Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	)	Docket No. 160331306-6306-01
	)	
	)	
	)	

COMMENTS OF THE GSM ASSOCIATION

The GSM Association ("GSMA") respectfully comments on the National Telecommunications and Information Administration's ("NTIA") request for input ("Request") on the benefits, challenges, and potential roles for the U.S. government in fostering the advancement of the Internet of Things ("IoT").[1]

I. INTRODUCTION AND SUMMARY

Much like prior phases of the Internet, the IoT is fast becoming the new driving force behind the global economy. Analysts estimate that by 2020, there will be over 15 billion connected devices, with 3.4 billion in North America alone.[2] This includes wearable devices like fitness trackers, home devices such as thermostats or coffee makers, farming devices like watering systems, autonomous vehicles, robotics, transportation systems, and telecommunications systems, to name a few. Of these, 1.2 billion will represent cellular M2M connections, an important part of the competitive connectivity landscape.[3] The global business

---

1 National Telecommunications and Information Administration, Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956, 11956 (Apr. 6, 2016) ("Request").

2 Machina Research (2016).

3 *Id.*

impact of M2M—achieved through cost reductions and improved quality of service—may reach $4.5 trillion in that same timeframe.[4]

IoT offers unrivalled opportunities for economic productivity and innovation; it can even create entirely new markets. The positive impacts of IoT on citizens, consumers, businesses, and governments will include improving individual health and well-being, helping governments reduce healthcare and other costs, improving consumers' quality of life, reducing carbon footprints, increasing access to education and other public services, improving transportation safety, and energy efficiency. Globally, nations are scrambling to seize the opportunities this new digital age promises.

And although it is developing quickly, IoT still is in its infancy. Its many opportunities could be lost without the right enabling conditions. To accelerate the emergence of IoT-led growth and ensure the full realization of its benefits, the United States should focus on the following critical imperatives.

First, the United States should forbear from regulating IoT and avoid reflexively extending legacy regulations designed for outdated technologies to the IoT. As the IoT unfolds, market forces will best address legal and regulatory challenges and encourage the creation of innovative solutions. Regulators and policymakers should avoid attempts to develop laws to deal with challenges that IoT proliferation *might* bring, and instead allow the IoT to develop within the private sector. The U.S. government also should work to curtail regulations at the state and local level that could impede IoT deployment. This approach will encourage investment and innovation and drive consumer adoption.

[4] PriceWaterhouseCoopers, Report, Realising the Benefits of Mobile-Enabled IoT solutions (March 2015).

Second, the U.S. government should support and promote industry alignment around interoperable, industry-led specifications and standards across the global IoT ecosystem. Many possible applications of the IoT have been conceived, but they will not be realized until cohesive interoperability and technical standards have been developed to allow the IoT to grow to scale and reach its full potential. To encourage the development of interoperable standards without hindering innovation, policy frameworks should be technology- and service-neutral and treat equivalent services similarly.

Third, the U.S. government should promote the allocation of globally harmonized spectrum that can support IoT. International harmonization is essential in all personal mobile communications, but will be even more so for M2M devices. To be cost effective, devices should only need to support a minimal number of frequency bands. This will also permit equipment manufacturers to achieve truly global—not just national or regional—scale.

Fourth, the U.S. government should encourage industry to build trust into IoT devices. Existing laws and regulations, operating in tandem with self-regulatory regimes and best practices, will provide sufficient protection to consumers as the IoT develops. Regulators should refrain from stove-piping general issues of privacy and security within IoT by creating IoT-specific approaches. In doing so, regulators also can guard against the potential for multiple, overlapping, or inconsistent regulatory frameworks for privacy and security.

Finally, the U.S. government should engage on a bilateral and multilateral basis, as appropriate, to ensure that international IoT activities similarly encourage competition, investment, and innovation. Regulatory interference at this stage—from any source—could lead to fragmentation and impede innovation, inhibiting the IoT's ability to reach its full potential to deliver benefits to consumers.

