Hewlett Packard Enterprise

June 2, 2016

The Honorable Lawrence Strickling
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, Room 4725
Washington, D.C. 20230

RE: Response to Federal Register Notice on Internet of Things
81 FR 19956, Docket 160331306-6306-01

Dear Assistant Secretary Strickling:

Hewlett Packard Enterprise (HPE) is pleased to submit comments in response to the Federal Register Notice on *The Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things.* We applaud your recognition of the importance of nurturing a supportive policy environment and identifying appropriate government roles in order for the Internet of Things (IoT) to flourish.

IoT systems enable a range of opportunities for new economic growth and efficiency–such as smarter transportation, improved energy management, intelligent manufacturing and supply chains, and enhanced public safety. Effective IoT systems leverage the power of connectivity, computing, big data analysis, and security to achieve these outcomes.

HPE has a comprehensive portfolio of IoT platform, compute, data analytics, security, and connectivity solutions and services, as well as a robust ecosystem of top-tier partners. From this perspective, we are pleased to offer our expertise to the U.S. government (USG) on policies related to IoT.

Below we highlight four key areas where we see the USG playing a critical role:
1.) Supporting pilot projects and related research
2.) Fostering standards development and cyber security
3.) Opening and maintaining spectrum for IoT uses
4.) Ensuring robust and flexible privacy and data protection measures

1) Supporting pilot projects and related research

We encourage the USG to be an early adopter of IoT technologies in support of agency missions as well as interagency collaboration–such as heightened battlefield awareness for our soldiers, improved weather forecasting, smarter farming, improved energy efficiency, better monitoring of aging transportation infrastructure, and traffic management for highway safety.

In addition to leveraging IoT for its own needs, the USG acts as a catalyst for collaboration on IoT. For example, the Administration's *Smart Cities Initiative* encourages pilots and research activities across a range of agencies to spur innovation, partnerships, and widespread use and acceptance of IoT-enabled technologies and environments.

The National Science Foundation should continue to support cutting-edge research proposals for advancing next generation infrastructure, such as through its cyber physical systems initiative. As a related discipline, High-Performance Computing (HPC)[1] resources will be needed to manage, process, and analyze the massive amounts of data that IoT will generate. The U.S. must continue to invest in leading and exascale research through the National Strategic Computing Initiative (NSCI).

[1] See Information Technology Industry Foundation, Vital Importance of High Performance Computing (HPC) to U.S. Competitiveness

2) Fostering standards development and cyber security

Common standards will facilitate the adoption and growth of IoT from its current fragmented state. Standards are evolving along two dimensions: (i) technology standards, including those to facilitate interoperability and (ii) industry standards based on end uses (e.g. connected car, smart grid).

We encourage voluntary, technology-neutral IoT standards, developed in open and global collaborative processes with industry and open source communities. The National Institute of Standards and Technology (NIST) plays a central role in facilitating this process in the U.S., as well as on the international stage. USG international engagement, through standards fora and trade policy, will be important to facilitate adoption of global standards, facilitate interoperability, and counteract country-specific standards and data localization requirements.

Cyber security concerns present one of the greatest perceived barriers to adoption of IoT. HPE has identified the lack of common security standards and fragmentation as making IoT particularly vulnerable to cyber attacks.[2] We appreciate the effort NIST has undertaken specifically to develop a framework to approach security related to cyber physical systems. We encourage the USG to consider its own IoT security within a comprehensive framework and as part of cyber risk assessments.

3) Opening spectrum for IoT uses

With so many IoT devices connecting to each other and the Internet, lack of available spectrum will become an enormous constraint on the growth of IoT. Given the expected diverse forms of IoT devices, the amount of spectrum, the required channel widths and the duration and persistence of transmissions will vary widely. The lack of an adequate block of no less than 50 MHz of contiguous, globally-harmonized spectrum below 1GHz is a constraint on the growth of IoT. We encourage regulators to look at efficient uses of white spaces and dynamic approaches to assigning spectrum.

