarming privacy risks. Not only will much of the data collected by consumer-facing devices be benign, changing social norms, market forces, existing rules, and other factors will impose controls that limit undesirable uses of data without the need for new regulation. It is important for the government to recognize that many privacy concerns raised about the Internet of Things today are speculative and overblown, and will likely have little bearing on the actual harms warranting new rules or regulations that will materialize as the technology develops.[47] Additionally, even if some advocacy groups can conceive of hypothetical privacy concerns, regulators should be careful to recognize that these concerns are just that—hypothetical. Establishing privacy rules based on speculative fears, without evidence that consumers are actually experiencing concrete harm, would substantially restrict the potential beneficial applications of the Internet of Things and limit its growth. For example, privacy activists raised objections when several cities made plans to install gunshot detection sensor networks in public spaces.[48] However, the effectiveness of these technologies in reducing gun crime has proven to be valuable to law enforcement, and none of the privacy fears raised have materialized.[49]

C. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

As the Internet of Things is still emerging, the federal government should be cautious when considering impose new rules or restrictions that could limit the technology's growth or have other unintended consequences. In general, the government should wait until unsubstantiated privacy fears subside and market forces and changing social norms can

reveal what legitimate consumer privacy issues should be addressed, if any, as the technology matures.

As with cybersecurity, industry-led best practices for privacy should be sufficient to address the majority of the privacy challenges presented by IoT. And importantly, when privacy concerns do arise, regulators have a responsibility to perform a cost-benefit analysis that considers whether the benefits of a practice—to consumers or competition—outweigh any harms.[50] But if actual evidence of consumer harms materializes and rules to protect consumers' privacy are necessary, regulators should act quickly to enact narrow and targeted protections.[51]

19. IN WHAT WAYS COULD IOT AFFECT AND BE AFFECTED BY QUESTIONS OF ECONOMIC EQUITY?

The Internet of Things poses substantial opportunity to address economic inequities by providing an inexpensive and effective method of ensuring underserved populations can participate in and benefit from an increasingly data-driven world. However, without government action to ensure the equitable deployment of these technologies, IoT risks exacerbating these disparities.[52] For a more detailed explanation, see the answer to question 1-B.

INTERNATIONAL ENGAGEMENT

23. ARE THERE POLICIES THAT THE GOVERNMENT SHOULD SEEK TO PROMOTE WITH INTERNATIONAL PARTNERS THAT WOULD BE HELPFUL IN THE IOT CONTEXT?

The U.S. should champion policies and practices that allow data to be easily shared and reused within and across organizations, countries, and regions. In addition, the U.S. should

encourage countries to work collaboratively on IoT solutions so that the devices and data from these devices are compatible globally. The Department of Commerce should follow the lead of NIST and the Department of Energy, which established the International Smart Grid Action Network, a 17-country collaboration to encourage the adoption of common international standards for smart grid technologies, and identify other IoT applications that would benefit from international collaboration on standards adoption.[53]

24. WHAT FACTORS CAN IMPEDE THE GROWTH OF THE IOT OUTSIDE THE U.S. (E.G., DATA OR SERVICE LOCALIZATION REQUIREMENTS OR OTHER BARRIERS TO TRADE), OR OTHERWISE CONSTRAIN THE ABILITY OF U.S. COMPANIES TO PROVIDE THOSE SERVICES ON A GLOBAL BASIS? HOW CAN THE GOVERNMENT HELP TO ALLEVIATE THESE FACTORS?

The Department of Commerce should push back against countries that have or are attempting to mandate the use of particular standards for the Internet of Things within their borders, as well as those attempting to limit the flow of data across borders. For example, India requires gateways and application servers that support the Internet of Things to be located inside the country if they service Indian customers. [54] The rationale for localization requirements is to protect national security, even though such requirements have no impact on security whatsoever, and the true motive is to artificially prop up domestic industry.[55] Such requirements limit the ability of international device manufacturers and service providers to analyze data collected from the Internet of Things around the world, thereby reducing the technology's potential value.[56] The government should ensure that international trade agreements prohibit restrictions on the ability of international device manufacturers to enter domestic markets and ensure that companies can freely exchange data across borders.[57]

ADDITIONAL ISSUES

25. ARE THERE IOT POLICY AREAS THAT COULD BE APPROPRIATE FOR MULTISTAKEHOLDER ENGAGEMENT, SIMILAR TO THE NTIA-RUN PROCESSES ON PRIVACY AND CYBERSECURITY?

