Information Technology Industry Council

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet

Internet of Things Hearing Testimony of
Dean C. Garfield, President and CEO of the
Information Technology Industry Council

Good morning. Thank you Chairman Issa, Ranking Member Nadler, and Members of the Subcommittee for inviting me to testify this morning. The issue we are discussing today has the potential to positively transform our world more than perhaps any development since the invention of the Internet itself.

My name is Dean C. Garfield, and I am President and CEO of the Information Technology Industry Council (ITI). ITI represents 61[1] of the most innovative and forward-looking companies in the world. Our membership includes companies from all verticals of the technology sector, including semiconductor, network equipment, software, digital services, hardware, mobile device, and Internet companies. This gives ITI a broad perspective on the transformational economic, societal, and commercial opportunities the Internet of Things (IoT) is creating. Note, I say "is creating" because for all of our companies, this market is real. Companies are investing in IoT, and 80 percent of those that do are seeing increased revenue as a result of IoT initiatives, with the average increase in revenue being 15.6 percent.[2] Eighty seven percent of CEOs expect long-term job growth from IoT.[3] But development and innovation will only continue with appropriate support from policy makers, and I look forward to discussing these opportunities with you today.

Definition and Categories of IoT

The IoT is a collection of external devices and sensors that generate data, which, through an Internet connection, can be analyzed to provide actionable information. The range and application of these devices is virtually limitless, but we generally view them in three distinct categories: 1) commercial or industrial, 2) personal or mobile, and 3) household.

Commercial and industrial IoT devices are by far the largest category, and the area where many of our companies see the biggest opportunity to enhance productivity and efficiencies, improve real-time decision making, and solve critical societal problems. Estimates for this specific

[1] See membership list here: http://www.itic.org/membership/member-companies
[2] Tata Consultancy Services, *Internet of Things: The Complete Reimaginative Force*, rel. July 2015.
[3] Accenture, *CEO Briefing 2015, From Productivity to Outcomes: Using the Internet of Things to drive future business strategies*, rel. 2015.

category of IoT are predicted to eclipse $7 trillion by 2030.[4] This category includes predictive maintenance of equipment, facility heating, cooling and lighting management, transportation fleet management and improvement, and many other large scale uses where the aggregate of small changes on a large scale equates to significant cost, energy, and other efficiency and productivity improvements. Exhibit 1 demonstrates how IoT applications can be deployed in a specific industrial setting, namely mining and resource transportation. Roughly 70 percent of the potential value from IoT comes from commercial and industrial IoT applications.[5]

Personal or mobile IoT technologies - probably the most familiar as wearable watches, health monitors, and similar devices that connect to the Internet via wireless broadband or through a mobile phone - are becoming ubiquitous. But the real gross domestic product (GDP) impact from this category will be derived from autonomous vehicles and cars connected to the Internet via cellular or other wireless technologies. The defining characteristic of this group is the mobile nature of the IoT application and the reliance on a wireless broadband connection.

Lastly, household IoT applications range from smart appliances to smart thermostats, and intelligent home monitoring and security systems. These products will connect through a residential broadband connection or home Wi-Fi network to provide energy savings and home automation and security benefits.

IoT Technologies In Action

ITI was pleased to participate in the inaugural Congressional Internet of Things Caucus event last week on "Smart Cites: How IoT is Changing Communities." As that panel discussed, IoT will disrupt nearly every public and private sector function, including trash collection and street lighting, and in so doing will make our cities not only smarter but also more livable, more workable, more resilient, and more competitive. Public and private sector partnerships will be essential in leveraging IoT to make such advancements in our cities. Is there a role for the federal government in doing so? I think so, but as the Chairman stated at an event this spring that I moderated, "Congress' role is to learn to do only what's necessary and no more." We look forward to working with the Chairman and this Committee in an effort to narrowly target only that which is necessary. This will involve focusing on acceleration of efforts and projects that will help the key stakeholders achieve their collaborative maximum. Cities will be a key incubator for the collaborations that we seek, and ITI looks forward to working with this Subcommittee on ideas for how the federal government can be a partner in this regard.

Similarly, ITI and our member companies have been increasingly focused on smart transportation policy as major automotive companies and major technology companies are increasingly partnering to embed complex, computer-based technology in their new vehicles.

[4] Accenture, *Winning with the Industrial Internet of Things*; rel. 2015.
[5] McKinsey & Company, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*; rel. June 2015.

Again, this is an area where Congress and the federal government can play an important role where appropriate, but must be careful not to thwart U.S. innovation and competitiveness. For example, connectivity and communications between vehicles must be secure and reliable, especially for safety applications; this is something that Congress, the Department of Transportation, the Federal Trade Commission (FTC), and other government stakeholders should oversee to protect consumers. Additionally, to advance U.S. global competitiveness, policymakers also must promote investment and development of a wide range of innovative automotive and transportation technologies to improve the safety, mobility, and efficiency of America's roads and highways.