II. DISCUSSION

A. General Questions

1. *Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?*

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

    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?*

    c. *What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?*

IoT is a nascent industry, and much is still unknown about its future, including industry structures, business models, and the markets and services that will develop. What is clear, however, is that the IoT differs in many ways from traditional mobile telephony voice and messaging services. Applying legacy regulation therefore has the potential to stifle IoT deployment and innovation. The U.S. should avoid reflexively extending legacy regulations and instead apply a "light touch" to IoT that promotes flexible, technology-neutral policies that will encourage innovation and drive widespread consumer adoption.

The IoT differs in many ways from the traditional mobile telephony voice and messaging business. The IoT ecosystem and its value chain will be composed of a large number of diverse players. In most cases, IoT services will not seek to provide open Internet or "any-to-any" voice communications services and, as such, will have closed user groups. In addition, IoT customers generally will be businesses seeking global distribution coverage and managed platforms for the provision of global services—not consumer end-users. As a result, these enterprise services will realize significantly lower average revenue per connection than traditional voice and messaging

services. This means they are more likely to be hampered by burdensome regulations and fragmentation.

Policymakers should keep in mind these distinguishing characteristics of the IoT—particularly its wide deployment scale and low average revenue per connection. In addition, regulators and policymakers should avoid prescriptive, IoT-specific regulation and instead allow the IoT market to mature under generically applicable frameworks. Excessive or technology-biased regulation will stifle innovation, raise costs, discourage investment, and harm consumers. Policymakers also should encourage industry to build trust and facilitate interoperability at all levels of the IoT: across devices, analytics platforms, and network connectivity. In order to facilitate the worldwide reach and scale that many IoT technologies will need to be successful, IoT policies and standards should be flexible and broadly interoperable around the globe.

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?*

The Request correctly notes that multiple definitions exist for IoT. However, efforts to define IoT are premature and can have unintended consequences by narrowing the full potential of IoT innovation or by paving a path toward IoT-specific regulation. Rapid innovation in IoT likely will mean that early definitions quickly will become obsolete. It also is unclear why a definition is necessary unless regulation is being considered.

In its report on Enabling the Internet of Things, the Body of European Regulators for Electronic Communications ("BEREC") notes that "it is not necessary to determine in detail which [IoT] definition is most appropriate. Fixing a definition of M2M communications or IoT

services only makes a crucial difference if obligations explicitly depend on that distinction."[5] BEREC's report undertook a comprehensive study of the state of play of IoT services in the European Union without defining IoT. NTIA should seek to do the same.

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?*

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

Following a consultation in the EU on "Enabling the IoT," BEREC concluded that no special treatment for IoT services is necessary at this time, except in a few specific areas.[6] According to the Report, one of the most significant regulatory obstacles facing IoT development and deployment is international and domestic roaming regulation. Depending on the particular IoT use case, underlying connectivity for the IoT service may be provided using international roaming. Such roaming may occur on a permanent or transitory basis. Permissive roaming frameworks therefore will be critical for the provision of some IoT use cases.

Some countries, however, already restrict or are planning to restrict the use of permanent roaming to support global IoT services.[7] This would be a mistake, as restrictive roaming regulations could deter the proliferation and efficacy of IoT. Regulators and policymakers instead should recognize the truly global nature of IoT and facilitate global connectivity. Service

---

[5] Body of European Regulators for Electronic Communications, Report, Enabling the Internet of Things, at 6 (Feb. 2016) ("BEREC Report").

[6] BEREC Report at 5.

[7] Roaming generally is implemented through bilateral agreements between operators. Roaming has traditionally been designed as a service to enable foreign visitors to continue to use their mobile service while travelling abroad—*i.e.*, as a temporary service for an individual, facilitated by a host provider. For IoT, the roaming end user may be companies offering IoT services in foreign markets, also facilitated by a host provider. Such roaming might not be temporary.

providers and IoT device manufacturers will require global coverage and managed platforms for economic viability and the provision of consistent global services.

