Billing Code 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Docket No. 160331306-6306-01

RIN 0660-XC024

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

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice, Request for Public Comment.

SUMMARY: Recognizing the vital importance of the Internet to U.S. innovation, prosperity, education, and civic and cultural life, the Department of Commerce has made it a top priority to encourage growth of the digital economy and ensure that the Internet remains an open platform for innovation. Thus, as part of the Department's Digital Economy Agenda, the National Telecommunications and Information Administration (NTIA) is initiating an inquiry regarding the Internet of Things (IoT) to review the current technological and policy landscape. Through this Notice, NTIA seeks broad input from all interested stakeholders — including the private industry, researchers, academia, and civil society — on the potential benefits and challenges of these technologies and what role, if any, the U.S. Government should play in this area. After analyzing the comments, the Department intends to issue a "green paper" that identifies key issues impacting deployment of these technologies, highlights potential benefits and challenges, and identifies possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector.

DATES: Comments are due on or before 5 p.m. Eastern Time on [insert date 45 days after publication in the *Federal Register*].

ADDRESSES: Written comments may be submitted by email to iotrfc2016@ntia.doc.gov. Comments submitted by email should be machine-readable and should not be copy-protected. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue N.W., Room 4725, Attn: IOT RFC 2016, Washington, DC 20230. Responders should include the name of the person or organization filing the comment, as well as a page number on each page of their submissions. All comments received are a part of the public record and will generally be posted to http://www.ntia.doc.gov/category/internet-policy-task-force without change. All personal identifying information (for example, name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information. NTIA will accept anonymous comments.

FOR FURTHER INFORMATION CONTACT: Travis Hall, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4725, Washington, DC 20230; telephone (202) 482-3522; email thall@ntia.doc.gov. Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482-7002.

SUPPLEMENTARY INFORMATION:

Background: As part of the Department of Commerce's Digital Economy Agenda, the National Telecommunications and Information Administration (NTIA) is requesting comment on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things (IoT).

Description of IoT and its Impact on the Economy: IoT is the broad umbrella term that seeks to describe the connection of physical objects, infrastructure, and environments to various identifiers, sensors, networks, and/or computing capability.[1] In practice, it also encompasses the applications and analytic capabilities driven by getting data from, and sending instructions to, newly-digitized devices and components.

Although a number of architectures describing different aspects or various applications of the IoT are being developed, there is no broad consensus on exactly how the concept should be defined or scoped. Consensus has emerged, however, that the number of connected devices is expected to grow exponentially, and the economic impact of those devices will increase dramatically.[2] While some types of devices will fall into readily identifiable commercial or public sectors in their own right – for example, implantable health devices – most will serve the function of enabling existing industries to better track, manage, and automate their core functions. The potential health, safety, environmental, commercial, and other benefits of IoT are enormous, from reducing the risk of automobile-related injuries and fatalities to enabling micro-cell weather forecasting. IoT has the potential to catalyze new user applications and give rise to new industries. For example, IoT is the foundation for "Smart Cities" efforts, which use

---

[1] The term was initially coined by Kevin Ashton in 1999 in a presentation at Proctor and Gamble in reference to radio-frequency identification tags (RFIDs). *See* Kevin Ashton, *That 'Internet of Things' Thing*, RFID Journal (June 22, 2009), http://www.rfidjournal.com/articles/view?4986.

[2] In 2003, there were only around 500 million connected devices, but by 2015 there were around 25 billion connected devices. Devices now outnumber people by 3.5 to 1. (Intel, *A Guide to the Internet of Things Infographic*, available at http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html). It is expected by 2020 that there will be up to 200 billion connected devices and these devices will outnumber people by 26 to 1. The McKinsey Global Institute estimates that the cross-sector impact of IoT technologies will be between $3.9 trillion and $11 trillion by 2025. *See* James Manyika et al, *Unlocking the Potential of the Internet of Things*, McKinsey & Co. (June 2015), http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.

pervasive connectivity and data-driven technologies to better manage resources, meet local

challenges, and improve quality of life.

However, the IoT also presents challenges,[3] which in turn have begun to generate initial

thinking and policy responses both inside and outside of government. A number of Federal

agencies – for example, the National Highway Traffic Safety Administration (NHTSA) and the

Food and Drug Administration (FDA) – have already begun grappling with potential health,

safety, and security issues arising from the connection of cars and medical devices to the

Internet.[4] The Federal Trade Commission (FTC) has identified privacy and cybersecurity

aspects of IoT, and proposed some possible best practices.[5] Pursuant to the White House Smart

Cities Initiative, the U.S. Government is providing $35 million in new grants and nearly $70

million in new spending on Smart Cities across several departments.[6] Additional activities at the

federal level seek to take advantage of the potential opportunities as well as address any possible

issues raised by the deployment of IoT in relation to agency missions. IoT has also garnered

---

[3]See, for example, the concerns laid out by the National Security Telecommunications Advisory Committee (NSTAC) in *NSTAC Report to the President on the Internet of Things* (Nov. 2014), pg. 21-22.
https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

[4]*See* U.S. Dept. of Health and Human Services, *Radio Frequency Wireless Technology in Medical Devices: Guidance for Industry and Food and Drug Administration Staff* (Aug. 14, 2013),
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ ucm077272.pdf; *see also* NHTSA, *Vehicle-to-Vehicle Communications* (last accessed March 9, 2016), http://www.safercar.gov/v2v/index.html.

