usacm ACM US Public Policy Council

Association for Computing Machinery (ACM)
ACM US Public Policy Council (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

June 2, 2016

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

Re: Public comment on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things – Docket No. 160331306-6306-01

Dear NTIA:

Thank you for the opportunity to comment on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things (IoT), 81 Fed. Reg. 19956 (Apr. 6, 2016), Docket No. 160331306-6306-01. We provide responses to specific questions given in the notice.

With more than 100,000 members, ACM (Association for Computing Machinery) is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. These comments were developed by the ACM U.S. Public Policy Council (USACM), which serves as the focal point for ACM's interaction with the U.S. government in all matters of U.S. public policy related to information technology. The membership of the ACM U.S. Public Policy Council is comprised of computer scientists, educators, researchers, and other technology professionals. ACM U.S. Public Policy Council statements represent the views of the Council and do not necessarily represent the views of the Association.

Responses to Specific Questions

Question 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?

The Internet of Things ecosystem is expected to become among the next mainstream computing paradigms, growing exponentially during the next decade. The number of devices and sensors in our physical environments will increase and user interfaces may not be available or visible. New identifiers, components, devices, and infrastructure will raise issues of computing capability, privacy, security, usability, accessibility, spectrum availability, standards, networks and interoperability. These IoT devices and sensors are going to capture an unprecedented variety and density of information. Some may include cyber and/or mechanical control mechanisms that can manipulate the physical environment.

The understated presence of many data collection points combined with ongoing advancements in the ability to correlate this data into meaningful information exceeds the opportunities and risks associated with the capabilities of past technologies. New concerns will involve the responsible use and protection of the data collected, as well as the creation of privacy paradigms that adapt to the ubiquity of IoT environments and user preferences. These concerns are expanded and complicated because IoT systems can and do operate across borders creating challenges for protecting the broader integrity of IoT systems and individual privacy. Fostering and leveraging cooperation among governments and the private sector is vital to achieving an innovative and resilient IoT ecosystem (see Question 20).

The large-scale pervasiveness of the IoT environment and the continuous interaction involved will bring about novel technological challenges. Among these challenges lie new and powerful concerns with privacy and security (see Questions 16 and 17).

Question 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 different interpretations of IoT and what it encompasses reflect the continuing development and evolution of IoT systems and technologies. At least three government agencies – the FTC, FBI, and NIST – agree that interconnectedness is a primary characteristic of IoT and related systems. The agencies' definitions involve a level of interaction among the "things" that they respectively consider part of IoT or related concepts. The agencies also incorporate networked connectivity as part of this interconnectedness. Differences lie, however, with the nature of the connectivity and networked systems and whether connectivity needs to be automatic. They also differ in their interpretations of the scope of IoT and overlapping concepts.

In 2015, the FTC released a staff report titled: "Internet of Things: Privacy & Security in a Connected World."[1] The report outlined consumer risks and benefits associated with IoT. The report used the term IoT "to refer to 'things' such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet."[2] The scope of the report was limited to consumer-related technologies. The agency stated that the report did not cover IoT technologies involved in business contexts.

The FBI addressed IoT in a public service announcement for homeowners and businesses about cybersecurity risks associated with IoT. For this warning, the FBI considered IoT as "any object or device, which connects to the Internet to automatically send and/or receive data."[3] By referring to "any," the

[1] FTC Staff Report: Internet of Things: Privacy & Security in a Connected World (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[2] *Id*. at 5-6.

[3] FBI Public Service Announcement: Internet of Things Poses Opportunities for Cyber Crime (Sept. 10, 2015), http://www.ic3.gov/media/2015/150910.aspx

FBI included a greater variety of devices than the 2015 FTC staff report, which excluded computers, smartphones, and tablets. The FBI also included the condition that devices must send or receive data "automatically." Although IoT devices and sensors may automatically send or receive data, the “things” do not need to be constantly connected. They can connect intermittently. Also, they may not use standard Internet protocols at the system edge; rather, they may be directly or remotely accessed, configured, or operated manually or non-autonomically.

