Internet of Things Working Group

Year-End White Paper
December 30, 2016
Co-Chairmen Rep. Bob Latta (R-OH) and Rep. Peter Welch (D-VT)

Introduction:

The goals of our working group are to educate members on the Internet of Things (IoT), identify issues affecting deployment of these emerging technologies, explore the benefits and challenges of the IoT for consumers and interested stakeholders, examine the possible role of the federal government in advancing IoT technologies, and explore the potential for public private partnerships in this sector.

The working group held five Member-level roundtables from the launch of the working group in May 2016 to the end of the year. These off-the-record roundtables presented an opportunity for robust dialogue between Members and interested stakeholders exploring the many sectors that IoT impacts and questions that need to be addressed moving forward.

Roundtables:

Intro to IoT

The first meeting of the working group was an introduction to what IoT is, how it is currently being utilized, the benefits of the emerging technology and potential for continued growth, and some challenges and risks associated with the technology. The roundtable participants discussed the importance of understanding the global challenges impacting technology growth, including regulations and security concerns. There was also an emphasis from participants on how IoT has two major segments: consumer and industrial. Privacy and cybersecurity were central topics introduced during this meeting that were regularly discussed throughout the five working group meetings. There was also discussion and debate about the benefit of government mandates and some participants recommended any government action take a holistic approach but not a one-size-fits-all mandate.

Advanced Vehicles

Safety, security, and privacy were the focus of the advanced vehicles IoT working group roundtable. Connected cars have smart driving assistance and the ability to alert drivers to potential collisions by speaking to other cars in their immediate vicinity. Members recognized that this consumer fueled innovation has the potential to enhance travel experiences and reduce deaths on the road. The roundtable participants discussed how IoT can offer solutions for traffic management and emission reduction by utilizing autonomous vehicles, especially for ride-sharing purposes. The working group members emphasized the benefits consumers will realize with IoT technology, but security and privacy challenges continue to be a critical aspect of the deployment of the technology. The roundtable participants from the vehicle industry acknowledged the importance of and their commitment to securing vehicles and protecting consumer privacy.

Cybersecurity and Privacy

The recurring interest and discussion around securing devices in all IoT verticals led the working group to focus a roundtable on cybersecurity and privacy. In an age of connected devices, managing cyber and privacy risks is not a new topic of concern. However, recent examples of cyberattacks on IoT devices have exposed not just the potential impact on individual consumers, but the possible vulnerability on the broader Internet infrastructure. The roundtable participants had differing viewpoints on how best to create an environment that promotes IoT and protects consumers and networks. They also grappled with whether or not a solution should rely on industry established standards, agency recommendations, legislation, or a combination of all the above. Although the participants lacked consensus on the best way forward, all agreed that security and privacy issues are critical to address within this emerging technology. Some participants also emphasized that consumers need to do their part to protect data by securing devices through good cyber hygiene practices.

Energy

The roundtable participants discussed how the energy sector has been employing variations of technology advancements, such as IoT, for decades while managing the risks of protecting the nation’s access to power. The industry has had to comply with regulations focused on safety and security because of the importance of electric infrastructure around the country. The participants discussed the opportunity for the energy sector to help other industries balance information sharing and cooperation with the government due to their experience sharing information when discovering new threats. Members also discussed how technology has empowered consumers to have more control and influence over the type of energy they use, and the amount of energy they consume throughout the day. Given the rapid pace that technology is being deployed in homes and businesses that impact energy usage, the participants echoed the need for any regulatory action to be workable to handle the evolving technology and sophisticated threats.

Health

The participants discussed how the utilization of IoT in healthcare personalizes care and treatment for patients. The participants shared that in addition to improvement of care with IoT devices; IoT can also increase access and reduce healthcare costs. Members and participants acknowledged the many benefits of advanced technologies to patients and the healthcare industry, but many challenges were also presented. One challenge discussed was the need for interoperability within the healthcare system for data analytics and integrated systems to allow providers to improve patient treatment and offer more choice in where they seek care. In this meeting it also became evident that just like every other industry, participants in the healthcare sector view data protection, cybersecurity, and privacy as top concerns and priorities. It was recommended by some roundtable participants that the industry continue to work to limit vulnerabilities by developing software and devices with security in mind rather than solely based on functionality.

Initiatives Outside of Congress:

IoT devices and systems have increasingly become part of our everyday lives – enhancing consumer experiences and spurring innovation and economic productivity. In light of the growth of network-connected devices, we've seen federal agencies and the private sector come forward to offer recommendations and guidance on best ways to secure IoT.

The National Telecommunications and Information Administration (NTIA) has taken an active role in conducting a review of the benefits, challenges and potential roles for the government in fostering the advancement of IoT. NTIA has held multistakeholder process meetings on this topic recognizing the need for a secure approach to IoT devices and systems that are upgradable, patchable, and consumer friendly by establishing broad security definitions.

The National Institute of Standards and Technology (NIST) published guidance for securing interconnected devices as well. This guidance has been recognized as a strong set of security recommendations that represent a holistic approach to establishing trustworthy and secure systems by incorporating security by design principles.

Additionally, as network-connected devices and systems are increasingly integrated with and rely upon our nation's critical infrastructure, the Department of Homeland Security (DHS) issued guidance on securing the IoT ecosystem. The involvement of DHS stresses the need to secure IoT in order to prevent malicious cyber activities that threaten infrastructure and public safety.

The Federal Trade Commission (FTC) issued a report that recommended best practices for businesses to follow that would enhance and protect consumers' privacy and security. Similar to other agency guidance, the FTC suggests security should be built into device design, vendors and providers should be capable of maintaining reasonable security, and patches and upgrades should be available to reduce vulnerabilities. The report also recommends that companies notify consumers and give them choices about how their information will be used.

The private sector has also been active in developing standards and codes by which different IoT verticals seek to commit to best practices and instill consumer confidence in products. While efforts have been uncoordinated in the past, as the dialogue has increased there has been an increased willingness by companies and associations to share their best practices. Many of the working group roundtable participants expressed an interest in continuing these efforts in conjunction with the federal efforts that we have seen on guidance and best practices.

A goal that participants and Members shared is mitigating cyber risks through a multitude of channels, including but not limited to adopting best practices and basic security measures, software updates, encrypted communication, and mutual authentication and authorization. Depending on the vertical and nature of the device, vulnerabilities will differ; therefore, multifaceted approaches must be taken into consideration. We must encourage continued open dialogue between the federal government and private sector as technology develops.

Conclusion:

IoT technology is rapidly evolving and growing in ways that greatly impact the U.S. and global economy, as are the threats associated with this technology. The activity of the working group has allowed Members to increase their knowledge surrounding IoT and has provided opportunities to discuss the best role for Congress moving forward.

As we look to the next Congress, we know there is still much more to be learned about IoT with both the potential this technology fosters and the challenges it faces. We look forward to working to continue to explore opportunities for the Committee on Energy and Commerce to lead on the Internet of Things.