THE **PROVIDENCE** GROUP

June 2, 2016

Mr. Travis Hall
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Attn: IOT RFC 2016
Washington, D.C. 20230

Via email

Dear Mr. Hall,

We applaud the Department of Commerce for the opportunity to comment on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things. We believe the United States needs a national strategy for the Internet of Things (IoT) since the IoT represents transformative 21st century technologies that promises to revolutionize homes, cars, health care and industry in general. Whether we call it Smart Cities, the Internet of Everything, or the Industrial Internet-- the IoT is about innovation and represents the future of the internet ecosystem itself. Despite the existence of radio frequency identification sensors for decades, we are still at the beginning of the promise and understanding of the IoT. We believe our collective mission must be to protect privacy and security and enable innovation in the IoT ecosystem.

We believe the U.S. needs a coordinated federal IoT strategy to continue to lead the world in IoT technology development and applications to drive global competitiveness and economic growth. Such a strategy needs to be proactive from the most senior levels of the executive branch of government as industry, government and civil society seek to work together to design a strategy allows the United States to continue to lead the world in IoT innovation and economic growth.

The IoT is a broad term that describes the ecosystem of sensors that interact with each other, persons, and services in computer-aware environments supported by analytics. The complexity of this ecosystem includes sensors that will only interact with each other, sensors that will interact with the broad ecosystem through local area networks (LANs) as well as sensors that may be in direct contact with the Internet. Consideration must be given to the

breadth and potential implications of all policy actions on this emerging, yet complex, ecosystem.

The potential benefits of the IoT are only now emerging, as sensors can interact with other objects or people in computer-aware environments to make use of cloud-based services supported by Big Data and powerful analytics. While consumers are already using internet enabled devices to reap the benefits of social media and e-commerce, industry is beginning to explore ways in which connected devices can improve the safety and reliability of complex industrial processes; achieve greater energy and operational efficiencies; create faster more cost effective means of communications; and improve the safety of medical devices and services. If the vast societal and economic benefits of the IoT are to be realized, the Department of Commerce must embrace a broad vision for the IoT and confront the opportunities and challenges with evidence-based work toward practical solutions that protect the individual, encourage responsible use of data, and foster robust innovation.

Some IoT devices will employ user interfaces which will clearly indicate to individuals how data is being collected and may offer controls directly or through LANs as appropriate; other technologies will collect and transfer data with little to no recognizable interface and with little or no communication to the individual about the nature of the data collection. Further, while some IoT devices will interact directly with the consumer and be designed principally for the consumer, others (such as connected airplane engines, wind turbines and locomotives) will operate principally in the industrial space and therefore involve a separate set of considerations on issues such as the practicality and utility of one-to-one consent.

IoT applications will challenge traditional notions of how to apply privacy frameworks like the Fair Information Practice Principles (FIPPS) that have been in place since the 1970's. Those established frameworks have served us well but much has changed since the era of centralized databases, highly structured data and relatively straightforward consumer transactions involving one buyer and one seller. Unlike the client server infrastructures of fifteen years ago, today's internet ecosystem contains an abundance of unstructured data, is highly transactional and thrives on a one-to-many model with many players including cloud services providers, intermediates routing traffic and establishing connectivity and entities providing enhanced security. Similarly, other industries using IoT devices, like the health care industry, now involve a complex network of providers, payer entities, product providers and service agendas, and researchers.

The advent of the IoT compels policy makers, industry and civil society to confront traditional notions of notice and choice, security and consent. While we should not abandon the FIPPS, we do need to adapt, interpret and update

them in a way that serves the IoT environment. We need to move away from an approach centered on the collection of data to focus in practical terms on what happens to that data and how it's used, bearing in mind potential real world harms and consequences.

We now enter a new era where many of the devices make it difficult or impossible for an individual to read something that looks like a privacy policy. Data aggregation from sensors and machine-to- machine communications -- the IoT-- and the increased value from data analytics mean individuals will not always know who holds data relating to them. At the same time, many IoT applications will be designed to give users more customization, and provide for better authentication and greater control over their data.

Data must be used in ways that are transparent whether or not an individual has had the opportunity to consent. We need to confront when it is reasonable to expect an individual to consent to their data being processed. Unfortunately, consent often places an unreasonable burden on individuals to understand how their data will be used in complex environments, while at the same time consent may be impossible to obtain in many contexts. A focus on accountability and transparency shifts the burden from the individual back to the organization that holds the data, as it encourages responsible behavior even for situations where consent cannot be obtained. This shift, in turn, will promote innovation and the development of new business models, while, encouraging responsible behavior even for situations where consent cannot be obtained.

The complex data environment will put an even higher priority on security. As technology stores more data relating to individuals, the threat of potential exposure of the information will increase. These threats, and the possible increased risk to the individual, require increased focus on securing the IoT. We believe securing the IoT is best managed through an enterprise risk model of governance. The FTC and other federal agencies have identified potential security concerns related to nascent IoT technology. A one-size fits all tactical approach to the IoT is insufficient. We believe the best way to address cybersecurity and privacy in the IoT is through an enterprise wide strategic risk management approach. Securing the IoT must remain collaborative, flexible, and innovative over the long term. The voluntary NIST Cyber Security Framework serves as an excellent model to frame cyber security and privacy risks and to manage and mitigate those risks in the IoT ecosystem.

Having served as Deputy Assistant Secretary for Technology Policy and Chief Privacy Officer at the Department of Commerce shaping the transatlantic IoT debate since 2005, we strongly urge a higher level of global IoT policy engagement including global best practices for securing the IoT initiated five years ago and led by the IoT Dynamic Coalition at the Internet Governance

Forum (IGF). http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/

In addition, there needs to be a much greater focus on Transatlantic IoT collaboration between the United States and the European Union as US Ambassador to the EU, Anthony L. Gardner, highlighted in his speech to the Forum Europe 7th Annual Internet of Things European Summit, entitled, "The Internet of Things: A Transatlantic Bridge to the Future on May 17, 2016. http://useu.usmission.gov/sp-051816.html

Specifically, elevating the IoT as a formal agenda item at the annual US-EU Bilateral Information Society Dialogue would encourage broader dialogue with the EU and executive branch collaboration with the Departments of Health and Human Services, Transportation, Energy, State, and Defense, among others, along with federal independent agencies including the FTC and FCC. In addition, greater policy level involvement in transatlantic EU IoT projects like Picasso and Discovery would be welcome.

Policy experts, academics and regulators have, on the whole, not succeeded in predicting the emergence and success of future business models. To avoid well-intentioned but unintended consequences, the Department of Commerce must provide strong leadership to create a federal interagency IoT working to avoid unnecessary constraints on innovation or adoption of proscriptive polices to allow IoT markets to develop. Industry stands ready to work together with the Department of Commerce to achieve the full benefit of the IoT.

Sincerely,

Dan Caprio
Co-Founder and Chairman