C_TEC

U.S. Chamber of Commerce
Technology Engagement Center

Questions for the Record from Hearing Entitled
"Internet of Things Legislation"
U.S. House Energy and Commerce Committee,
Subcommittee on Digital Commerce and Consumer Protection

Responses from Tim Day
Senior Vice President
Chamber Technology Engagement Center ("C_TEC")
U.S. Chamber of Commerce

July 11, 2018

Questions from Chairman Robert Latta

1. *In your opinion, are current efforts, both in the government and among private groups, on IoT issues siloed? Do you believe the SMART IoT Act will help improve collaboration?*

Answer: C_TEC applauds the efforts of Chairman Latta and the Digital Commerce and Consumer Protection Subcommittee to bring about greater collaboration among agencies with regard to the Internet of Things ("IoT") by introducing the SMART IoT Act. Regulatory certainty provides an environment in which innovation and technology can thrive. When technology developers and producers are subject to a patchwork of vague, duplicative or contradictory agency regulations, the pace of innovation slows.

IoT and other internet-connected technology have changed the regulatory landscape for companies that traditionally were regulated by one agency. Now for instance, a company making a device for connected cars could be subject to consumer protection regulations at the Federal Trade Commission ("FTC"), transportation safety regulations at the National Highway Traffic Safety Administration, and spectrum allocation rules at the Federal Communications Commission ("FCC").

While agencies like the FCC and FTC are working together on issues such as internet regulation,[1] the rise of multi-agency jurisdiction over IoT requires policies that increase collaboration. The SMART IoT Act is a step in the right direction toward providing regulators and industry stakeholders information on which agencies are involved in IoT. This information can also inform Congress on ways to streamline and improve IoT regulation.

2. *The SMART IoT Act directs the Secretary of Commerce to conduct a study on the IoT ecosystem—both at the public and private level—so that we can create a single source of information on who is doing what in the IoT space. How do you see this benefiting future policy efforts in this area?*

Answer: C_TEC strongly supports the expansion of publicly available government data to solve our nation's challenges.[2] C_TEC applauds the introduction of the SMART IoT Act and its aim to improve information access to Congress and stakeholders about IoT. The SMART IoT Act has the potential to provide Congress with the information necessary to address conflicting and duplicative regulation by assessing which regulatory bodies are engaging the IoT ecosystem.

Questions from Representative Michael Burgess

1. *Sector-based Information Sharing and Analysis Centers (ISAC) have been successful in coordinating information sharing between private sector critical infrastructures and the government. These ISACs help industry protect from cyber and physical threats, as well as coordinate responses with government, when appropriate.*

   a. *Will the study on the internet-connected devices industry evaluate the feasibility of establishing an Internet of Things ISAC?*

Answer: The U.S. Chamber of Commerce believes that it is possible the SMART IoT Act could lead to evaluating the feasibility of establishing an IoT ISAC.

   b. *Would it be appropriate to recognize the Internet of Things Environment as critical infrastructure? If so, what barriers currently exist?*

Answer: IoT technology will have an enormous impact on the national and world economy. By some accounts, "the IoT has a total potential economic impact of $3.9 trillion to $11 trillion a year by 2025."[3] IoT technology is being deployed to enhance

[1] FCC-FTC Memorandum of Understanding (December 14, 2017) *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/fcc_fcc_mou_internet_freedom_order_1214_final_0.pdf.

[2] *See, e.g.* Coalition Letter Supporting OPEN Government Act (April 5, 2017) *available at* http://www2.datainnovation.org/2017-OPEN-gov-data-act-support-letter-full.pdf.

[3] McKinsey Global Institute, Report, Unlocking the Potential of the Internet of Things, at 2 (Jun. 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-ofdigitizing-the-physical-world.

public safety as well. For example, cities are now using IoT technology to detect gunshots.[4] IoT will also greatly assist health care professionals to provide services to patients with geographical barriers.