Other regulatory issues pose less of an immediate challenge. For example, while the availability of sufficient numbering resources must be ensured to accommodate the forecasted growth of IoT devices that will be connected to the Internet, we are not facing imminent scarcity. Both extra-territorial and international global numbers are being used to deploy IoT connected devices. Still, this potential issue should be carefully monitored, and a flexible approach by regulators is essential as different IoT services may have different requirements.

Regulators and policymakers also should consider incentives to encourage IoT adoption. In Brazil, for example, IoT-specific tax reductions have dramatically increased the uptake of innovative IoT services.[8] Brazil's tax incentives recognize that M2M connections yield a much lower ARPU than retail connections. According to GSMA's studies, M2M devices benefitting from the tax reduction grew at a rate of 26 percent, compared to 7 percent growth of other M2M standard devices. To keep pace with international growth, the U.S. government similarly should consider policies that incentivize IoT adoption.

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 v. industrial; public v. private; device-to-device vs. human interfacing.*

IoT technologies exist along a broad spectrum, and do not match the kind of clean dichotomies that Request 4 envisions. Important distinctions can be made in three areas: business models, connectivity technology, and privacy and security issues. Distinctions along

[8] *See* Sylwia Kechiche, GSMA Intelligence, M2M in Latin America: State of the Market (May 13, 2015).

these lines can guide policymakers and improve the precision with which IoT policy issues are discussed.

With respect to business models, most IoT connected services are based on B2B or B2B2C models. Thus, for many IoT use cases, customers will be businesses—not consumers. Consumer protection rules designed to protect end-users may not be relevant. On many issues, businesses negotiating their connectivity needs will have countervailing buying power to ensure appropriate contract terms; there would not be any need for regulatory concern.

Similarly, IoT devices generally can be classified as consumer-facing or enterprise. Enterprise IoT will not raise the same privacy and security issues that consumer-facing IoT may raise. The very nature of most industrial IoT services will be to collect, store, and share data in which there is no cognizable privacy interest. For example, turbidity sensors measuring water quality do not present the same privacy concerns as a diabetic patient's connected glucose monitor. Devices that monitor major assets in the electrical grid also may present little in the way of privacy issues, but their security may be a matter of greater concern. IoT services are no different in this respect that other existing technologies and services.

Finally, IoT technologies will differ based on how they connect to the Internet—whether by fixed, satellite, low-power-wide-area ("LPWA") networks, cellular, or other solutions. At this early stage of the technology, it is important that any policies are technology-neutral so as to allow all IoT technologies and use cases an equal opportunity to flourish. Otherwise, regulators and policymakers may inadvertently discourage investment and innovation.

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?*

GSMA has published a wealth of information on IoT which may be helpful to NTIA as it conducts its inquiry. These studies provide high-level overviews as well as focused, comprehensive research into important aspects of the IoT. A brief list is provided below.

- The GSMA Connected Living Programme, http://www.gsma.com/connectedliving/. This website covers GSMA's IoT activities and is a reliable reference for up-to-date information.

- Realising the Benefits of Mobile-Enabled IoT Solutions (March 2015), http://www.gsma.com/connectedliving/wp-content/uploads/2015/04/Realising-the-benefits-of-mobile-IoTsolutions-v4_7Apr2015.pdf. This report highlights the socio-economic benefits that IoT can generate for governments, citizens, end-users, and businesses. The report also reviews an array of existing mobile-enabled solutions and analyzes how they are fundamentally changing business models, creating more opportunities, and conserving resources.

- Driving Innovation in Connected Living: The US Flags the Future of M2M (September 2014), http://www.gsma.com/connectedliving/wp-content/uploads/2014/09/us-m2m-2014.pdf. This report investigates why the U.S. is the vanguard of M2M, opportunities for further expansion, and, importantly, how operators themselves are unlocking more value for M2M customers.