In the NIST draft Framework for Cyber-Physical Systems (CPS), the CPS Public Working Group categorized IoT along with Industrial Internet and other similar systems as overlapping and related concepts of “cyber-physical systems.”[4] The framework did not offer a conclusive definition of IoT. However, because the concepts are often used interchangeably and have "significant overlap," the Working Group asserted that the approaches outlined in the framework are equally applicable to IoT.

A review of the definition of IoT and related concepts has shown a lack of consensus. Given the current and expected technology, we caution against prematurely adopting a definition. We encourage further discussion among government and stakeholders, including businesses, academia, professional societies, consumer advocates, nonprofits, and other civil society organizations on what encompasses the IoT landscape and how it relates to or differs from other related systems.

Question 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?

ACM's conferences, publications, and Special Interest Groups provide forums for computing professionals from around the globe to exchange information on the technical, social, ethical, and policy aspects of IoT.

Some of the ACM Special Interest Groups addressing IoT include the Special Interest Group on Computer-Human Interaction (SIGCHI), the Special Interest Group on Applied Computing (SIGAPP), the Special Interest Group on Spatial Information (SIGSPATIAL), the Special Interest Group on Management of Data (SIGMOD), the Special Interest Group on Mobility of Systems, Users, Data and Computing (SIGMOBILE), the Special Interest Group on Security, Audit and Control (SIGSAC), and the Special Interest Group on Embedded Systems (SIGBED), among others.

Among ACM’s existing publications providing technical and policy information about IoT are articles submitted for an ACM *Ubiquity* symposium on the topic.[5] The symposium articles explore the complex issues of IoT from multiple perspectives, including privacy and security. A forthcoming Special Issue of the ACM Transactions on Computer-Human Interaction (ACM TOCHI) will address end user development for IoT.[6] Further, upcoming ACM conferences and workshops will address topics such as

[4] NIST Cyber-Physical Systems Public Working Group, Draft Framework for Cyber-Physical Systems (Sept. 2015), available at https://pages.nist.gov/cpspwg/.

[5] *Ubiquity* Symposium on "The Internet of Things (IoT)" (2016), http://ubiquity.acm.org/symposia.cfm

[6] Special Issue of ACM Transactions on Computer-Human Interaction (ACM TOCHI) on “End User Development for the Internet of Things” (forthcoming), https://tochi.acm.org/end-user-development-for-the-internet-of-things/

IoT systems in urban spaces,[7] IoT security,[8] and the trustworthiness of embedded devices and sensors within IoT.[9]

Additionally, USACM has formed a working group to address the emerging policy issues related to IoT. The working group will survey the IoT policy landscape and support stakeholder discussions. The group will examine technological issues related to IoT such as interoperability, network, standards, and spectrum. The group will analyze privacy and security concerns unique to IoT.

Question 6. What technological issues may hinder the development of IoT, if any? A) Examples of possible technical issues could include interoperability, insufficient/contradictory/proprietary standards, spectrum availability and potential congestion, availability of network infrastructure or an issue not listed B) What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

Interoperability allows the different components of the IoT ecosystem to function in harmony. Interoperable systems have impacts on privacy and security. The ability for devices and sensors to interact allows vulnerable legacy items to be phased out and replaced with updated components. Conversely, selective non-interoperability can enhance privacy by preventing information flow into certain contexts where privacy might be in peril. There may be contexts in which lack of interoperability should actually be seen as a goal or mitigation rather than an obstacle.

Composability will be a technical issue to consider, particularly given the large number of IoT devices and sensors that interact with each other. As a unit, a device or sensor may meet security, privacy, and safety requirements. However, when combined or integrated with other devices and sensors, as expected in IoT, there is no certainty that these properties will remain. In a composable infrastructure, systems can assemble in a variety of combinations based on user needs. The integration of all these properties and behaviors brings opportunity but also can have unintended consequences for the IoT ecosystem.