The Department of Commerce should also publicly weigh in on the plans of the intelligence community to use the Internet of Things for surveillance. Intelligence agencies are investigating how to leverage Internet of Things devices to improve their surveillance capabilities. In a recent congressional testimony, James Clapper, the US director of national intelligence, explained the Internet of Things could be used "for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."[58] Improper and excessive use of this technology for intelligence gathering, especially of ordinary Americans, could substantially reduce U.S. companies' competitiveness abroad and discourage adoption of the technology by consumers. The Department of Commerce should contribute to this public debate, including through a related multistakeholder working group.

26. WHAT ROLE SHOULD THE DEPARTMENT OF COMMERCE PLAY WITHIN THE FEDERAL GOVERNMENT IN HELPING TO ADDRESS THE CHALLENGES AND OPPORTUNITIES OF IOT? HOW CAN THE DEPARTMENT OF COMMERCE BEST COLLABORATE WITH STAKEHOLDERS ON IOT MATTERS?

The Department of Commerce should regularly convene industry, consumer, government, academic, and other stakeholders to study challenges, develop solutions, and create strategies to capture the benefits of the Internet of Things. For example, the working group that the DIGIT Act would establish would be an effective model for addressing specific issues and informing policymakers. In addition, the Department of Commerce should make using the Internet of Things within its own organization a key priority as part of its data

strategy and plan to share lessons learned and best practices with the rest of the government.

27. HOW SHOULD GOVERNMENT AND THE PRIVATE SECTOR COLLABORATE TO ENSURE THAT INFRASTRUCTURE, POLICY, TECHNOLOGY, AND INVESTMENT ARE WORKING TOGETHER TO BEST FUEL IOT GROWTH AND DEVELOPMENT? WOULD AN OVERARCHING STRATEGY, SUCH AS THOSE DEPLOYED IN OTHER COUNTRIES, BE USEFUL IN THIS SPACE? IF THE ANSWER IS YES, WHAT SHOULD THAT STRATEGY ENTAIL?

Given the broad array of opportunities and challenges presented by the Internet of Things, and because many aspects of the Internet of Things directly relate to public sector activities, the U.S. should develop a national strategy for the Internet of Things. As explained in the response to question 1-B, comprehensive national strategies detailing policies that remove obstacles and support widespread deployment of the Internet of Things are necessary to overcome the market failures, regulatory obstacles, and equity concerns that hinder the technology's growth and limit its value.[59] A national strategy for the Internet of Things, if designed and implemented correctly, would maximize the opportunity for the Internet of Things to deliver substantial social and economic benefits. The United States will not successfully capture these benefits by leaving development of the Internet of Things solely up to the market, just as no government actions could capture all of the potential benefits without a robust private sector that can innovate unencumbered by overly restrictive regulations.

28. WHAT ARE ANY ADDITIONAL RELEVANT ISSUES NOT RAISED ABOVE, AND WHAT ROLE, IF ANY, SHOULD THE DEPARTMENT OF COMMERCE AND, MORE GENERALLY, THE FEDERAL GOVERNMENT PLAY IN ADDRESSING THEM?

The U.S. government does not have a strategic plan for how it will adopt and deploy the Internet of Things across federal agencies, and individual agencies are similarly unprepared for how they will leverage the technology internally. In 2015, the Brookings Institute reviewed the strategic plans of all federal agencies and found that none even mentioned the Internet of Things.[60] As of May 2016, the Center for Data Innovation could still not find a federal agency address how it will use the Internet of Things in its strategic plan. Not only does IoT offer substantial benefits to the public sector, particularly in its capacity to support improved decision-making, increase efficiency, and support new and valuable public services, but government IoT adoption would have substantial benefits for the technology as a whole. For example, by being an early adopter of IoT, the federal government can reduce the perceived risk of the technology that limits investment and adoption by the private sector and state and local governments.[61] The government should actively pursue opportunities to deploy connected technologies to improve mission delivery, as well as comprehensively examine opportunities to transform agency operations around the potential of the Internet of Things and the data it generates.