- IoT Device Connection Efficiency Guidelines, Version 3.0 (March 2016), http://www.gsma.com/connectedliving/wp-content/uploads/2016/04/TS-34-v3-0v2.pdf. Good design is essential to ensure that IoT device performance is optimized and to prevent failure mechanisms creating runaway situations which may result in network overload. The Guidelines specify requirements for efficient use of mobile network connectivity.

- The Market for Smart Wearable Technology (February 2015), http://www.nickhunn.com/wp-content/uploads/downloads/2014/08/The-Market-for-Smart-Wearables.pdf. The report predicts rapid growth of the wearable market in the next few years and a unique role for operators.

- Understanding the Internet of Things (July, 2014), http://www.gsma.com/connectedliving/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf. This report sets forth the potential impact of the IoT and GSMA's vision of the "Connected Life."

- Cellular M2M Forecasts and Assumptions: 2010-2020, https://gsmaintelligence.com/research/?file=67b76e2ff86fa4cd7f11cf460e5d54dc&download. This report analyzes network technology trends relating to the cellular M2M market.

B. 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.*

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

As an initial matter, the government should encourage global interoperability and standards. IoT is global by nature, and it is crucial that IoT platforms develop on a global level. Globally interoperable services and standards reduce deployment costs and complexity, facilitate scalability, and enable consumers to enjoy intuitive connected experiences. The GSMA has been and will continue to be active in promoting interoperability and in defining standards for IoT. Specifically, GSMA is active in the IoT segment of the Third Generation Partnership Project ("3GPP") (LTE-MTC, NBIOT, and EC GSM). GSMA's objective is to modify and optimize existing mobile standards to fulfill the low data/throughput requirements and power consumption typical of the IoT environment. Global interoperability and standards development will be key to the success of IoT from a technical perspective, and the U.S government should actively support these efforts.

Second, the U.S. should emphasize the allocation of globally harmonized spectrum that can support IoT. International harmonization is essential in all personal mobile communications, but will be even more so for M2M devices. To be cost effective, devices should only need to support a minimal number of frequency bands. This will also permit equipment manufacturers to achieve truly global—not just national or regional—scale. Currently, mobile operators are using spare capacity on their existing 2G, 3G, and 4G networks and spectrum to support M2M services. The GSMA supports harmonization of frequency bands for mobile services, as it

ensures the efficient use of spectrum while also galvanizing the cellular IoT market by driving the widespread creation of low cost devices that can be used worldwide. To realize this goal, regulatory bodies should work with mobile and M2M stakeholders, including mobile network operators and equipment vendors, to examine which bands should be harmonized, and what band plan considerations should be prioritized. Harmonized spectrum bands need to be able to support the full range of potential M2M deployment scenarios. This includes high data-rate applications which could require substantially more spectrum than existing forecasts (based on today's usage profiles) would suggest.

To support global harmonization of spectrum, the GSMA recently announced the establishment of the "Mobile IoT Initiative," a new project backed by 26 of the world's leading mobile operators, OEMs, and chipset, module, and infrastructure companies. The Mobile IoT Initiative is designed to address the use of LPWA solutions in licensed spectrum. This group will work to accelerate the commercial availability of mobile IoT technology by facilitating demonstrations, proof of concept, and trials of a selection of complementary LPWA licensed spectrum technologies. LPWA technologies in licensed spectrum can be deployed in a simplified, cost-effective manner without sacrificing key customer requirements such as battery life and security. Mobile operators already provide reliable end-to-end IoT platforms that allow customers to scale and manage their business requirements. They also have unrivaled global network coverage as well as technical and business support to react to a customer's changing needs. Efforts by both the industry and regulators to promote global spectrum harmonization will play an important role in supporting continued IoT development.

