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

Attn: IoT RFC2016
Docket No. 160331306-6306-01
FR Document Number: 2016-11124

June 1, 2016

Comments on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

My name is Riley Walters. I am Research Assistant for cybersecurity and homeland security at The Heritage Foundation. I appreciate the opportunity to provide comments on the National Telecommunications and Information Administration's (NTIA) inquiry to review the current technological and policy landscape for the Internet of Things.[1] The views I express are my own and should not be construed as representing any official position of The Heritage Foundation.

New electronic devices are being connected every day with our mobile phones, personal computers, homes, businesses, street corners, and so on adding to the expansive environment that is the Internet of Things (IoT). The IoT refers to all electronic devices that are connected and communicate information across a network or networks. This can include consumer goods such as wearable devices, a home good such as a smart thermostat, industrial device such as supervisory control and data acquisition (SCADA) systems, and transportation device such as vehicle-to-vehicle (V2V) or vehicle-to-machine (V2M) systems.

Definitions of the IoT vary not only in the specificity of what constitutes as an IoT device but also in the scale of device interconnectedness. A collection of "smart" devices such as phones, smart homes, smart cities, and even smart countries plays into what some have termed the "Internet of Everything."

The exact benefits of a growing IoT are hard to define as the increase in interconnectedness creates new relationships between each IoT stakeholder. However it is easy to see from industry reports an overall positive trend in the growth of the IoT not just for IoT stakeholders, but for local, regional, and global economies by fostering innovation and production efficiencies.

For consumers, the IoT adds value in newer ways of monitoring and managing health better. It means cutting back on power and water over-usage in homes. It means adding better security to homes. And it means streamlining how consumers can manage their daily lives. For businesses, the IoT through monitoring, analytics, and automatization can reduce production downtime, reduce flaws in product manufacturing, and extend production capabilities. Farmers, manufacturers, and shipping industries alike will find benefit through IoT expansion. For regional economies, the IoT has the potential to reduce

[1] *Federal Register*, "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," May 11, 2016, p. 29254, https://federalregister.gov/a/2016-11124 (accessed June 1, 2016).

and mitigate man-made or natural hazards. The IoT has the potential to create a more efficient regional transportation, telecommunication, and utility infrastructure—value adding to the prospect of business investment and regional wealth.

It is clear from the NTIA's request for comment its commitment to understand each stakeholder's definition of the IoT, economic, policy, and social implications, and recommendations for how they view the government's role in the expanding IoT environment. I will attempt to address some of the policy issues that arise from a growing IoT discussed in "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things."

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 proliferation and efficacy of the IoT comes from the immediate sharing of information between devices, an increase in application autonomy, and the benefits to consumers from this increase of functionality.

The number of IoT devices will not only expand in the aggregate but expansion will vary in scope for each individually networked system. In brief we will see a variety of devices, industries, and policy implications continue to converge. This will include some of the most hotly debated issues such as privacy and data, encryption, spectrum, autonomous vehicles, and cybersecurity. Policy implications will reflect the interconnectedness of IoT devices by having spillover externalities throughout the entire IoT policy environment. One policy issue such as privacy will apply not to just consumer goods, but industrial goods, infrastructure goods, and so on.

One way the government in particular will affect the IoT's future is through the numerous agencies that have or will want to have authority to regulate areas on the IoT. The Department of Commerce (DOC) will review the economic implications of increased data and automation. The Federal Trade Commission (FTC) will seek to promote consumer security. The Federal Communications Commission (FCC) will pursue issues of spectrum and how this affects IoT devices. The Department of Homeland Security (DHS) will explore both cyber and physical threats to critical infrastructure. Agencies within the Department of Agriculture (DOA), Department of Energy (DOE), Department of Transportation (DOT), and Department of Health and Human Services (HHS) will each have some role in regard to a growing IoT.

Government will likely come to face jurisdictional challenges in addressing the IoT policies. Each regulatory agency, in crafting new legislation on an issue, may end up conflicting with other newly crafted or pre-existing regulations from other agencies. Government regulators should avoid overarching IoT policies that will conflict across other agency missions. An increase in agency transparency may help address some of the concerns other agencies have regarding how IoT technologies will be impacted. However, government must avoid repetitive or conflicting regulations that will economically harm IoT innovators.

There is also the issue that the legislative and regulatory processes move at a pace much slower than new technology comes to fruition. Private industry must remain undeterred as they continue to foster the IoT environment, as well as take the lead on addressing IoT concerns as they come to fruition. Only when a genuine risk seems to be developing can policymakers consider the full impact of new regulation. This includes both the positive and negative externalities of enacting such regulation, including cost-benefit analyses. Government regulators should refrain from attempting to address newly developing

IoT concerns *ad hoc*; private companies may have already self-remediated the issue and shifted focus onto new emerging issues.