It is important to recognize that the value of IoT is in ecosystems rather than the individual component or cross-device interactions. This goes beyond the standard concept of interoperability and composability at the communications or the software level and into information semantics. For example, data within streams that flow between IoT devices and sensors can mean different things to different components.

Data ownership, data maintenance, and data attribution are also important to consider in the development of IoT. These issues raise concerns about data quality, networked storage, and legacy file

[7] Second European Alliance for Innovation (EAI) International Conference on IoT in Urban Space, May 24-25, 2016, Tokyo, Japan (held In-cooperation with ACM SIGAPP, SIGCHI and SIGSPATIAL), http://urbaniot.org/2016/

[8] Theory of Implementation Security Workshop, October 24-28, 2016, Vienna, Austria (co-located with the 23rd ACM Conference on Computer and Communications Security), https://www.cosic.esat.kuleuven.be/events/acm-ccs2016/

[9] Sixth International Workshop on Trustworthy Embedded Devices, October 24-28, 2016, Vienna, Austria (co-located with the 23rd ACM Conference on Computer and Communications Security), http://th.informatik.uni-mannheim.de/trusted-workshop/2016/

formats. Moreover, the large scale of data creation and storage can overwhelm available infrastructure. A challenge that is inherently tied to these considerations is the maintenance of metadata, especially as it concerns data integrity and data ownership. Metadata, referred to as “data about data,” provide context on data. Some of the attributes that may be displayed by metadata are location, owner, domain, or manufacturer. A function of metadata is to provide context that can later be used for applications or analysis. If there are multiple data points for the same item, one may be materially older. Failure to maintain the metadata prevents usage of the most current data, which can have negative effects on later applications of the same data. Similar metadata concerns are associated with permissible use. Unless the premise is that all data collected may be used by everyone, data ownership will pose a serious challenge.

The emergence of IoT happens in a situation of unprecedented globalization where technical issues cross borders. As such, these discussions require coordination across governments (see Question 20).

Question 7. NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why?

The pervasiveness of IoT devices and sensors and their high interconnectedness will make it very difficult and expensive to retrofit and address issues like security, privacy, and safety. Proactively addressing these issues is important. Appropriately crafted principles to help guide technical development can help enable innovation and can help avoid systemic mistakes. We address privacy and security concerns related to these technical underpinnings in Questions 16 and 17.

We urge the federal government to consider prioritizing privacy and security research in IoT. Given that IoT involves many factors, we encourage research that addresses broad solutions.

Question 16. How should the government address or respond to concerns about IoT? A) What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?

The multifaceted nature of IoT brings with it a new set of opportunities and threats. Specific concerns raised by IoT are marked by the pervasiveness and diversity of IoT devices and sensors. IoT crosses virtual boundaries as devices and sensors are now intertwined with consumers’ lives in the physical world. Security threats with IoT have broader implications of physical security and safety risks.

We see the following two distinctive categories of technical, security-related properties that IoT systems introduce:

- **Pervasiveness.** Many IoT systems are already ubiquitous and invisible and may continue this trend as they mature, reducing opportunities for humans to control such systems due to their ubiquity and transparency of operation.
- **Heterogeneity.** IoT systems incorporate a wide variety of interconnected devices that create interoperability challenges. IoT interconnectivity naturally leads to interaction of systems and

components that are built by different vendors, according to different standards, and using different protocols. The magnitude of the diversity in IoT environments is extensive and introduces interoperability challenges that can lead to substantial system vulnerability.