C. Infrastructure

9. *Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?*

Security will be a key concern as IoT infrastructures develop. The emergence of the IoT will create thousands of new services that will connect billions of new IoT devices over the next decade. As more devices are connected, the threat of security breaches increases across the entire IoT ecosystem, with some industry players more experienced in this area than others. The GSMA believes that security has been vital to building and maintaining consumer confidence in mobile services to date, and it will be critical to the success of IoT connected services, as these services have the potential to support and deliver increasingly sophisticated and security-sensitive services. For security measures to be effective, robust solutions will need to be deployed across the entire value chain of the IoT market, including devices, chipsets, and software. Reducing vulnerabilities in devices, applications, and web services to ensure end-to-end IoT security should be a priority for all parties. Industry is already working on solutions in a layered and flexible manner. To assist in this effort, the GSMA has created a set of security guidelines to help service providers who are looking to develop new IoT products and services.[9]

Another major infrastructure challenge is connection efficiency. The GSMA has worked with its ecosystem partners to establish a set of GSMA IoT Device Connection Efficiency Guidelines.[10] These guidelines provide suggestions for how machines can communicate via the mobile network in the most intelligent and efficient way.

10. *What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?*

---

[9] GSMA, "GSMA IoT Security Guidelines," *available at* http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/.

[10] GSMA, "GSMA IoT Device Connection Efficiency Guidelines," *available at* http://www.gsma.com/connectedliving/gsma-iot-device-connection-efficiency-guidelines/.

There are several broad principles the government can promote to bolster the availability and resiliency of IoT infrastructures. First, the government should apply relevant legal frameworks consistently to all parties in the IoT value chain. Second, the government should support self-regulation by IoT stakeholders, risk management-based approaches, and privacy management programs that empower stakeholders to achieve important policy goals without regulation. Third, infrastructure protection should be practical and proportionate. Protections—for example, protection of user privacy—should be designed into IoT services, and should be implemented in a way that promotes transparency and consumer choice.

D. Economy

11. *Should the government quantify and measure the IoT sector? If so, how?*

    a. *As devices are manufactured or sold (in value or volume)?*

    b. *As industrial/manufacturing components?*

    c. *As part of the digital economy? (i) in providing services, (ii) in the commerce of digital goods*

    d. *In enabling more advanced manufacturing and supply chains?*

    e. *What other metrics would be useful, if any? What new data collection tools might be necessary, if any?*

    f. *How might IoT fit within the existing industry classification systems? What new sector codes are necessary, if any?*

The government should consider classifying IoT technologies by the type of underlying connectivity used: cellular, wired, satellite-enabled, Wi-Fi, LPWA, and/or other proprietary standards. IoT connections are expected to grow significantly in the coming years. Analysts estimate that by 2020 there will be over 15 billion connected devices, with 3.4 billion in North America alone.[11] Of these, cellular M2M connections will represent an important but small part

[11] *See* Machina Research (2016).

of a large competitive connectivity landscape, with an expected total of 1.2 billion connections worldwide by 2020, with 280 million in North America.[12] Thus, it may be practical to break down the IoT ecosystem by groups based on underlying connectivity type, as each will have its own unique characteristics and use cases.

12. *Should the government measure the economic impact of IoT? If so, how?*

    a. *Are there novel analytical tools that should be applied?*

    b. *Does IoT create unique challenges for impact measurement?*

A growing Internet of Things provides an enormous range of socio-economic benefits. The private sector is best positioned to quantify these benefits by taking into account not only the incremental benefits to consumers and businesses that take advantage of innovative IoT services, but also the cost savings and efficiencies enabled by the use of IoT in the conduct of business and delivery of public services. For example, IoT-enabled predictive maintenance activities are likely to result in significant cost savings and loss prevention for businesses, and these benefits should be quantified. Efforts to quantify IoT benefits should focus not only on private economic benefits, but also on the public benefits of IoT. IoT-enabled services will have wide-ranging social benefits such as improving the quality of life of patients, reducing carbon footprints, increasing access to education in remote or underserved communities, and improving transportation safety. For its part, GSMA (in conjunction with PriceWaterhouseCoopers) has undertaken numerous studies quantifying the economic impact of the Internet of Things.[13]