We applaud the NTIA's effort to identify spectrum to support IoT and hope the work extends to a search for globally harmonized spectrum. Using Spectrum Access Systems, as developed for TV white spaces, and extended to sharing in 3550-3700 MHz, and application-based approaches to assigning spectrum, as under development in ETSI ERM TG41, dynamic allocation can make efficient use of white spaces throughout the RF spectrum.

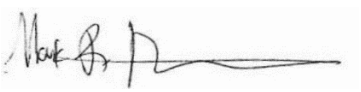
4) *Ensuring robust and flexible privacy and data protection measures*

Privacy concerns are another perceived barrier to adoption of IoT, particularly for consumers. Certainly, IoT challenges the traditional privacy notions of individual notification and consent, especially in environments where there is no user interface and machines are exchanging data. In this context, accountability and privacy by design become increasingly important. The overall privacy and data protection environment should be flexible enough for new technologies, and not create IoT-specific requirements. HPE has worked closely with the U.S. Commerce Department for many years on broader issues of privacy and data protection, and we look forward to continuing to do so.

Conclusion

HPE believes the USG can play an influential role in fostering the growth and adoption of IoT through the actions outlined above. We have attached HPE's formal policy position on IoT to provide more detail. Thank you for providing the opportunity to comment on the policy environment and government actions to support IoT. We look forward to collaborating with the USG to realize the technological, economic, and societal benefits of IoT.

Sincerely,



Mark Potter
Senior Vice President and Chief Technology Officer, Enterprise Group

[2] HPE and Economist Intelligence Unit, *Securing the Internet of Things*, April 2016

Hewlett Packard Enterprise

Policy Position
Internet of Things

Policies to accelerate the Internet of Things

- Deploying IoT-enabled public projects and pilots
- Ensuring available spectrum
- Fostering technology-neutral global standards
- Improving collaboration on security issues
- Advancing robust privacy and data protection frameworks

The Internet of Things (IoT) connects the physical and digital worlds as never before. IoT drives economic growth and efficiency with innovations such as smarter homes, cars, factories, businesses and entire cities. Hewlett Packard Enterprise (HPE)[1] advocates for government policies that encourage deployment of public pilot and large scale IoT projects, ensure spectrum availability, promote development of industry-led and technology-neutral global standards, address IoT security concerns, and provide robust privacy and data protection frameworks. HPE believes that such government policies will help realize the full development and positive potential of IoT technologies.

Policy recommendations

Adoption

- Governments can demonstrate leadership and encourage widespread confidence in the benefits of IoT by deploying pilot and large scale projects at local and national levels.
- End-to-end IoT solutions will require multiple participants to come together, particularly in delivering solutions for the common public good—such as next-generation transportation systems or smart utilities. Government policies should facilitate the deployment of IoT-enabled infrastructure and foster the development of ecosystems that promote open innovation.
- Common standards facilitate the adoption and growth of new networked technologies. We support technology-neutral IoT standards, developed in open and global collaborative processes with industry and open source communities.
- IoT policies and procurements should avoid country-specific technical standards to ensure the interoperability and competitiveness of technologies.

[1] Hewlett Packard Enterprise (HPE) is an industry leader in enterprise technology. Based in Palo Alto, CA, HPE was established on November 1, 2015 after the separation of Hewlett-Packard Company.

Spectrum

- Given the number and variety of devices connecting to each other and the Internet, lack of an adequate block of no less than 50 MHz of contiguous, globally-harmonized spectrum below 1GHz will constrain the growth of IoT. Working with international partners in the EU and elsewhere, the U.S. should take a leading role in identifying, advocating and allocating a worldwide harmonized band below 1 GHz with a minimum contiguous bandwidth of 50 MHz for IoT applications.
- We encourage regulators to look at dynamic spectrum sharing and application-based assignment techniques to promote efficient uses of white spaces. In addition, we recommend flexible re-farming of allocated spectrum wherever possible, while preserving the rights of incumbents, to build on the work done to develop Spectrum Access Systems for TV white spaces (TVWS), and extended recently to sharing in 3550-3700 MHz.

Security

- The emerging and fragmented nature of the IoT marketplace, coupled with few, if any, common security standards, put IoT devices and networks–whether personal, industrial or infrastructure–at risk of cyber attacks. Security must be addressed as part of the standards development process.
- We encourage cyber security regulations and legislation that are voluntary, outcome-based and flexible enough to address evolving threats and new technologies.

