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

Comments of Motorola Solutions, Inc

Introduction

Motorola Solutions, Inc (MSI) appreciates the opportunity to provide comments on the National Telecommunications and Information Administration's (NTIA) Request for Comments on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things". We hope the NTIA will find these comments helpful as it assesses the technology and policy landscape of the Internet of Things as it exists today, and evaluates what role the U.S. Government should play going forward.

While the Internet of Things today might mean different things depending upon the context, in the industrial world it will provide new ways to enhance operations across manufacturing, energy, agriculture, transportation and other critical sectors of the economy. It will also offer new ways to improve the flow of real-time information around an organization, and enable devices to be remotely managed and controlled, raising productivity to new heights while ensuring greater safety for both workers and the community.

Challenges and Opportunities of the Internet of Things

While experiencing exponential growth, the Internet of Things will face a variety of challenges, some of them familiar, and some of them different than have been faced before. The challenges arising from the IoT are familiar in the sense that most of the current technologies still remain in the Logical Layer, thus issues like information security are already a primary concern. However, when connecting physical objects to the Internet and providing them with logical properties like control & monitoring, this introduces a whole new set of concerns and challenges that must be addressed and managed in new ways.

One novel set of technology challenges that will be faced by the IoT relative to existing technology infrastructure and devices includes **scale and data management**. While current technologies are indeed capable of connecting millions of devices to the Internet, storing and managing data derived from these devices will be an immense task. The data being derived from the IoT is different since it is generated by monitoring millions of physical objects. Due to the volume of information being collected, in some cases there is redundant data going over the

network which might “mask” the important data; therefore, advanced technologies involving edge analytics, smart filtering and data analytics are required in order to filter and extract the important data and information.

A second novel technology challenge facing the IoT is **energy consumption.** In some cases “things” are unmanned and deployed throughout a vast geographical area, meaning that replacing a device’s power source or connecting it to the power grid might require a unique approach, thus requiring the “thing” itself and its supporting infrastructure to consume minimal power in order to allow a long time between battery replacements.

The IoT will open up new opportunities in multiple **Technological** areas, including expanding our capabilities in artificial intelligence, data analytics, communications cloud computing, and more. In addition, IoT will likely provide great **Economic** benefits by increasing demand in both the consumer markets and the public sector. Furthermore, since IoT can and will allow operations to be more productive through greater operational efficiency, it can potentially save costs and reduce downtime, potentially saving a great deal of money for businesses.

Internet of Things Definition and Classification

The Internet of Things has been defined in multiple ways, by multiple organizations, and probably needs a little clarification, at least for the sake of this discussion. The Internet of Things might imply that actual physical things are connected to the Internet and will own the same properties like any other data that exists on the Internet (for example the ability to search for a car in a searching engine). Furthermore it implies such things on a large scale. However, while in some cases this is a true statement, in other cases it is not - take an electric grid or a water distribution system, for example - in some cases these “things” (water pumps / electric meters, etc) will be connected over a private network (sometimes even isolated from the Internet) and will serve a primary purpose of collecting real time monitoring data from systems which are not necessarily related to the Internet. In this case, the term “Internet of Things” is interchangeable with the term “Network of Things,” and it can be treated as such.

Generally speaking the Internet of Things is a broad enough term to cover all cases where a physical item/thing is being connected to the network and will provide the user the ability to monitor a device and, in some cases, control it.

Nevertheless the possible reasons to divide different “types” of IoT use cases will derive from different needs - for example:

- Public Safety IoT - will require higher availability and might require higher security standards, and may even require specific frequency allocations
- Medical IoT - could require more extensive certification processes
- Utilities IoT - in some cases utilities will be more “sensitive” for cloud based deployments and will be slower in adopting new tech, hence will be different from Consumer IoT

Advancement of the Internet of Things

The development of IoT is more likely to be hindered by market adaptation rate than by technological issues – as can be shown by mapping the IoT system components:

- Sensors and edge devices - the main technical challenges are:
    - Power consumption - in some cases the sensors will be required to stay operational for a long time without requiring any site visit. We see industry solving this in various ways e.g. providing IoT oriented WAN network which will provide sufficient bandwidth but still not requiring high power utilization
    - Price – we see chipset manufacturing constantly lowering the price of sensors and edge units
- Communications infrastructure - here we also see how the industry is constantly providing solutions for issues like frequency utilization/ power / and price, with examples including LoRA/LTE M, Network virtualization technologies and more
- Data services / Analytics - We see big companies and universities investing a great deal of money to develop better tools to distribute data/ present data and analyze data in ways which are not yet fully utilized by the end users