---

[12] *Id.*

[13] *See, e.g.,* PriceWaterhouseCoopers, Realising the benefits of mobile-enabled IoT solutions (March 2015), *available at* http://www.gsma.com/connectedliving/wp-content/uploads/2015/04/Realising-the-benefits-of-mobile-IoTsolutions-v4_7Apr2015.pdf; PriceWaterhouseCoopers, Socio-economic impact of mHealth: An assessment report for Brazil and Mexico (June 2013), *available at* https://www.pwc.in/assets/pdfs/consulting/strategy/socio-economic-impact-of-mhealth-brazil-and-mexico.pdf; PriceWaterhouseCoopers, Socio-economic impact of mHealth: An assessment report for the European Union (June 2013), *available at* http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/Socio-economic_impact-of-mHealth_EU_14062013V2.pdf.

E. 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 IoT already is expansive and will continue to grow exponentially. Given the multitude of effects that the IoT will have on daily life, as well as the impact that other policy areas might have on the IoT environment, the U.S. government should be mindful of the profound impact that premature regulation could have on the future of the IoT. With that in mind, the following principles and recommendations will ensure an environment for IoT that will allow it to evolve in response to the market and technological innovation.

Adopt Policies that Encourage Investment. The IoT could ignite countries' productivity growth and usher in a new era of global competitiveness for industries. But, this opportunity could be lost without the right enabling conditions. To ensure progress, the U.S. government must adopt policies that accelerate IoT investment. Prior phases of the Internet benefitted immensely from a decidedly "hands-off" approach to regulation that allowed investment and innovation to flourish free from regulatory burdens and uncertainty; the same will hold true for the IoT.

Recognize the truly global nature of IoT. The IoT has the potential to create new ecosystems that cut across traditional geographic and industry boundaries and value chains. However, concerns about interoperability or about sending data across borders will impede the potential for deep ecosystem development. The U.S. government should encourage interoperable IoT deployments and facilitate the seamless flow of information across borders. IoT service providers and device manufacturers will require global distribution coverage and managed platforms for adequate scale, economic viability, and the provision of consistent global services.

Ensure the availability of permanent roaming to support IoT. Uncertainty around the availability of permanent roaming to support IoT threatens to hold back IoT deployment and innovation. In fact, permanent roaming likely will be the single most important regulatory issue that is likely to have an immediate impact on the extra-territorial use of IoT. Permanent roaming massively simplifies the process for providing connectivity, and the U.S. government should seek to encourage permissive policies both domestically and abroad.

Maintain a technology- and service-neutral framework across the entire IoT ecosystem. The U.S. government should ensure that policy frameworks are technology- and service-neutral and treat equivalent services similarly. Indeed, end-to-end IoT solutions will require a large number of diverse participants and technologies to work together. Regulators should guard against the impulse to impose legacy tax or regulatory frameworks that are designed for outdated technologies and services on portions of the IoT value chain. At the state and local level, governments should avoid placing undue restrictions on the network deployments that will be necessary to support the IoT. The federal government can help identify and remove such barriers.

Build trust by protecting consumer privacy. Existing, well-established privacy laws and regulations around the world are sufficient to ensure that IoT services align with consumer privacy expectations. In fact, policymakers should curtail the potential for multiple, overlapping, or inconsistent regulators or regulatory frameworks relating to privacy. Privacy considerations that accompany IoT will affect different sectors of the economy, and conflicting, sector-specific regulations will hinder IoT development and deployment.

Support interoperable, industry-developed standards. Standardization is a must for the full vision of IoT to become reality. The U.S. government should support and promote industry-

led, interoperable standards across the IoT industry. Interoperable IoT platforms will reduce costs, facilitate scale, and ensure that customers enjoy intuitive connected experiences.