ITI's companies are innovating in this exciting, new area. Advanced driver assistance systems include sensors to provide features such as brake assist and adaptive cruise control. A broad range of wireless communication technologies will allow vehicles to communicate with one another and with infrastructure, which will enable a world of new safety, traffic flow, and other applications. Autonomous driving technology has received significant attention with many companies conducting extensive testing of these technologies around the world – and today's consumers already expect partially-autonomous technologies like parking assist and adaptive cruise control when they buy a new car. These are all very promising technologies that will provide tremendous safety, efficiency, mobility, and economic benefits. It is critical that while the government oversees things like security standards for communications between vehicles, it must also foster innovation. To this end, policymakers should encourage the development of all of these advanced automotive technologies by letting the marketplace evolve, and not promoting one specific technology over others. The safety of our citizens on U.S. roads and highways is paramount, and the U.S. must lead globally with the most innovative, effective, and secure technologies.

The home is another platform familiar to the public where IoT technology will drive significant benefits and cost savings for consumers. Home energy management – smart thermostats and appliances – chore automation, and home security and monitoring systems have the potential to create an economic impact of more than $200 billion per year by 2025.[6]

Enabling IoT Development – a Public-Private Effort

Let me clarify at this point, while I provided statistics from multiple studies predicting immense economic benefits through further development of the IoT, none of this is guaranteed. The estimated economic benefits often cited are dependent on a fertile innovative environment comprised of favorable policies and minimal regulatory barriers. Congress, the Administration, and governments around the globe will play an important role in realizing or, alternatively, falling short of those potential estimates for economic and societal growth.

[6] McKinsey & Company, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*; rel. June 2015.

To motivate IoT adoption, applications and devices must evoke user trust through hardened security and privacy solutions. ITI's member companies are at the forefront of providing security solutions from the devices at the network edge to the cloud. With billions of additional devices coming online, ITI's companies are embedding security in IoT platforms at the outset of the manufacturing and design process for each new device that extends and expands the network. Security must be built into both hardware and software at the outset to ensure there are redundancies, to prevent intrusions, and to create secure and trusted IoT systems. Different systems, products and applications bring very different security needs, and the technology sector addresses those needs on a case-by-case approach. There is not a one-size-fits-all approach to addressing security, particularly in the IoT space given the broad range of applications, and industry stands ready to work with policymakers to develop a policy framework that enhances privacy in the IoT. ITI previously released cybersecurity principles, which are applicable to the IoT in their approach to addressing security.[7]

With the same design and manufacturing phase emphasis, companies build their IoT products to appropriately respect and protect user privacy. This privacy-by-design approach is critical to incentivize consumer adoption of these technologies, thereby enabling the aggregation, filtering, and sharing of data across network and devices. As more data is shared securely, companies and users will certainly find new ways to use that data – especially in the aggregate. In some applications, de-identified aggregate data is what is needed to serve the necessary purpose, thus minimizing privacy implications. [8] New constraints on the collection and use of data may hinder innovation in this area and dampen the promising uses of this aggregated data in areas such as medical research. Resisting new restrictions, however, does not mean the IoT will become the wild west of privacy. IoT technologies collect and utilize a wide variety of data, much of which is already subject to existing laws or rules governing collection, use, and sharing.[9] If the maximum benefit is to be derived from the IoT, policymakers should avoid adding unnecessary layers of regulation or requirements by considering the types of data that will be collected, and instead ensure compliance with existing rules and regulations.[10]

---

[7] See ITI's *Cybersecurity Principles for Industry and Government*: http://www.itic.org/public-policy/CybersecurityPrinciplesforIndustryandGovernment.pdf

[8] This would be the case for an application that reports potholes to a city, either from a user manually entering that data, or from technology in a mobile device or car autonomously reporting that information.

[9] For example, there are existing laws that impose privacy requirements on certain health and financial information, and the FTC has the authority to take action against unfair or deceptive acts or practices in connection with the IoT.

[10] For instance, a sensor on a motor that measures vibrations or heat output to recognize preventative maintenance is significantly different from heart rate, body mass index, or blood pressure data collected by a smart watch.