Privacy/data protection

- IoT and other new technologies challenge the traditional privacy notions of individual participation and consent, due to a lack of user interfaces, and large volumes of data being exchanged by machines. We advocate for robust and interoperable privacy and data protection frameworks that are flexible enough to address the new technology environment.
- HPE, an industry leader in privacy and data protection, is committed to accountability, maintains one of the most robust privacy programs in the world, and actively engages with privacy officials worldwide to strengthen and harmonize privacy frameworks and address privacy issues around new technologies.

Issue background

IoT technologies will connect the physical and digital worlds in new ways, providing opportunities for positive social outcomes such as decreased household energy use through smart meters, lower healthcare costs with better personal monitoring of health and fitness, and reduced traffic through smart cars and automated transportation systems. In industry, smarter factories will use less energy, quickly identify and correct manufacturing problems, monitor performance and use of installed equipment, and better align production to demand. IoT and the related data analytics will empower all companies to better understand and serve their customers. Widespread use of IoT technologies will generate staggering amounts of data, providing opportunities to identify actionable insights on issues ranging from climate and traffic to healthcare and public safety by applying big data analysis while maintaining personal privacy.

By 2025, IoT has a total potential annual economic impact of up to $11 trillion per year, roughly 11% of global GDP, according to the McKinsey Global Institute. Developing countries will represent 40% of the IoT value. Business to business applications will generate about 70% of the potential value, with consumers capturing 90% of the benefits.[2]

[2] McKinsey Global Institute. The Internet of Things: Mapping the Value Beyond the Hype, June 2015

Spectrum[3]

With so many IoT devices connecting to each other and the Internet, lack of an adequate block of globally-harmonized, available spectrum will become an enormous constraint on the growth of IoT, Given the expected diverse forms of IoT devices, the amount of spectrum, required channel widths and duration and persistence of transmissions are likely to vary widely. Currently, there are several standards and proprietary solutions, but as the growth begins to expand exponentially, more must be done to ensure that IoT will not be limited by regulatory roadblocks.

Today, unlicensed spectrum in the 2.4 GHz and 5 GHz bands for Wi-Fi and other IEEE-based technologies is fairly universal, but is only a good choice for a narrow class of consumer and enterprise IoT use cases due to its limited propagation, large channel bandwidths, high energy consumption, and supported network topologies. These bands do nothing for the vast majority of long-range, low-bandwidth, minimal duty-cycle, energy optimized IoT devices that are the principal focus of most market forecasts. The U.S. 900 MHz band (902-928 MHz) is a good candidate for a number of reasons, and with the move to Wi-Fi of many devices that formerly relied on this band, it has become temporarily less congested than in prior years. Unfortunately, spectrum below 1GHz allocated to IoT is not only inadequate, but is completely different in major regulatory domains around the world. The lack of a globally-harmonized band or bands for IoT devices will directly affect the speed, scale, and success of such deployments in the U.S.[4] This will raise the price of IoT radios and act as a huge brake on adoption in all countries, including the U.S. Working with international partners in the EU and elsewhere, the U.S. should take a leading role in identifying, advocating and allocating a worldwide harmonized band below 1 GHz with a minimum contiguous bandwidth of 50 MHz for IoT applications.

A vibrant marketplace of both public and private connectivity options is essential to the future of IoT in the U.S. There are almost an infinite number of IoT use cases with different data workloads, duty cycles, and geographic coverage requirements. Some obviously fit into wide area deployments that are clearly suited for operator-managed networks such as rail or vehicular uses, while others have far smaller geographic footprints and/or involve equipment deployed exclusively on private property such as at container ports, factories or oilfields. HPE believes that both privately-owned and operator-managed IoT communications networks have a strong role to play in a variety of industries and applications, however the current market focus is almost exclusively on the latter. There must be enough unlicensed spectrum to enable both. There is a real risk that operator build-outs of new technologies in the limited 915 MHz band may crowd out the ability of private parties to deploy their own systems. HPE believes that all providers, including new market entrants, should be able to compete in the 915Mhz band with well established, legacy operators, so long as deployed equipment complies with Federal Communication Commission requirements.