The past few years have seen changes in business models related to greater infrastructure utilization, and these changes will result in better IoT adaptation, including:

- Selling software as a service or offering cloud platform as a service, which will likely mean more revenue coming from services which includes IoT services, and less revenue coming from hardware - this model will result in the IoT growth in North America.
- Selling radio infrastructure as a service - we see companies building new radio infrastructure which will serve only IoT customers and will collect revenue through network utilization
- There are other more consumer-oriented trends that are changing and will keep changing the way the users get advertisements, buy things and more

.

In addition, we believe that infrastructure providers are rapidly working to prepare for the expected growth of IoT users in their network - we see technologies like network virtualization[1], different flavors of LTE, LTE Gen 5 and more that are currently being deployed and utilized.

[1] Isam Ishaq, Jeroen Hoebeke, Ingrid Moerma, Piet Demeester “Internet of Things Virtual Networks: Bringing Network Virtualization to Resource-constrained Devices,” in *2012 IEEE International Conference on Green Computing and Communications, 2012 Conference on Internet of Things, and 2012 Conference on Cyber, Physical and Social Computing*, pp 293-300

The US government should encourage, and perhaps even enhance where possible, the use of IoT in the following places:

- Safety - We believe IoT can enhance safety with regards to smart transportation, smart roads and vehicles
- Medical - Here the government might play a bigger role in clearing the way for the adoption of medical IoT
- Industrial - The ability to control / monitor and predict system issues within the utility grids can potentially reduce worker injuries and financial losses which can occur due to power/water outages and similar issues by automating the grid where possible

U.S. Industrial Policy and the Internet of Things

As mentioned above there are numerous examples where the IoT can impact industrial practices, with some examples including:

- Power grid automation - here IoT can enable safer and more efficient power distribution, lowering downtime in the grid
- Water distribution and monitoring - Here IoT can allow more productive water distribution, less “water losses” and safer water treatment
- Manufacturing and supply chains are also good examples of industries where the IoT can optimize processes, save costs, and increase efficiencies

Implementing such technologies will raise challenges like:

- Security and data integrity - since many of the verticals within the industrial world provide services for large populations, or provide critical infrastructure to the citizens, the level of cybersecurity and data integrity (at all levels) should be graded higher as compared to the Consumer IoT. This alone will introduce challenges when implementing and migrating existing systems to the IoT

While the growing presence of the IoT may generate more jobs in the software and data sections, it can also lower the demand for “mid/low tech” positions, since many of these processes will become automated or semi-automated.

On the other hand, automating processes and allowing the implementation of IoT tools will raise economic productivity through optimization. IoT solutions can also make workplaces safer by providing sensing capabilities within the workspace through constant environmental monitoring within a workplace or through worker body sensors.

Government policies that might affect IoT are primarily related to how and where data will be stored, the frequency of data utilization, and standards. While some of these policies will help in expediting the IoT market others, such as policies which might require automation of processes within the industrial markets or policies which require cities to utilize safety related sensors, will surely expedite IoT deployment. On the other hand a policy which prevents data from being stored offshore could hinder IoT development.

Cybersecurity and the Internet of Things

Cybersecurity attacks on IoT systems and in particular transportation, utilities and industrial systems are different from regular Cybersecurity attacks since such attacks can affect physical objects like the electrical grid, safety related networks and more.

Cybersecurity concerns are definitely one of the reasons for categorizing the IoT landscape, mainly because each category has different levels of vulnerability. Furthermore, there are IoT applications that will be affected more when attacked - e.g. the power grid, safety applications, etc.

Due to the critical nature of many of these systems, the Federal government should enforce and in some cases finance the usage of cybersecurity protections in critical infrastructure & safety related automated systems.

Conclusion

Motorola Solutions thanks you for this opportunity to provide inputs on the Request for Comments on “The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things”. As noted above, we believe the U.S. Government can best assist the growth of the digital economy by helping to encourage deployment and adoption of IoT in a variety of industrial markets. We also support the encouragement of good cybersecurity practices for the IoT, as this will be a critical concern for the Internet of Things across all areas where it is deployed.