[5] Federal Trade Comm'n, *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, FTC (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

[6] The White House, *FACT SHEET: Administration Announces New "Smart Cities" Initiative to Help communities Tackle Local Challenges and Improve City Services*, The White House Office of the Press Secretary (Sept. 14, 2015), https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

interest by other national governments, standards organizations, and intergovernmental organizations that are interested in understanding how to engage in the IoT ecosystem to encourage economic growth and innovation.[7] Unfortunately, country specific strategies threaten the possibility of a global patchwork of approaches to IoT, which would increase costs and delay the launch of new products and services, dampening investment. The U.S. government will need to work with stakeholders to develop industry-driven solutions; however, thus far no U.S. government agency is taking a holistic, ecosystem-wide view that identifies opportunities and assesses risks across the digital economy.

The Department's Digital Economy Initiatives: More than six years ago, the Department created the Internet Policy Task Force (IPTF) to identify and address leading public policy and operational challenges in the Internet ecosystem. The IPTF collaborates across bureaus at the Department, seeks public comment, and has produced policy papers on a variety of important topics.

In recognition of the broad impact that the Internet and digitization are having across the economy, in 2015 the Department created the Digital Economy Leadership Team (DELT). Comprised of senior officials from across the Department, the DELT provides high-level guidance and coordination, leveraging the substantial expertise within the agency to promote initiatives that have a positive impact on the digital economy and society. The DELT currently focuses on the four pillars of the Department's 2015-16 Digital Economy Agenda: promoting a free and open Internet worldwide; promoting trust and confidence online; ensuring Internet access for workers, families, and companies; and promoting innovation in the digital

---

[7] For example, the Internet Engineering Task Force (IETF), International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and ISO and IEC's Joint Technical Committee 1 (ISO/IEC JTC1) and the International Telecommunications Union's Standardization Sector (ITU-T) have initiated discussion and work related to IoT.

economy. Working closely together, the DELT and IPTF ensure that the Department is helping businesses and consumers realize the potential of the digital economy to advance growth and opportunity.

Given the cross-cutting nature of the IoT landscape, the Department of Commerce — through the DELT and IPTF — is able to provide important perspective and expertise on IoT. The mission of the Department is to help establish conditions that will enable the private sector to grow the economy, innovate, and create jobs. The Department also has statutory authority, expertise, and ongoing work streams in numerous areas that are critical to the development of IoT, including: cybersecurity, privacy, cross-border data flows, spectrum, international trade, advanced manufacturing, protection of intellectual property, standards policy, Internet governance, big data, entrepreneurship, and worker skills. For example:

- The Department has long standing technological and policy expertise and experience that it is applying to IoT. The Department's National Institute of Standards and Technology (NIST) has coordinated the development of a draft reference architecture for Cyber-Physical Systems and is conducting a Global City Teams Challenge to foster the development of Smart Cities and promote interoperability. NTIA's spectrum planning and management activities contemplate the growth of IoT and its Institute for Telecommunications Sciences (ITS) has begun testing the possible effects of IoT on spectrum usage. Both NIST and NTIA have been actively engaged with international standards bodies and international organizations on aspects of IoT and other related areas (e.g., cybersecurity), and have been further engaged with other Federal agencies.

- The Economic Development Administration (EDA) provides grants to communities around the country to build up their technology-focused innovation ecosystems in order to grow their local economies and create jobs.

- The U.S. Patent and Trademark Office (USPTO) continues to improve its patent quality, especially in new technological domains, including IoT. USPTO also plays a key role in the alignment of intellectual property policies around the world, so that U.S. inventors of IoT technology can have access to the protections they need to continue innovating and sell their products and services everywhere.

- The International Trade Administration (ITA) is an active promoter of IoT and Smart Cities on the international stage, including participation in the CS Europe Smart Cities Initiative and working with the other Federal agencies to consider innovative financing mechanisms for Smart City projects. ITA hosts roundtables on an ad hoc basis with the private sector and federal partners to discuss Smart Cities and infrastructure financing. In addition, ITA's Office of Textiles and Apparel is holding a Smart Fabrics Summit (http://smartfabricssummit.com/) on April 11, 2016.

The Department, through this RFC and subsequent green paper, will capitalize on the Department's experience and holistic economic perspective to craft an approach to IoT and its potential impacts that will best foster IoT innovation and growth. Where relevant, comments received may also inform the work of other federal initiatives, such as the recently created Commission on Enhancing National Cybersecurity.

Request for Comment:

Instructions for Commenters: The Department invites comment on the full range of issues that may be presented by this inquiry, including issues that are not specifically raised in

the following questions. Commenters are encouraged to address any or all of the following questions. To the extent commenters choose to respond to the specific questions asked, responses should generally follow the below structure and note the number corresponding to the question. Comments that contain references to studies, research, and other empirical data that are not widely published should include copies of the referenced materials with the submitted comments.