CONCLUSION:

The Internet of Things will be one of the defining technologies of the first half of the twenty-first century, and it is encouraging to see the Department of Commerce take an active role in attempting to understand the benefits and challenges of the technology to support its growth. It is also particularly encouraging to see the Department interested in the potential for a national Internet of Things strategy to ensure that the United States can fully capture its benefits and establish itself as a world leader in the technology.

[1] "Data Access," National Oceanic and Atmospheric Administration, accessed May 31, 2016, https://www.ncdc.noaa.gov/data-access.

[2] "About Us," National Oceanic and Atmospheric Administration, accessed May 31, 2016, https://www.ncdc.noaa.gov/about.

[3] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

[4] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

[5] Ibid.

[6] Ibid.

[7] Daniel Castro, "The Rise of Data Poverty in America," Center for Data Innovation, September 10, 2014, http://www2.datainnovation.org/2014- data-poverty.pdf.

[8] Ibid.

[9] Daniel Castro and Joshua New, "Comments in Response to the National Institute for Occupational Safety and Health's Center for Direct Reading and Sensor Technologies' Request for Information on Sensors for Emergency Response Activities," Center for Data Innovation, March 22, 2016, http://www2.datainnovation.org/2016-sensors-emergency-response.pdf; Joshua New, "The Internet of Things Means a More Accessible World," Center for Data Innovation, May 11, 2015, https://www.datainnovation.org/2015/05/the-internet-of-things-means-a-more-accessible-world/; Daniel Castro and Mark Doms, "Data is the Key to the Factory of the Future," Center for Data Innovation, October 2, 2014, https://www.datainnovation.org/2014/10/data-is-the-key-to-the-factory-of-the-future/; and Daniel Castro and Joshua New, "Accelerating Data Innovation: A Legislative Agenda for Congress," May 11, 2015, http://www2.datainnovation.org/2015-data-innovation-agenda.pdf.

[10] "General Wellness: Policy for Low Risk Devices," Food and Drug Administration, January 20, 2015, http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf.

[11] Ibid.

[12] "Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices," Food and Drug Administration, February 9, 2015, http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm401996.pdf.

[13] "FCC Raises Record USD 44.9 Billion in AWS-3 Airwaves Auction," *America Herald*, February 1, 2015, http://www.americaherald.com/fcc-raises-record-usd-44-9-billion-in-aws-3-airwaves-auction/22530/; John Leibovitz, "Breaking Down Barriers to Innovation in the 3.5 GHz Band," Federal Communications Commission, April 21, 2015, https://www.fcc.gov/news-events/blog/2015/04/21/breaking-down-barriers-innovation-35-ghz-band; Colin Gibbs, "600 MHz Incentive Auction Primer: Who Will Bid, When it Will Happen, How it Will Work, and How Much Money it Will Raised," *FierceWirelss*, March 22, 2016, http://www.fiercewireless.com/special-reports/600-mhz-incentive-auction-primer-who-will-bid-when-it-will-happen-how-it-wi; and "Notice of Inquiry," Federal Communications Commission, October 17, 2014, https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-154A1.pdf.

[14] "Internet of Things: Privacy & Security in a Connected World," U.S. Federal Trade Commission, January 2015,https://www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internetthings-privacy/150127iotrpt.pdf.

[15] Ann Cavoukian and Daniel Castro, "Big Data and Innovation, Setting the Record Straight: De-identification Does Work," Information Technology and Innovation Foundation, June 16, 2014, http://www2.itif.org/2014-big-data-deidentification.pdf.

[16] For example, California's Online Privacy Protection Act of 2003 requires companies that collect personal data from users of their website to clearly display their privacy policies, and the FTC's Behavioral Advertising Principles suggests website operators notify users about their data collection practices. "California Online Privacy Protection Act of 2003," Cooley Godward LLP, June 2004, https://cooley.com/files/ALERT-Cal_OPPA.pdf, and Leuan Jolly, "Data Protection in United States: Overview," Practical Law, July 1, 2015, http://us.practicallaw.com/6-502-0467#a904003.

