Association for Computing Machinery (ACM)
ACM US Public Policy Council (USACM)
usacm.acm.org
facebook.com/usacm
twitter.com/usacm

March 13, 2017

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

Re: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things – Docket No. 170105023-7023-01

Dear National Telecommunications and Information Administration:

Thank you for the opportunity to comment on the National Telecommunications and Information Administration (NTIA) green paper "Fostering the Advancement of the Internet of Things," 82 Fed. Reg. 4313 (Jan. 13, 2017), Docket No. 170105023-7023-01. We provide input on the issues raised by the green paper, as well as the proposed approach, current initiatives, and next steps.

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.

Question 1. Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?

We support the Department's cross-cutting guiding principle to ensure the IoT environment is inclusive and widely accessible to consumers, workers, and business. We affirm our commitment to working with the Department to ensure that IoT policy approaches foster digital inclusiveness, accessibility, and usability. We are glad to see the Department advocate for an interoperable IoT environment and encourage IoT growth and innovation. We also commend the Department for working with the range of stakeholders to identify ways to foster privacy and security within a trustworthy IoT environment.

The Department should consider expanding the privacy section to further capture issues related to IoT and big data. IoT components should receive, process, and/or create data that is accurate, consistent, and relevant for the purposes it was collected. Identifying and addressing challenges related to data integrity, completeness, accuracy, and quality is more important than ever due to the ubiquity and heterogeneity of IoT components.

In the section on privacy, we would also like to see addressed challenges related to the sources of data, and data collected, shared, and used by IoT devices and sensors. We agree with commenters that concerns related to IoT and big data are intertwined with security. Because of the likelihood of data to be compromised, challenges related to IoT and big data should include privacy and security. The Department can foster an understanding of verification of data sources, integrity, quality, and accuracy and can ensure that these topics form part of the conversation on IoT privacy challenges.

A trustworthy IoT ecosystem is reliable, resilient, secure, and safe[1] and can significantly improve privacy. Appropriately crafted policies, procedures, and principles will help maintain the highest data integrity and quality as it is collected, implemented, and stored via IoT devices and sensors. Exploiting the full potential of IoT applications will depend on whether data collected is private and secure. We would like to see the Department's commitment to trustworthiness preserved in the final paper and encourage the Department to ensure that current initiatives and next steps recognize the importance of the interdisciplinary nature of trustworthiness in hardware, software, operating systems, applications, compilers, network protocols, cryptography, and human interfaces.

In the green paper, commenters pointed out challenges brought on by IoT and data-driven decision-making. We would like to see the Department address additional issues in relation to data-driven decision-making and algorithmic capabilities. The ACM U.S. Public Policy Council has identified algorithmic transparency and accountability as an important issue that must be taken into serious consideration and has developed a set of principles to address these challenges.[2] As the ubiquity of IoT expands, so will that of algorithms. Algorithmic capability is especially valuable in areas rich with recorded information. However, the use of algorithms for automated decision-making can result in harmful or unintended consequences. We urge the Department to engage stakeholders to address this topic.

We want to highlight the complementary nature of privacy and security. The Department should advance approaches that adopt and support the relationship between privacy and security. We also encourage the Department to promote the inclusion of privacy concerns and security at all stages of the life cycle, from conception through development to deployment. Further, privacy and security must be similarly embedded into associated processes. This will help prevent major systemic mistakes in IoT devices and sensors and minimize the risks of difficult and costly retrofitting. This needs to occur sooner rather than later due to the rapid proliferation of IoT devices and sensors in the environment.

The green paper states that the difficulties and costs of implementing encryption on technically limited devices drew attention from commenters. In this regard, we urge the Department to continue to monitor NIST's lightweight cryptography project[3] and to consider advancements in cryptographic

[1] NIST Special Publication 800-183, Networks of 'Things' (July 2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
[2] ACM U.S. Public Policy Council, Statement on Algorithmic Transparency and Accountability (January 2017), https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf
[3] NIST Lightweight Cryptography, https://www.nist.gov/programs-projects/lightweight-cryptography

ACM US Public Policy Council
1701 Pennsylvania Ave NW, Suite 300
Washington, DC 20006

+1-202-355-1291 x13040
acmpo@acm.org
usacm.acm.org

coprocessors. These options may lessen the challenges of encryption on devices with limited computational and energy resources.