16. How should the government address or respond to cybersecurity concerns about IoT? What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns? How do these concerns change based on the categorization of IoT applications? 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?

Because of the diverse applications seen within the IoT environment—considering the multitude of stakeholders, technologies, and evolving capabilities of malicious actors—there are a number of concerns regarding the cybersecurity of the IoT.

Certainly there is no silver bullet to securing IoT devices as there is no silver bullet to cybersecurity. Cyber risk depends on a combination of factors including what sort of security measures are being continuously added into these devices either in their initial production or through the device lifetime to deter, mitigate, and defeat malicious actors. Other factors include how capable a malicious attacker is and the implication of a successful attack. The implied threat to a single person's Global Positioning System (GPS) coordinates being stolen is inherently different than a car being cyber hijacked with passengers inside on a highway or a dam's sluice gate being opened over a major city.

Many of the cybersecurity implications we face on our desktop computers are similar to those we will face with a growing IoT environment. This can include the threats of ransomware, distributed denial of service (DDoS) attacks, and information stolen and being used against victims in the form of targeted phishing campaigns. As technology becomes more integral to our lives all stakeholders of the IoT, especially the government should continue to emphasize the importance of good cyber hygiene.

One issue specific to the IoT is the interconnection of cyber devices and physical infrastructure. This means that while devices are at risk of traditional cyber threats, physical threats are now possible through successful cyber attacks. Alternatively, IoT device deployment will proliferate to meet the demand of expansive physical infrastructure. Consider the number of traffic sensors needed to be deployed on every street intersection. The increase in IoT devices will increase the attack vector malicious actors can attempt to exploit. It will increase the importance of maintaining the physical integrity of these IoT devices from malicious actors and natural hazards and it will increase the intricacies of information security as each sensor is connected and sharing information.

Device and information integrity is not only important for IoT functionality, but an important emphasis along IoT supply chain production. Malicious software or unintended product deficiencies can negatively harm the final IoT device or IoT system. The government can highlight the important role supply chain security will play as more businesses create and rely on these IoT networked systems.

IoT device developers have economic costs to consider in securing IoT devices, whether that security be cyber or physical in nature. Focusing entirely on security would make IoT investment unprofitable. Being completely void of security could render IoT producers liable for putting consumers at risk. As IoT devices continue to proliferate and security concerns come into question, more and more companies will likely advertise device security as market leverage—mutually beneficial to both the consumer's security and IoT producer brand name.

Ironically, it will be the use of technologies such as online forums and consumer reports that help keep information transparent between the consumer and producers. Government should support this transparency of information.

Of course even consumers and IoT producers can be unaware of how products become unsecure or how malicious actors are finding new ways to breach products' security. Third-party stress tests and reporting on the security of devices can be mutually beneficial to both the consumers and producers. Government should encourage and defer to private industry IoT device security ratings.

The government may also emphasize the importance of securing IoT devices through the product lifetime, as well as the transparency and sharing of threat information regarding both cybersecurity and IoT device security.

20. What factors should the Department consider in its international engagement: Standards and specific organizations? Bilateral and multilateral engagement? Industry alliance? Other?

Sovereign countries and businesses alike will have varying opinions on standardization. It is important that governments allow the standardization of the IoT to remain market driven. Even domestically there can be competition within standardization. Companies are already cooperating to create sets of standards. Countries will emphasize that standardization is necessary for market access. This is true to some degree for assurance, but it can also have limiting factors for those who choose not to adhere to those standards. Or for the country if companies are unwilling to accept the country's preferred standards.

We are already seeing companies working together to establish standards for better cyber and physical security in IoT devices. They are working together and with local governments in the facilitating and growth of IoT networks. Local and regional governments should emphasize their willingness to work with private industry in allowing new IoT technologies to flourish. Consumers benefit from the development and proliferation of IoT devices in their homes, places of work, and throughout their daily lives. It is important that private industry remain untethered as they explore new means and ways of developing and expanding IoT networks.

Conclusion

The IoT environment is not new to the tech world, simply new to the policy world. There are no certainties of how the IoT will develop and benefit each individual directly, but it is certain to benefit both local and regional economies as we see the IoT continue to proliferate. It is important that the slow cycle of legislation and regulatory process remains removed from the high-pace market-driven cycle of technology development. The government should remain as removed for deterring of the innovation and proliferation of the IoT as possible.

I would like to thank the NTIA and the DOC again for allowing me to comment on this developing issue. I am optimistic of how the IoT may change our daily lives for the better. I hope that the government will continue to support private business as they seek innovation and the development of newer IoT products. Governments will also benefit from the proliferation of the IoT, but only so long as it remembers there are negative economic costs with new regulation that can in fact stifle innovation and deter IoT proliferation as well.