[17] Joshua New, "When it Comes to Regulating Data, the FTC Has an Economics Problem," Center for Data Innovation, February 15, 2016, https://www.datainnovation.org/2016/02/when-it-comes-to-regulating-data-the-ftc-has-an-economics-problem/.

[18] Ibid.

[19] Center for Data Innovation, "Statement in Response to FTC's Internet of Things Staff Report," news release, January 27, 2015, https://www.datainnovation.org/2015/01/statement-in-response-to-ftcs-internet-of-things-staff-report/.

[20] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

[21] "Preliminary Discussion Draft: Framework for Cyber-Physical Systems," National Institute of Standards and Technology, March 3, 2015, http://www.hldataprotection.com/files/2015/03/NIST-Cyber-physical-Framework-PRELIMINARY-DISCUSSION-DRAFT.pdf.

[22] Ibid.

[23] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[24] Michael McEvilley, Janet Oren, and Ron Ross, "Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," National Institute of Standards and Technology http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf and Evelyn Brown, "Building Security into Cyber-Physical Systems: NIST Researchers Suggest Approach for Trustworthy Modern Infrastructure," National Institute of Standards and Technology, May 4, 2016, http://www.nist.gov/itl/csd/building-security-into-cyber-physical-systems-nist-researchers-suggest-approach-for-trustworthy-modern-infrastructure.cfm.

[25] "Guidelines for Smart Grid Cybersecurity," National Institute of Standards and Technology, September 2014, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf, and "Technical Considerations White Paper," Federal Communications Commission, December 2015, https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf.

[26] "NIST Big Data Interoperability Framework: Volume 1, Definitions," National Institute of Standards and Technology, September 2015, http://www.nist.gov/itl/bigdata/bigdatainfo.cfm.

[27] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," National Institute of Standards and Technology, May 2014, http://www.nist.gov/smartgrid/upload/Draft-NIST-SG-Framework-3.pdf, and "IoT-Enabled Smart City Framework," National Institute of Standards and

Technology," February 18, 2016, https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/IoT-EnabledSmartCityFrameworkWP.pdf.

[28] "About Us," Department of Transportation Intelligent Transportation Systems Joint Program Office, accessed June 1, 2016, https://www.standards.its.dot.gov/About/ProgramActivities.

[29] Developing Innovation and Growing the Internet of Things Act of 2016, 2. 2607, 114th Cong. (2016).

[30] Ibid.

[31] S.Res.110, 114th Cong. (2015), and H.Res.195, 114th Cong. (2015).

[32] Office of Congresswoman Suzan DelBene, "U.S. reps. DelBene and Issa Announce Creation of the Congressional Internet of Things Caucus," new release, January 13, 2015, https://delbene.house.gov/media-center/press-releases/us-reps-delbene-and-issa-announce-creation-of-the-congressional-internet.

[33] John Eggerton, "House Members Form IoT Working Group," *Broadcasting & Cable*, May 24, 2016, http://www.broadcastingcable.com/news/washington/house-members-form-iot-working-group/156777.

[34] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf, Daniel Castro and Joshua new, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 4, 2014, http://www2.datainnovation.org/2014-iot-policy-principles.pdf, and Daniel Castro and Jordan Misra, "The Internet of Things," Center for Data Innovation, November 18, 2013, https://www.datainnovation.org/2013/11/the-internet-of-things/.

[35] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

[36] "E-Commerce Statistics (E-STATS)," U.S. Census Bureau, accessed June 1, 2016, http://www.census.gov/programs-surveys/e-stats.html.

[37] James Hagerty, "How Many Turns in a Screw? Big Data Knows," *Wall Street Journal*, May 15, 2016, http://www.wsj.com/news/articles/SB10001424127887324059704578472671425572966.

[38] Ibid.