For any response, commenters may wish to consider describing specific goals or actions that the Department of Commerce, or the U.S. Government in general, might take (on its own or in conjunction with the private sector) to achieve those goals; the benefits and costs associated with the action; whether the proposal is agency-specific or interagency; the rationale and evidence to support it; and the roles of other stakeholders.

General:

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?

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.[8] 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?

3. With respect to current or planned laws, regulations, and/or policies that apply to IoT:

   a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?

   b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.

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?

Technology: Technology is at the heart of IoT and its applications. IoT development is

---

[8] Federal Trade Comm'n, *Internet of Things: Privacy and Security in a Connected World*, FTC (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Abdella Battou, *CPS PWG: Reference Architecture*, National Institute of Standards and Technology (accessed March 9, 2016), http://www.nist.gov/cps/cpspwg_refarch.cfm.

being driven by a very diverse set of stakeholders whose expertise in science, research, development, deployment, measurements and standards are enabling rapid advances in technologies for IoT. It is important to understand what technological hurdles still exist, or may arise, in the development and deployment of IoT, and if the government can play a role in mitigating these hurdles.

6. What technological issues may hinder the development of IoT, if any?

    a. Examples of possible technical issues could include:

        i. Interoperability

        ii. Insufficient/contradictory/proprietary standards/platforms

        iii. Spectrum availability and potential congestion/interference

        iv. Availability of network infrastructure

        v. Other

    b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

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?

Infrastructure: Infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services.

8. How will IoT place demands on existing infrastructure architectures, business models, or stability?

9. Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?

10. What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?

Economy: IoT has already begun to alter the U.S. economy by enabling the development of innovative consumer products and entirely new economic sectors, enhancing a variety of existing products and services, and facilitating new manufacturing and delivery systems. In light of this, how should we think of and assess IoT and its effects? The questions below are an effort to understand both the potential economic implications of IoT for the U.S. economy, as well as how to quantify and analyze the economic impact of IoT in the future. The Department is interested in both the likely implications of IoT on the U.S. economy and society, as well as the tools that could be used to quantify that impact.

11. Should the government quantify and measure the IoT sector? If so, how?

    a. As devices manufactured or sold (in value or volume)?

    b. As industrial/manufacturing components?

    c. As part of the digital economy?

        i. In providing services

        ii. In the commerce of digital goods

    d. In enabling more advanced manufacturing and supply chains?

    e. What other metrics would be useful, if any? What new data collection tools might be necessary, if any?

    f. How might IoT fit within the existing industry classification systems? What new sector codes are necessary, if any?

12. Should the government measure the economic impact of IoT? If so, how?

    a. Are there novel analytical tools that should be applied?

    b. Does IoT create unique challenges for impact measurement?

13. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?

    a. What will be the benefits, if any?

    b. What will be the challenges, if any?

    c. What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?

14. What impact (positive or negative) might the growth of IoT have on the U.S. workforce? What are the potential benefits of IoT for employees and/or employers? What role or actions should the government take in response to workforce challenges raised by IoT, if any?

Policy Issues: A growing dependence on embedded devices in all aspects of life raises questions about the confidentiality of personal data, the integrity of operations, and the availability and resiliency of critical services.

15. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

16. How should the government address or respond to cybersecurity concerns about IoT?

    a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?

    b. How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

c. 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?

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?

b. Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

c. 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 privacy and the IoT?

18. Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?

19. In what ways could IoT affect and be affected by questions of economic equity?

a. In what ways could IoT potentially help disadvantaged communities or groups? Rural communities?

b. In what ways might IoT create obstacles for these communities or groups?

c. What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access?

d. What role, if any, should the government play in ensuring that the positive impacts of IoT reach all Americans and keep the negatives from disproportionately impacting disadvantaged communities or groups?

International Engagement: As mentioned earlier, efforts have begun in foreign jurisdictions,

standards organizations, and intergovernmental bodies to explore the potential of, and develop standards, specifications, and best practices for IoT. The Department is seeking input on how to best monitor and/or engage in various international fora as part of the government's ongoing efforts to encourage innovation and growth of the digital economy.

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?

21. What issues, if any, regarding IoT should the Department focus on through international engagement?

22. Are there Internet governance issues now or in the foreseeable future specific to IoT?

23. Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?

24. What factors can impede the growth of the IoT outside the U. S. (e.g., data or service localization requirements or other barriers to trade), or otherwise constrain the ability of U.S. companies to provide those services on a global basis? How can the government help to alleviate these factors?

Additional Issues:

25. Are there IoT policy areas that could be appropriate for multistakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity?

26. What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the Department of

Commerce best collaborate with stakeholders on IoT matters?

27. How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would an overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?

28. What are any additional relevant issues not raised above, and what role, if any, should the Department of Commerce and, more generally, the federal government play in addressing them?

Dated: April 1, 2016.

/s/

Lawrence E. Strickling,

Assistant Secretary for Communications and Information.