Recognizing the economic and public welfare benefits of IoT technology, nevertheless the Chamber believes that it is premature, given the nature of this fledgling and diverse technology, to determine whether it would be appropriate to designate the entire IoT ecosystem as critical infrastructure.

2. *In the past few years, vulnerabilities in information technology systems and programs have led to large-scale cyber-attacks. Often, devices and applications are produced for government and public use by the same company. Will the results of the study help determine the level of vulnerability in the current Internet of Things environment?*

Answer: The Chamber believes that it is possible that the results of the study directed by the SMART IoT Act will help determine the level of cybersecurity vulnerabilities in the IoT environment. The study could enable Congress and other policymakers to learn from the private sector about how companies are identifying security threats and vulnerabilities.[5]

With regard to IoT, the Chamber's members have developed the following security principles[6]:

- Any approach to IoT security should be data-driven, based on empirical evidence of a specific harm, and adaptable both overtime and cross-border.
- Security demands should never be used as industrial policy to advance protectionism or favor national economic interests.
- National boundaries need not become arbitrary obstacles to the movement of devices or data, or to the offering of IoT-related services.
- Global standards are the best way to promote common approaches and technology solutions. Such standards should be open, transparent, and technology-neutral.
- Any government IoT strategy should promote technical compatibility and interoperability to the maximum extent possible.
- Everybody is vulnerable; cyber threats must be met with global information sharing and collaboration to improve and safeguard the IoT ecosystem.
- End users need to be educated about their roles and responsibilities in this digital age.

[4] Stephen Shankland, "The Internet of Things knows when gunfire happens," CNET (July 27, 2014) *available at* https://www.cnet.com/news/internet-of-things-becomes-gunfire-locating-tool-for-cities/.

[5] *See, e.g.*, Andrew Ross, "Fico release free cyber security ratings service to companies worldwide," Information Age (June 19, 2018) *available at https://www.information-age.com/fico-cyber-security-rating-123473126/*; Brian Nordli, "How engineers at NSS labs put the 'security' in cybersecurity," Built in Austin (May 30, 2018) *available at* https://www.builtinaustin.com/2018/05/30/NSS-Labs-Engineering-Spotlight.

[6] Principles for IoT Security, U.S. Chamber of Commerce (September 19, 2017) *available at* https://www.uschamber.com/IoT-security.

- Manufacturers and vendors should be encouraged to routinely evaluate and improve endpoint security.
- The international community must collectively condemn criminal activities that infect and exploit the openness and connectivity of the internet and our digital future.
- Governments must work together to shut down illegal activities and bring bad actors to justice.

3. *Earlier this year we held a Disruptor Series hearing that explored manufacturing applications of IoT. Can you explain the potential you see in industrial IoT and how the optimization of manufacturing benefits not only businesses, but also consumers?*

Answer: According to one study by Accenture, the industrial IoT technology has the potential to add at least $10.6 trillion in global GDP by 2030.[7] The Chamber's members have emphasized that manufacturers and their supply chain partners are increasingly recognizing the transformational role of IoT solutions in driving growth and improving performance in several areas including:

- Increasing total production and throughput;
- Improving the ability to adjust fluctuating market demand;
- Increasing the number of product variants;
- Increasing visibility across a given business enterprise; and
- Decreasing the cost of production and eventually, prices to consumers.

All of these benefits converge to drive higher levels of productivity for individual workers, companies, industrial sectors and, over time, the overall American economy. These benefits operate to make the United States a better place to locate manufacturing and other high-wage jobs. This leadership in industrial IoT can be fostered by forward-thinking government policies that can be informed by the SMART IoT Act.

[7] Mark Purdy and Ladan Davarzani, "The Growth Game-Change: How the Industrial Internet of Things can Drive Progress and Prosperity," at 5, Accenture (2015) *available at* https://www.accenture.com/t20150523T023647Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Industrial-Internet-of-Things-Institute-Report-2015.pdfla=en.