[39] Joshua New, 'Germany and the U.S. Need Each Other's' Help to Build the Factory of the Future," Center for Data Innovation, February 9, 2016, https://www.datainnovation.org/2016/02/germany-and-u-s-need-each-others-help-to-build-the-factory-of-the-future/.

[40] Ibid.

[41] Ibid.

[42] Daniel Castro and Joshua New, "Accelerating Data Innovation: A Legislative Agenda for Congress," May 11, 2015, http://www2.datainnovation.org/2015-data-innovation-agenda.pdf.

[43] The true definition of competitiveness is the ability of a region to export more in value added terms than it imports. This calculation includes accounting for "terms of trade" to reflect all government "discounts," including an artificially low currency, suppressed wages in export sectors, artificially low taxes on traded sector firms and direct subsidies to exports. It also controls for both tariff and non-tariff barriers to imports. Robert Atkinson, "Competitiveness, Innovation, and Productivity: Clearing up the Confusion," Information Technology and Innovation Foundation, August 2013, https://itif.org/publications/2013/08/19/competitivenessinnovation-and-productivity-clearing-confusion.

[44] Daniel Castro and Joshua New, "Accelerating Data Innovation: A Legislative Agenda for Congress," Center for Data Innovation, May 11, 2015, http://www2.datainnovation.org/2015-data-innovation-agenda.pdf.

[45] James Manyika et al., "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey Global Institute, May 2011, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

[46] "Data Science Revealed: A Data-Driven Glimpse into the Burgeoning New Field," EMC, 2011, http://www.emc.com/collateral/about/news/emcdata-science-study-wp.pdf.

[47] Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," Information Technology and Innovation Foundation, September 2015, http://www2.itif.org/2015-privacy-panic.pdf.

[48] Dan Keating, David Fallis, and Andras Petho, "ShotSpotter detection system documents 39,000 shooting incidents in the District," Washington 13 Post, November 2, 2013, http://www.washingtonpost.com/investigations/shotspotter-detectionsystem-documents-39000-shooting-incidents-in-thedistrict/2013/11/02/055f8e.

[49] Ibid.

[50] Joshua New, "When it Comes to Regulating Data, the FTC Has an Economics Problem," Center for Data Innovation, February 15, 2016, https://www.datainnovation.org/2016/02/when-it-comes-to-regulating-data-the-ftc-has-an-economics-problem/.

[51] Daniel Castro and Joshua new, "10 Policy Principles for Unlocking the Potential of the Internet of Things," Center for Data Innovation, December 4, 2014, http://www2.datainnovation.org/2014-iot-policy-principles.pdf.

[52] Daniel Castro, "The Rise of Data Poverty in America," Center for Data Innovation, September 10, 2014, http://www2.datainnovation.org/2014- data-poverty.pdf.

[53] "Smart Grid National Coordination," National Institute of Standards and Technology, accessed June 1, 2016, http://www.nist.gov/el/smartgrid/sgridcoord.cfm, and "International Coordination," National Institue of Standards and Technology," accessed June 1, 2016, http://www.nist.gov/smartgrid/international-coordination.cfm.

[54] "National Telecom M2M Roadmap," Ministry of Communications & Information Technology, May 2015, http://www.dot.gov.in/sites/default/files/Draft%20National%20Telecom%20M2M%20Roadmap.pdf, and Daniel Castro, "The False Promise of Data Nationalism," Information Technology and Innovation Foundation, December 2013, http://www2.itif.org/2013-false-promise-datanationalism.pdf.

[55] Daniel Castro, "The False Promise of Data Nationalism," Information Technology and Innovation Foundation, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

[56] Ibid.

[57] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

[58] Spencer Ackerman and Sam Thielman, "US intelligence chief: we might use the internet of things to spy on you," *The Guardian*, February 9, 2016, https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

[59] Ibid.

[60] Kena Fedorschak, Kevin C. Desouza and Gregory Dawson, "Federal agencies behind the curve: IoT and

BYOD," Brookings Institution, March 16, 2015, http://www.brookings.edu/blogs/techtank/posts/2015/03/16-iot-byod-government-computers.

[61] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," Center for Data Innovation, December 16, 2015, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.