Because of its excellent propagation characteristics, the 915 MHz band already supports numerous wide area IoT networks in municipalities across the United States that are critical to energy grid management and demand response. While there is huge innovation with a tremendous number of new radio technologies entering the market in this band, their uncoordinated channelizations range from tens of KHz to tens of MHz, creating uneven loading and interference duty cycles. It is truly a wild west of modulations, center frequency, bandwidths, topologies, error correction techniques, device addressing schemes and more. HPE strongly supports innovation in these bands, but there is not nearly enough spectrum to accommodate all of the marketplace developments currently underway and ensure fair coexistence between them.

New spectrum allocation techniques and out-of-the-box approaches will be required to achieve this goal. There is no unallocated spectrum below 1 GHz in major regulatory domains, so allowing flexibility and dynamic re-farming of

[3] While these comments focus on spectrum below 1 GhZ, we note that HPE joined other organizations to file comments with the Federal Communications Commission related to LTE-U and LAA technology. See FCC, Office of Engineering and Technology and Wireless Telecommunications Bureau Seek Information on Current Trends In LTE-U and LAA Technology, ET Docket No. 15-105, filed Oct. 21, 2015.

[4] It is widely recognized that one of the key factors that enable Wi-Fi to achieve its success was the existence of an adequate amount of spectrum in the 2.4-GHz that was allocated worldwide in a common manner. This in turn enabled the industry to develop low-cost radio systems that did not need to be adapted to individual countries, and that could share common hardware including both baseband and front-end components.

allocations, while protecting the rights of incumbents is something that must be explored and exploited. Technologies such as Spectrum Access Systems, developed for TV white spaces, and subsequently extended to sharing in 3550-3700 MHz, may hold great promise. Application-based approaches to assigning spectrum, as under development in ETSI ERM TG41, with dynamic allocation can make efficient use of white spaces throughout the RF spectrum.

Standards

Standards are important to accelerate adoption and wide scale deployment of IoT technologies and networks. Currently, the industry has multiple actors and competing solutions, which has led to fragmented approaches. Both industry and technical standards development efforts are currently underway through various consortia and in collaboration with government agencies and standards bodies. Governments should refrain from requiring unique, non-global technical standards in IoT, which would restrict interoperability and dampen growth. According to McKinsey Global Institute, "interoperability is critical to capturing maximum value," on average in 40-60% of IoT settings.[5]

Security

Cyber threats are evolving for a multitude of reasons: threat actors are more organized, funded, and capable than ever before. The "perimeter" that we secure is shifting and changing with the rapid expansion and widely acceptable use of new technologies such as cloud, mobile computing, IoT, and industrial internet. Greater reliance on and pervasiveness of technology, connectivity and automation is happening globally, and there are no international internet boundaries. Online security is directly impacted by the security practices of other countries, and this is an ongoing and growing risk when it comes to cyber defenses.

Next generation cyber threats are anticipated to emerge in new areas that could affect international supply chains and critical infrastructure, placing at risk some of the benefits of IoT-enabled innovations such as digital smart grids and smart factories. HPE research has identified IoT devices and networks as likely new avenues of cyber attack, due to the fragmented nature of the marketplace with few to no common security standards in place. According to our research, the lack of common IoT interfaces and proprietary implementation of updates creates vulnerabilities and places emerging IoT devices and networks at risk for malicious attacks.[6] Additionally, HPE Security Research analyzed ten popular IoT consumer devices and found 80% of devices raised security concerns ranging from password complexity/reset to insecure network access and user interfaces.[7] The possibility of attacks on connected critical infrastructure such as energy grids, water supply, and nuclear power plants has already garnered much attention and concern.

Privacy/data protection

The emergence of new technologies, such as IoT, upends the traditional legal notions of individual participation and consent, and heightens the importance of accountability and privacy by design in dealing with personal information and data protection. The emergence of IoT, cloud, and big data technologies have strained current legal privacy frameworks, raising questions around consent, secondary use, data transfers, accuracy, access and consumer data correction. Consistent guidance across countries regarding the governance, sovereignty, and ownership of data from IoT devices will also be critical for rapid deployment of IoT solutions.

