Public Comments of the Application Developers Alliance on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things
Docket No: 160331306-6306-01

May 23, 2016

Background and Introduction

The Application Developers Alliance ("Alliance") is a global industry organization that includes nearly 200 companies and more than 60,000 individual developers.

- Alliance corporate membership includes small and large app publishers, infrastructure and service providers, and software industry stakeholders.
- The individual developers in the Alliance network are the workforce of the future — creators and builders whose forward-thinking products and services are improving our world.
- All Alliance members are invested in a digital future that requires powerful, efficient, open, and secure networks. These networks are the backbone of every software application.

The Alliance was formed to promote and support the interests of developers as creators, entrepreneurs, and innovators. Developers build the apps and software that enable products and systems that in turn support consumers, power businesses, and connect industries. All of our members' activities are interconnected, and it is equally in all our members' interests to ensure network stability, speed, trust and security. In this regard, the Alliance is pleased to comment on the Internet of Things and the growth and opportunity it will create.

The connected machines, devices, and applications that make up the Internet of Things are creating a new paradigm — making our lives healthier and more prosperous. Increased

connectivity is helping to link users with their "things," and their "things" to each other. The arena is ripe for growth, and it is estimated that by 2020, the IoT market will approach $2 trillion and include nearly 50 billion connected objects.[1] Innovators are already creating wearable devices that can detect breast cancer, toilets that can measure glucose levels, and biochips that measure water contaminants. These developments and IoT's predicted growth are immensely promising for both the economy and users' lifestyles. However, the market will not realize its full potential if policymakers prematurely enact burdensome laws and regulations that will unnecessarily impede the deployment and adoption of IoT.

Principles for Effective IoT Policymaking

Effective policymaking in the IoT arena begins with understanding and trusting the user-innovator relationship. Users cherish their privacy *and* the innovative products and services that are making their lives healthier, more convenient, and more prosperous. Innovators work hard to practice data's golden rule: they are collecting and using their customers' data in the same manner they would want their own data collected and used. The government should practice regulatory restraint and understand that this user-innovator relationship is spurring never-before-seen growth. More importantly, policymakers must know that data can be, and indeed already is, a force for good. Any IoT policymaking must be thoughtful and include input from an array of private- and public-sector stakeholders.

Do Not Fear Data or its Innovative Uses

Developers depend on data to innovate, grow, and improve our lives. For virtually every business in today's digital economy, data is the foundation upon which they operate. The IoT ecosystem is rapidly evolving, and industry is transparent with users on what data they collect, how it will be used, and who has access to it. Industry leaders have long valued consumer transparency and trust because their growth depends on it. Access to and use of data are critical to industry growth in this evolving ecosystem. For example, Strap, a human data analytics and wearable technology company, relies on complex data to drive their business. One doctor who works with Strap affirmed the value of the company's services, stating, "I don't

---

[1] Lindsay, Greg; Beau Woods; Joshua Corman. *Smart Homes and the Internet of Things.* Atlantic Council: Brent Scowcroft Center on International Security. March 2016. Washington, DC

want my patients' raw step count. I want to know how their recent activity trends impact their specific condition, and ultimately have my treatment decisions informed by those insights."[2] To fully capitalize on IoT's potential and to best serve consumers, Strap needs the flexibility to collect a variety of data. Policies that place unreasonable limits on data collection or storage hamstring developers' ability to innovate, ultimately harming consumers, entrepreneurs, and businesses alike.

Do Not Harm Innovation or Growth

The IoT ecosystem is complex, and regulations should not impose unnecessary burdens on developers, impede innovation or growth, or create tech mandates. Regulations should be consistent wherever possible and applied neutrally so that businesses operate on a level playing field. Companies already comply with state, federal, and sectoral laws and regulations, and any new rules must be reflective and address concrete harms, not supposed threats. Inter-agency cooperation is also important to ensure regulations do not duplicate or add additional obstacles that companies must navigate. Top-down government regulation, particularly in the areas of data privacy and security, will dramatically slow the pace of entrepreneurial innovation.