Make available and harmonize spectrum to support IoT. Spectrum for IoT must be a top priority for policymakers. Policymakers should ensure not only that spectrum is available to support IoT innovation, but that it is harmonized to encourage scale and cost-effectiveness. Harmonized spectrum will lower costs, as manufacturers will have to implement fewer spectrum bands in devices. Meanwhile, uncertainty regarding the availability of spectrum will discourage investment.

17. *How should the government address or respond to privacy concerns about the IoT?*

    a. *What are the privacy concerns raised specifically by IoT? Howe are they different from other privacy concerns?*

    b. *Do these concerns change based on the categorization of IoT applications (e.g., based on categories for question 4, or consumer vs. industrial)?*

    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?*

The coming wave of connected devices raises important questions about consumers' privacy expectations. GSMA and its members have extensive experience protecting consumers' personal information and working with IoT partners, including device manufacturers and mHealth and mEducation service providers, to build in privacy protections up front—right into design specifications and architectures for new systems and processes. Rather than adopt prescriptive privacy rules that could stifle innovation, policymakers should encourage innovators similarly to conceive of and build in features that safeguard consumers and their data, and to communicate appropriate information to consumers.

Before reflexively resorting to IoT-specific regulation, policymakers should allow the IoT to mature under the well-established approaches that already exist to protect privacy. If any

gaps emerge, best practices, self-regulatory efforts, and multistakeholder processes will be more effective than prescriptive rules that could hinder innovation. Regulatory intervention should be limited—if used at all—to identified, demonstrable risks of real consumer harm that are not covered by existing measures.

Policymakers also should guard against the potential for multiple, overlapping, or inconsistent privacy regulations. As discussed above, privacy considerations that accompany IoT may arise in diverse sectors of the economy, potentially inviting multiple regulators to address privacy within industry verticals. This is a recipe for inconsistent and potentially conflicting regulatory mandates that could inhibit innovation and growth of the IoT.

19. *In what ways could IoT affect and be affected by questions of economic equity?*

    a. *In what ways could IoT potentially help disadvantaged communities or groups? Rural communities?*

    b. *In what ways might IoT create obstacles for these communities or groups?*

    c. *What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access?*

    d. *What role, if any, should the government play in ensuring that the positive impacts of IoT reach all Americans and keep the negatives from disproportionately impacting disadvantaged communities or groups?*

Technology has great potential to address inequality and improve lives. For example, through the delivery of remote health and education services, IoT holds immense promise for disadvantaged and rural communities. Integrating IoT features into medical devices will greatly improve the quality of and effectiveness of service while also expanding reach and reducing costs. IoT-enabled remote health monitoring, for example, will allow medical professionals to facilitate early interventions, improve adherence, reduce readmission rates, and reach rural

populations in more efficient and creative ways.[14] Remote education services similarly will simplify access to content and experts, overcoming traditional constraints of time, location, and collaboration.[15]

Smart cities technologies also will significantly improve the quality of life for city residents, including for low-income residents. Among other applications, these services can improve the efficiency and safety of mass transit, improve safety monitoring of public spaces, monitor air and water quality in real time, and provide crucial information to public safety. As discussed above, the U.S. government can unlock these benefits through policies that provide the right incentives for growth and innovation.

F. International Engagement

20. *What factors should the Department consider in its international engagement in:*

a. *Standards and specification organizations?*

b. *Bilateral and multilateral engagement?*

c. *Industry alliances?*

d. *Other?*

GSMA has been active in promoting industry alliances and cooperation in order to encourage ecosystem convergence toward global, industry-led standards for IoT. As described above, GSMA's Mobile IoT Initiative, a project backed by 26 of the world's leading mobile operators, OEMs, and chipset, module, and infrastructure companies, is working to accelerate the commercial availability of mobile IoT technology by facilitating demonstrations, proofs of concept, and trials of a selection of complementary LPWA licensed spectrum technologies. GSMA's Embedded SIM Specification also provides a single, *de facto* standard mechanism for

[14] *See, e.g.*, http://www.telcare.com.