HPE considers effective data protection an enabler of current and future technology offerings. Accordingly, we seek to maintain robust privacy and data protection, with principles derived from the OECD Guidelines and the EU Data Protection Directive, which we apply across the globe as the highest existing data protection standard. Hewlett-Packard Company, the predecessor to HPE before company separation, was the first company to be approved under both the Binding Corporate Rules (BCR) and Asia-Pacific Economic Cooperation's Cross-Border Privacy

[5] Ibid
[6] HPE and Economist Intelligence Unit, *Securing the Internet of Things*, April 2016
[7] HPE Internet of Things research study 2015, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

Rules (CBPR) systems and we are recognized for leading the development of today's accountability-based approach to privacy and continue to serve as a trusted advisor to regulators worldwide.

HPE adheres to four core principles around data protection: 1.) Privacy is a fundamental right; 2.) Accountability is integral to data stewardship; 3.) Global harmonization and interoperability of privacy frameworks are essential; 4.) Regulatory solutions must be flexible to address an ever-evolving global marketplace.

We are taking an active role in shaping and evolving privacy frameworks to ensure the right balance of innovation, business goals, social responsibility and ethical practices. We advocate globally for robust privacy and data protection legislation and regulations that emphasize accountability and are flexible enough to address issues for emerging technologies, without requiring separate legislation for individual technologies, such as IoT.

Big data analysis is a central part of the IoT ecosystem, and presents challenging privacy questions. We are engaged in efforts to evolve data governance to ensure society trusts and reaps the benefits of big data while still protecting individual privacy. We are working with the Information Accountability Foundation to develop the Unified Ethical Frame for Big Data Analysis, an effort to address big data privacy issues that is backed by regulators, companies, and the privacy community. We believe accountability and balanced ethics-based assessments are critical for big data governance and applicable beyond private sector activities, since governments are potentially major users of big data processes. Therefore, we believe that accountability practices should be applied to the public sector as well as the private sector.

HPE's leadership in IoT

We stand ready to provide our expertise to governments on policies related to IoT. HPE has a comprehensive portfolio of IoT compute, data analytics, security, and connectivity solutions and services, as well as a robust ecosystem of top-tier partners. HPE Universal IoT Platform simplifies integrated communications across disparate devices and systems, enabling more complete access to data and analytics, provided on a secure cloud platform. HPE Edgeline IoT Systems, the result of a joint partnership with Intel, sit at the network edge, enabling customers to securely aggregate and analyze data in real-time and control devices and things. HPE Aruba has a broad portfolio of secure wireless, wired, remote access, locationing, and network access control solutions, and offers Suite B encryption to serve both commercial and government IoT applications up to classified Top Secret. To analyze and generate actionable information from the big data sets IoT will generate, the integrated HPE Haven platform combines the power of Hadoop open source software, HPE IDOL real-time unstructured data analysis (such as video and voice), HPE Vertica massive database platform, enterprise security and next-generation applications to deliver cutting-edge and relevant information analytics for public sector and enterprise customers. In addition, HPE has developed security solutions that specifically enable organizations to proactively mitigate and respond to the inherent risks that IoT devices present, including comprehensive security testing across device, network, mobile and cloud. To integrate all of these technologies, HPE also provides a suite of services to accelerate the adoption of IoT solutions in the marketplace. These industry-focused IoT services help customers assess IoT needs and identify opportunities to transform their business.

For example, HPE Future Cities initiative uses HPE Haven to develop a detailed understanding of local constituencies, identify trends, and target services to citizens when and where they need them, ranging from healthcare and education to public safety and traffic management. Our technologies enable citizen-centered government that delivers public value and drives economic progress. We are using innovative IT solutions to help cities put the needs of local citizens and businesses at the center of decision making—from setting budgets to delivering public services in the United States to Europe, Asia, and Australia. By deploying solutions that use IoT technologies to support big data collection and analysis, cloud services, mobility, and security, we help improve local government services and reduce public costs. These innovations enable governments to be more agile and resilient, improve quality of life for citizens, and drive economic growth.