Indeed, the creators of IoT products recognize the market's growth potential. In a recent survey of 340 software developers, nearly 60 percent of respondents expressed interest in wearable devices or smart homes; 45 percent in connected cars; and 38 percent in connected retail.[3] What is more, in a separate survey, just half of all developers say they have the skillsets needed to meet today's IoT demands, indicating industry's difficulty to keep pace with growing consumer interest.[4]

Do Trust Developers to Protect Their Consumers

Developers understand the risks of cyber-attacks, which can shake consumer confidence in IoT and stifle innovation in the space. To mitigate these risks, developers are implementing

---

[2] Caldwell, Steve. *Why mHealth Data is Not Enough*. Strap Blog. 4 May 2016. Cincinnati, OH.
[3] *Developer Snapshot: Interested Areas*. Application Developers Alliance. November 2015 – March 2016. Washington, DC.
[4] *State of IoT: 2015 Global Developer Study.* Progress and Harbor Research. January – Feburary 2015. Bedford, MA.

procedures to preempt attacks and keep their users safe. Policymakers should leverage the innovation taking place in the global private security market instead of forcing companies to comply with an often outdated patchwork of state and national regulations. For instance, FileOpen Systems, a software company that provides tools to control distribution of valuable documents, relies upon industry-standard technologies and protocols to enable the global interchange of encrypted documents. According to CEO Sanford Bingham, "The introduction of country-specific encryption mandates would make it difficult, if not impossible, for FileOpen to produce a product capable of working internationally, thus undermining one key purpose of the software, which is to enable secure information interchange between national governments."

Developers are good data custodians, collecting and using data to create new and exciting products and improve existing ones with their users' best interests in mind. Furthermore, developers are employing robust security measures to protect this data. As an industry best practice, innovators are implementing privacy-by-design in an effort to protect their products and users throughout all aspects of a system's engineering. Many developers are encrypting data while in use, in transit, and at rest. Regulators must ensure developers have the necessary flexibility to create cutting-edge improvements to defend their products and services and protect their users.

Do Update our Nation's Infrastructure and Bridge the Digital Divide

Too many communities lack adequate internet access, affecting everything from a student's ability to complete online homework assignments to a person's ability to conduct basic financial transactions. Policymakers are already working to increase availability and access to affordable high-speed broadband with an eye to underserved communities. Additionally, policymakers must effectively manage spectrum capabilities to ensure this valuable resource is available for the new devices coming online every day. By 2020 there could be as many as 50 billion connected devices, but in order for this market to fully mature, appropriate investments are required to update the nation's infrastructure.[5] Massive additional infrastructure investments will be necessary to support the proliferation of new connections. The Alliance encourages

---

[5] Lindsay, Greg; Beau Woods; Joshua Corman. _Smart Homes and the Internet of Things._ Atlantic Council: Brent Scowcroft Center on International Security. March 2016. Washington, DC

policymakers to adopt a light-touch approach to IoT in order to encourage the necessary commitments from the private sector.

Do Create Public-Private Partnerships and Multi-Stakeholder Efforts

Public-Private Partnerships (PPPs) allow the government to leverage private sector talent for the public's benefit and achieve what the public or private sector alone may not be able to accomplish. By partnering with private entities, the government is able to fast-track research and development, test the viability of specific projects, and implement or scale them in an efficient way. Smart cities, for instance, are only achievable via PPPs. One example of an IoT PPP implementation is in San José, where the city has partnered with Intel to use a smart city design to achieve San José's "Green Vision" initiative.[6] In addition, multi-stakeholder efforts that convene policymakers, academics, industry professionals, and other stakeholders to review the effectiveness of existing laws and regulations, outline future strategies, and identify burgeoning issues and regulatory concerns have proven to be very effective.

Do Create a National Plan

As a disruptor in virtually every sector of our economy, IoT deserves a national strategy that policymakers can execute against. Like any national priority, IoT planning must include an array of governmental agencies, industry stakeholders, academics, and others to identify avenues for widespread IoT deployment and adoption. Ultimately, any national strategy should address workforce shortages, improving access to broadband, access to capital, interoperability, data collection and security, consumer privacy, protecting innovators and their works from abusive patent litigation and regulatory jurisdictions, among other things.

Conclusion

While still in its infancy, the Internet of Things ecosystem is already providing untold benefits to all people and facets of our economy. Connected devices and the data that power them are making the world healthier and more prosperous. As the government considers what, if any, role

---

[6] *San José Implements Intel Technology for a Smarter City*. Intel Newsroom. 11 June 2014. Washington, DC.

it will play, it is critical to continue enabling "permission-less" innovation, and carefully consider the effects new laws and regulations in the space will have on users, companies, and the economy. We encourage the government to premise policies on trusting savvy consumers and innovators who will determine the size and scope of the IoT marketplace.

The Alliance is available to the NTIA and all other federal agencies to discuss this submission, or any other matter of interest to our industry. Thank you for the opportunity make this submission.

Respectfully submitted,

Jake Ward
President & CEO
Application Developers Alliance
1015 7th Street NW, 2nd Floor
Washington, D.C. 20001