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

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

July 28, 2017

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW., Room 4725
Attn: Evelyn L. Remaley, Deputy Associate Administrator
Washington, DC 20230

Re: Public comment on promoting stakeholder action against botnets and other automated threats – Docket No. 170602536-7536-01

Dear NTIA:

Thank you for the opportunity to comment on promoting stakeholder action against botnets and other automated threats, 82 Fed. Reg. 27042 (June 13, 2017), Docket No. 170602536-7536-01. The Notice states that as new scenarios emerge, including those exploiting a new generation of "Internet of Things" (IoT) devices, there is an urgent need for coordination and collaboration across a diverse set of ecosystem stakeholders. We provide the ACM U.S. Public Policy Council (USACM) and the ACM Europe Council Policy Committee (EUACM) joint Statement on IoT Privacy and Security addressing existing and expected privacy and security concerns in the IoT ecosystem.

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 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 USACM is comprised of computer scientists, educators, researchers, and other technology professionals.

EUACM is a standing committee of ACM Europe. It serves as the focal point for ACM's interactions with governmental bodies in Europe, the computing community, and the public in matters of European public policy related to computing and technology.

USACM statements represent the views of the Council and do not necessarily represent the views of the Association. EUACM statements represent the views of the Committee and do not necessarily represent the views of the Association.

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

Statement on Internet of Things Privacy and Security

by ACM U.S. Public Policy Council and ACM Europe Council Policy Committee

Internet of Things (IoT) systems have rapidly assumed important roles in daily life by providing new capabilities to streamline diverse tasks. IoT catalyzes new capabilities and creates opportunities for increased productivity and societal benefits.

As the IoT ecosystem unfolds, this wide range of functions and components will result in significant privacy and security challenges that should be addressed. Large-scale, pervasive networks that collect data about the world around us and new predictive technologies and algorithms enable innovative IoT uses. Yet, the data collected from IoT devices and algorithms that use this data for decision-making can result in unintended consequences. The ubiquity of IoT also presents new security and privacy concerns, making it important to incorporate privacy and security controls into the life cycle of IoT devices.

Certain IoT components have minimal functionality, limited computational power and storage, and low energy resources, which can sometimes make conventional security and privacy protections difficult to deploy. Such deployments may need to take advantage of new protocols and system designs that are better equipped to operate in resource-limited environments.

Policy and technical approaches to emerging IoT privacy and security challenges should continue to encourage innovation while ensuring that consumer confidence in these devices and systems is bolstered by strong privacy and security practices. The principles outlined in this statement provide an approach for addressing privacy and security challenges in the IoT ecosystem:

Support Privacy and Security Throughout the IoT Device Life Cycle

- **Address privacy and security risks throughout the IoT device life cycle:** Addressing IoT privacy and security challenges from requirements specification to end-of-life, including across changes in maintenance ownership, can help prevent systemic vulnerabilities and avoid difficult retrofitting. Manufacturers and solution providers should conduct scheduled privacy and security assessments and ensure the efficacy of privacy and security measures prior to deployment and regularly over the course of a device's life span.

- **Ensure continuous, reliable device operation:** The failure of IoT systems can cause irreparable damage and have serious implications for physical safety. The pervasiveness of IoT systems in the everyday lives of consumers raises the stakes. IoT device manufacturers should aim to deploy reliable and dependable systems.

- **Provide regular patches, upgrades, and software updates:** IoT components may ship with vulnerabilities, and new vulnerabilities may be discovered over time; manufacturers are encouraged to provide mechanisms to maintain the privacy and security of IoT components throughout their life cycle. It is similarly important to build consumer understanding and awareness on the importance of software upgrades and to encourage manufacturers to deploy patching and software updates whenever possible.

- **Consider issues with abandoned, orphaned, and legacy components:** Manufacturers should monitor concerns related to abandoned or legacy technology that can pose privacy and security threats to existing or new components as new vulnerabilities arise.

Develop New Technologies to Support IoT Privacy and Security

- **Support flexible access control:** IoT components, especially those without user interfaces, should support secure and private interactions and updates. The IoT ecosystem needs flexible approaches to access controls that foster privacy and security.

- **Leverage advances in cryptography and cybersecurity:** Technically-limited IoT components may benefit from advances in "lightweight" cryptography and new encryption implementations. These options are less resource intensive and therefore more usable within the constraints imposed by many IoT components.

Protect Consumer Data

- **Address data ownership:** The ubiquity of IoT components means an increase in the scale of data captured, shared, collected, and analyzed. Stakeholders should plan for future challenges of data ownership as they relate to privacy, security, and intellectual property.

- **Build consumer awareness about privacy and data sources:** As IoT permeates consumers' lives, it will be important to educate consumers on the privacy and security issues that IoT presents and on how to best protect themselves from attacks. Organizations should be transparent to consumers about how data about them is collected, used, retained, and shared.

- **Protect data integrity:** IoT components should receive, process, and create data that is accurate, consistent, and relevant for the purposes for which it was collected or produced.

Foster Cooperation Among Stakeholders

- **Promote an interdisciplinary approach to trust:** Hardware and software engineering, cryptography, human factors, and social science can all contribute to fostering a safe, secure, and trustworthy IoT ecosystem.

- **Encourage coordinated efforts among stakeholders:** Improved coordination between the public and private sectors can foster IoT innovation and protect privacy and security. Cooperation among governments and other stakeholders, including businesses, academia, professional societies, consumer advocates, nonprofits, and other civil society organizations will help drive and realize IoT innovation. Similarly, technical issues cross borders and require international coordination and cooperation.

Thank you again for the opportunity to comment on promoting stakeholder action against botnets and other automated threats. The staff and members of USACM 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