[15] *See, e.g.*, GSMA and McKinsey&Company, Transforming Learning through mEducation (2012).

the remote provisioning and management of M2M connections, allowing "over the air" provisioning.[16] The U.S. government should encourage industry to engage in these types of collaborations and align around interoperable, industry-led standards.

The U.S. government, in turn, should remain vigilant against international IoT activities that could hinder these industry-led efforts. IoT-related issues have gained tremendous traction at the United Nation's International Telecommunications Union ("ITU"), where a newly created study group, Study Group 20 ("SG20"), is focusing on standardization of end-to-end architectures for IoT and mechanisms for the interoperability of IoT applications and data sets. SG20 outcomes could result in ITU-T Recommendations that set *de facto* requirements at the regional or country-specific level—particularly in developing countries—even where the standards have been surpassed by other efforts or by evolving technology. The U.S. government should engage the ITU to ensure that the work of the ITU on IoT does not exceed its mandate and does not duplicate or conflict with other efforts.

21. *What issues, if any, regarding IoT should the Department focus on through international engagement?*

Many countries are moving aggressively on IoT and, as discussed above, regional and intergovernmental organizations also are staking out early roles on IoT policy and technical issues. U.S. diplomacy can best support U.S. innovation and economic growth in IoT by advancing the following policies: (i) promote public policy approaches conducive to investment and innovation in the IoT ecosystem, as described in response to Request 15 above; (ii) promote interoperable, industry-led technical specifications and standards across the IoT industry; and

[16] GSMA, Remote SIM Provisioning for Machine to Machine, *available at* http://www.gsma.com/connectedliving/embedded-sim/.

(iii) promote the use of harmonized spectrum, using both licensed and unlicensed spectrum to ensure operators can deploy the most appropriate technology mix.

22. *Are there Internet governance issues now or in the foreseeable future specific to IoT?*

As a general matter, standards and principles that are applicable to the Internet, including Internet governance, also are applicable to the IoT. To date, the Internet has evolved and flourished under a multistakeholder governance model, in which governments participate on an equal footing with the private sector, civil society, and academia. This open and transparent governance has encouraged broad participation from a wide range of stakeholders and spurred innovation and economic growth that benefits consumers around the world. The IoT undoubtedly presents challenges to traditional Internet governance models, but if it is to develop in manner that continues to ensure an open, secure, and accessible Internet, these challenges must be addressed within the multistakeholder framework.

23. *Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?*

The same policies that will drive IoT development and deployment domestically will ensure its success globally. In fact, efficiencies achieved by economies of scale require that international partners promote an enabling environment for IoT. Thus, the U.S. government should promote the same policies outlined in response to Request 15 with international partners.

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?*

An increasing trend of data localization requirements and other government policies that restrict the seamless flow of information across borders pose a serious risk to the growth of IoT. Many IoT services will rely on reaching global scale to maximize their effectiveness and commercial potential. National or regional rules that restrict data flows or impose localization

requirements will drive up costs and slow deployment, diminishing the scale that IoT can achieve. Such restrictions may also prevent full deployment in the jurisdictions adopting them, thereby reducing the benefits of IoT compared to other, less restrictive countries. The U.S. government must step up efforts to avoid measures that require data localization, wherever they may arise.

III. CONCLUSION

The U.S. government should take actions consistent with these comments to foster the advancement of the IoT both domestically and around the world.

Respectfully submitted,

GSM ASSOCIATION

By: */s/ John Giusti*

John Giusti, Chief Regulatory Officer
GSM ASSOCIATION
2nd Floor
The Walbrook Building
25 Walbrook
London, UK
EC4N 8AF

June 2, 2016