For the various IoT categories listed above, different types and amounts of data will need to be collected, and used in many different ways. It is incumbent upon ITI's member companies, and all companies offering IoT applications, to be transparent about their practices. We must also ensure that data is appropriately protected. Businesses and consumers will be reluctant to adopt IoT applications if they have privacy concerns, or concerns that their data is not secure. If businesses realize the benefits that can be captured through continuous measurements of their energy use, or consumers understand braking data from their vehicle is being aggregated so autonomous vehicles can more accurately navigate roadways, and this data is being stored securely and used appropriately, there will be greater comfort in embracing these technologies. Should industry fail to do this, policymakers should act in a tailored fashion to address the specific problem, recognizing overreach could impact the broader development and potential of the IoT.[11]

The private sector is investing, and must continue to invest heavily in the communications networks and infrastructure that this data will traverse. The explosion of connected devices will expedite the growth trend for mobile data, which already is growing 55 percent year-on-year.[12] Continuous investment in our networks will be necessary to handle this growth. Robust broadband networks are a fundamental building block to the IoT, and only with ubiquitous, high-speed, affordable broadband will the public and private sectors be able to derive the maximum potential the IoT will offer. Congress, and the relevant federal agencies, must continue to make spectrum available for mobile broadband and enable efficient spectrum management. Effective spectrum management will encompass licensed, unlicensed, and licensed shared access regimes that promote spectral efficiency, and enable the diversity of spectrum uses across the broad range of IoT products and services. The federal government must also advance policies that foster private sector investment in wired and wireless networks, and promote build-out to all un- and under-served areas.

To enable broad adoption of IoT technologies and avoid IoT silos, attention must be placed on the ease of connectivity and interoperability of IoT devices, platforms, and infrastructure, as well as streamlined cross-border data flow. Systems of intelligent devices must be connected to each other or the network, often across geographic boundaries, to maximize the potential of the IoT. The private sector is leading the development of open standards that will enable interoperability across the IoT, and partnering with the public sector to encourage the sharing of best practices. Global standards will accelerate adoption, drive competition, and enable the

[11] The FTC's settlement with TRENDnet, Inc., the company that markets video cameras designed to allow consumers to monitor their homes remotely, is an appropriately narrow response to a specific problem. See *In the Matter of TRENDnet, Inc.* FTC File No. 122 3090 (September 11, 2013) (proposed consent order), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security- video-cameras-settles

[12] Ericsson, *Mobility Report, On the Pulse of the Networked Society*, rel. June 2015.

cost-effective introduction of new technologies. Open standards will also promote industry innovation and establish a better defined technology evolution path.

Lastly, but perhaps most importantly, a strategic national IoT plan and funding should be put in place, which encourages public-private partnerships (PPPs), accelerates IoT adoption, and enables vast economic and societal benefits from the IoT in both the near- and long-term. Successful PPPs will make IoT deployments an attractive investment for government and industry, and promote innovation, scalability, and sustainability. By leveraging PPPs, we can expedite IoT research and development and U.S. global IoT leadership. The development of a national IoT plan, and finding areas where the federal government can lead by example in the adoption of IoT, will both foster innovation and enable a multitude of cost savings, efficiencies, and other benefits to the public sector.

Policy Recommendations to Immediately Promote an Innovate IoT Environment

1. **IoT Strategy and Advisory Council** – Creating an advisory board with government and industry partners to produce a National IoT Strategy with ambitious timelines, and more tailored strategies for federal government adoption, smart city promotion, promotion of next generation transportation technologies, and similar efforts to maintain U.S. leadership in the IoT.[13]
2. **Security and Interoperability** – The federal government can encourage industry alignment of private sector developed state of the art security and interoperability solutions, and partner with the private sector to encourage the sharing of best practices.
3. **Public-Private Partnerships** – The federal government should incentivize the use of public-private partnerships as a means to accelerate IoT development and adoption, and U.S. global leadership.
4. **Infrastructure** – The federal government should make additional spectrum available for mobile broadband, implement effective spectrum management programs, and incentivize investment in network infrastructure.

[13] On March 24, 2015, the U.S. Senate unanimously passed S.Res. 110, A resolution expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment, that provided guidance for a national IoT strategy.

Conclusion

The Internet has transformed the world in ways we could never have dreamed possible, and the IoT is expected to have an even greater transformative impact in our lives, our economy, and our society. Similar to the Internet in the early 1990s, the IoT is in its very nascent stages and presents us with limitless possibilities if we have the vision and environment to achieve them. We look forward to working with Congress to advance these policy recommendations, and maintaining an open dialogue as IoT products, services, and applications evolve. We also ask that lawmakers evaluate existing policy tools and use caution before taking actions that may inadvertently or unnecessarily impede IoT innovation and disadvantage U.S. competitiveness.

I thank the Chairman, Ranking Member, and Members of the Subcommittee for inviting me here to testify and for their interest and examination of this important issue. I look forward to taking your questions.

Exhibit 1: McKinsey & Company, McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, p. 10; rel. June 2015.