Security threats are critical in the evolving context of the IoT ecosystem. IoT systems have network, device, and data levels that will require unique and tailored security. The limited configuration of certain technologies embedded within IoT may prevent necessary updates. IoT devices are likely to be long-lived (sometimes lasting decades), and will undoubtedly require patches as security issues are identified. Methods to allow updates from reputable sources, sometimes despite low bandwidth network and intermittent connections should be considered as they are necessary for the secure use of IoT devices and sensors, especially over the long term. The vulnerability of these legacy items can have potentially devastating consequences for users. It is imperative that standards and guidelines for the technologies in the IoT environment are able to adapt to the constant changes in IoT environments.

The ubiquitous, heterogeneous nature of IoT raises concerns involving the trustworthiness of the devices and sensors. The trustworthiness includes security, privacy, safety, reliability, and resilience. Trustworthiness poses a greater concern in IoT as devices and sensors continue to proliferate with high interconnectedness and integration.

Question 17. How should the government address or respond to privacy concerns about IoT? A) What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

Meeting the dual imperatives of protecting privacy and security will be an issue for IoT and raises questions on the relationship between cybersecurity and privacy risks. Many privacy risks are interdependent with other types of risks, data actions, and processes. Addressing privacy concerns will entail an understanding of the way privacy risks work in tandem with security risks so as to address risks comprehensively. Five major considerations should be technically addressed within the IoT infrastructure and these include data integrity, identity management, trust management, data protection, and data volume.

- **Data integrity** ensures that data produced and captured in the IoT environment can be trusted and has not been compromised.
- **Identity management** is the administration of identities within an IoT system.
- **Trust management** takes into account the human component of IoT devices and sensors as well as their ubiquity and ensures that the devices and sensors transmitting the data can be trusted. The ubiquity of the devices and sensors may require a multi-value and multi-dimensional approach to trust. Rather than trusted or untrusted, devices and sensors may have varying levels of trust, possibly dynamically determined.
- **Data protection**, from the technical viewpoint, encompasses the guarantee that sensitive information captured in a variety of environments, including information about physical environments, is protected while maintaining the functionality of IoT.
- **Data volume** refers to the massive amounts of data that IoT components capture that directly relate to human activity. The large volume of sometimes highly personal data can be used in unintended ways, like to create detailed predictive profiles of individuals. Moreover, the

availability of IoT data creates new privacy risks when combined with existing data sources such as web and social data that can increase their predictive power by combining online behaviors and behaviors in the physical environment.

As the devices and sensors within the IoT ecosystem become increasingly pervasive, they will contribute to the volume of data available, the velocity at which data will be generated, and the variety of devices and sensors capturing data. The massive collection of data and the new type and amount of data will likely reveal new insights. The disparate individual pieces of information when combined can reveal sensitive patterns that were previously not readily identifiable; this is known as mosaic theory. This raises privacy concerns because data collection, storage, and sharing might expose users to unexpected privacy risks. Furthermore, data that is collected for one purpose may allow inference of other information in ways that users and developers may not expect. As IoT devices and sensors become integrated into daily life, these risks will increase. They will be further exacerbated as algorithmic power progresses and predictive data capabilities continue to grow. We encourage further discussion on the various privacy concerns related to transparency, accuracy, metadata maintenance, user notification, data access, data usage, data attribution, and data sharing.

Question 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?

USACM encourages the Department to consider engaging with a wide range of stakeholders, including from government, the business sector, academia, nonprofits, professional associations, consumer advocates, and civil society. We support involvement of the United States in bilateral and multilateral engagements, international standards processes, and efforts to develop and incentivize voluntary marketplace measures. In particular, we support the involvement of the United States in international standards and processes for cybersecurity and privacy.

Thank you again for the opportunity to comment on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things. The staff and members of the ACM U.S. Public Policy Council are available if you have questions or would like additional information about the issues raised in this public comment.

Sincerely,

Eugene H. Spafford, Ph.D.
Chair
ACM U.S. Public Policy Council

Alec Yasinsac

Alec Yasinsac, Ph.D.
Leader, Working Group on IoT
ACM U.S. Public Policy Council