The Department has already taken steps to address the challenges of IoT security upgradability and patching. We encourage the Department to address the privacy and security risks associated with IoT devices and sensors that are discarded, orphaned, damaged, or nonfunctioning. As part of the multistakeholder process on IoT security, participants have identified issues with small producers and end-of-life products as areas of further focus. The Department should also consider that there might be sensitive data stored in these obsolete IoT components. Abandoned or legacy technology might pose threats to data privacy and security risks to existing or new IoT components. Abandoned, discarded, and orphaned IoT components may have extended life and range of operation due to advancements in power sources and connectivity. We encourage the Department to consider addressing the security, safety, and privacy implications of these capabilities in the final paper and in future actions.

We agree with the Department that interoperability is an important feature of the IoT ecosystem and want to note that interoperability, or lack thereof, should be addressed. Commenters noted that some device manufacturers limit interoperability for market advantage. The Department should consider that intentionally non-interoperable systems could limit data flows in situations where it is necessary to limit information exchange.

In the IoT ecosystem, each component has its own privacy and security properties. How the properties of the individual components interact needs to be understood and accounted for in the design of the larger system. This is an additional point of consideration for the Department. The fact that individual components exhibit specific required privacy and security properties does not necessarily imply that the system as a whole will exhibit those properties as a result of component interactions.

Question 2. Is the approach for Departmental action to advance the Internet of Things comprehensive in the areas of engagement? Where does the approach need improvement?

The Department identifies four broad areas of engagement to advance IoT. We suggest the following activities and initiatives for three of the engagement areas:

- **Enabling Infrastructure Availability and Access**
  As IoT continues to proliferate at an impressive rate, we support the Department's plans to work on IoT matters related to the increased demand on the country's infrastructure, connectivity, and spectrum. Addressing issues of increased demand will be helpful for IoT deployment and scalability.

- **Crafting Balanced Policy and Building Coalitions**
  Consistency and coordination are particularly important in the complementary areas of privacy and security. The Department has stated that it will encourage IoT growth and innovation by convening stakeholders to address public policy challenges. We agree that IoT policy approaches will require coordinated engagement by stakeholders from the technical community,

government, the private sector, academia, nonprofits, professional associations, consumer advocates, and civil society. For this multistakeholder approach to be successful, the Department should continue to ensure neutral facilitation so that no group of stakeholders is disadvantaged.

- **Promoting Standards and Technology Advancement**
  We support the Department's ongoing engagements to support global IoT interoperability and commitment to encourage the growth and innovation of IoT while protecting privacy, security, intellectual property, and other aspects.

Question 3. Are there specific tasks that the Department should engage in that are not covered by the approach?

We encourage the Department to consider and promote the complementary relationship between privacy and security in current Department initiatives and the next steps for each engagement area.

Question 4. What should the next steps be for the Department in fostering the advancement of IoT?

We propose the following next steps for the Department to consider in fostering the advancement of IoT:

- We encourage the Department to review existing technical and engineering approaches in relevant domains, including safety, security, and privacy. The body of relevant work from NIST is worth considering.[4] We also believe that maintaining a pluralistic perspective open to different models and methods that might be applied to IoT is essential.

- We encourage the Department to convene multistakeholder processes on IoT data collection and analytics challenges.

- We urge the Department to proactively support that privacy and security are complementary and to reflect this stance across all areas of engagement.

- The Department should continue to promote a trustworthy IoT environment and to consider the interdisciplinary nature of trustworthiness.

[4] For example: Introduction to Privacy Engineering and Risk Management in Federal Systems (January 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

Thank you again for the additional 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,

Stuart S. Shapiro, Ph.D.
Chair, ACM U.S. Public Policy Council
Association for Computing Machinery

ACM US Public Policy Council
1701 Pennsylvania Ave NW, Suite 300
Washington, DC 20006

+1-202-355-1291 x13040
acmpo@acm.org
usacm.acm.org