LOQUITURGROUP

Submission to the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce Docket No. 160331306-6306-01

Comments on behalf of the IoT Policy Network in response to NTIA's request for public comment on
The Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things
June 2, 2016

Introduction

Bruce Gustafson and Christopher Guttman-McCabe are joint founders of the IoT Policy Network (iotpolicynetwork.com). The Loquitur Group is filing this response on the Network's behalf.

The IoT Policy Network welcomes the opportunity to comment in this proceeding, and appreciates NTIA's outreach to industry and the multi-stakeholder community. The IoT Policy Network is a Washington-based advisory group supporting policies which encourage innovation and the sustainable growth of the Internet of Things, to the benefit of society and all ecosystem participants. The Network's primary mission is to build industry consensus on critical IoT policy issues and to speak with one voice on behalf of the many IoT industry stakeholders. We will focus on policy issues over technology issues in the response that follows.

Background

Industry is in broad alignment with the four pillars of the Department of Commerce 2015-2016 Digital Economy Agenda: promoting a free and open internet worldwide; promoting trust and confidence online; ensuring internet

access for workers, families and companies; and promoting innovation in the digital economy. While initially focused on the conventional internet, the extension to IoT is easily made and entirely appropriate, for the distinction between the two is fading and will become irrelevant in the near future. Thus, while this proceeding is focused on IoT, it should build upon work already underway for internet policy writ large. The reality is that anything connected to the internet is also part of IoT already, either passively or actively. It simply takes time for language and policy to catch up with the real world.

The overarching theme of NTIA's twenty-eight questions is, "What role should the government play in the evolution of IoT?" Policy oversight is clearly appropriate in an area as significant to the digital economy, and society generally, so the question is really one of balancing promotion, control, and organic evolution. The policy themes we will advance are: 1) moderate course corrections, and only when evidence indicates the need; 2) a government focus on removing roadblocks and providing clarity and simplicity where guidance is required; 3) passive government participation in all aspects of IoT's evolution, and active participation where the government holds key resources as steward for the public at large; 4) a primary role in analyzing and addressing the social and economic changes that a fully digital society will face.

The IoT policy question can be broken down into two components: what policy actions are recommended in the face of a disruptive new technology generally, and what policy actions are recommended specifically due to something inherent in IoT specifically? There is no debate that, like the emergence of the internet or the railroads, IoT is another innovation that will disrupt legacy business models. Policy makers must resist the temptation to build barriers by attempting to preserve legacy systems, especially those which have a history of regulatory protection. IoT will drive revolutionary changes in agriculture, transportation, energy distribution, government, and a myriad of other sectors reliant on complex real-world data inputs. Existing regulators will be challenged to adapt, and our recommendation is that each sector should focus on a critical reassessment and dismantling of historical

policy barriers in the face of new innovations like IoT. This is simply the process of change and rebirth that every disruptive innovation brings.

In the IoT domain specifically, however, the introduction of networked devices and large datasets into complex systems will amplify the importance of robust interconnection, access security, and data stewardship. Interconnection has been an industry priority since the emergence of the internet, and policymakers are already well informed and active in support of improving America's digital infrastructure: IoT is simply an extension of this established imperative. For commercial and industrial systems, security failures will have immediate and direct economic consequences - with subsequent market feedback. Like the broader internet industry, the IoT ecosystem already has strong incentives in place to make security the top priority. Finally, while data stewardship is the IoT policy area that is likely to generate the most political energy, the elevation of privacy as a topic for national and international debate is driving promising innovations in blockchain and encryption technology which will only accelerate as IoT systems come online.

General Questions

Question 1

NTIA asks whether we can learn from past technological changes as we look ahead to IoT, or whether IoT is in some way different. In large measure, the policy challenges we are already focused on with the growth of the internet and the digital economy will remain in play as IoT emerges. What will challenge policy makers is the scale of the issues and the speed at which they evolve. Policy discussions around personal and national digital security, privacy, data ownership, conflict of laws, and encryption will evolve naturally to include IoT. What will change is the breadth and scope of policy impacts in these areas.

Where novel policy areas will emerge is where IoT goes beyond hardware and data and begins to touch social and economic processes. For example,

we can anticipate significant shifts within many traditionally "non-networked" industries, where rich real-time datasets can now replace heuristics, approximations, and modeling. Agriculture is transforming the role of the farmer to one of owning land and capital, and setting crop strategy: allocation of resources like fertilizer and moisture, and the optimized control of machinery through IoT are being combined with services like engineered seed to radically change the skills, scale and risks of agribusiness. Elsewhere, government's role in providing public infrastructure like roads, bridges and traffic lights, may evolve to providing real-time transportation management services through publicly deployed sensors and open datasets. One could envision an FAA for surface transportation, tracking and routing countless vehicles through a safe and efficient IoT system designed to optimize the use of public infrastructure for public benefit. Healthcare is another example, where IoT can enable wide-scale health management systems based on real-time data and biometric sensors, lowering costs and improving patient outcomes and public health. These are not areas that have been well thought through during past technological evolutions.

In general however, the tools already exist to tackle these emerging policy questions, both in government and in the private sector. NTIA's adoption of the multi-stakeholder model for these complex digital economy issues should be extended to IoT-specific challenges as they emerge, with the recognition that in many instances IoT assets are privately held, while the rewards of good stewardship can be widely felt.

Question 2

Is there a sufficient definition of IoT, and do the differences between definitions matter? More to the point, where does IoT begin and not-IoT end? In large measure the precise definition is less relevant for policy makers - who will inevitably be looking at a specific subset of all that IoT is - than for economists who are looking to draw the system boundaries for academic analysis. All definitions envision connected devices, some no more than passive sensors, capable of collecting local data and making it available over networks. Most definitions also envision systems capable of interpreting that

data, usually in the context of other data, and taking action which can then be felt in the real world. Some require that both the incoming data and subsequent actions be through "things" and not people. Rather than looking for an all-inclusive definition, we would recommend policy-makers focus on breaking down IoT into smaller pieces where definitions can be a little crisper and more useful.

Question 3

NTIA is seeking examples of planned or existing rules and policies that a) appropriately foster IoT while protecting society, or b) inhibit IoT unnecessarily. This is a heavy lift, and in a sense foreshadows many of the recommendations commenters will ultimately provide. Rather than cite specific legislation, we can generally describe categories of rules and policies and place them on a continuum from "does no harm and much good" to "does no good and much harm". With luck the bucket "does no harm and no good" is monitored and continuously emptied.

In general, IoT is a product of the private sector, in contrast to the seed that became the internet, which originated through government-sponsored research. That is not to say that sponsored IoT research isn't being done, or shouldn't be, but it is no longer a necessary condition to get IoT off the ground. This immediately highlights a difference in government's role: from active developer to user, promoter, and public safety officer. We would encourage policy-makers to recognize that IoT is not a public asset, but largely a private one, and that government's role is simply as one more user and one more data and service provider (albeit a large and influential one).

Policies which focus on protecting bystanders, rather than policing the playing field, should be the early focus as IoT experiments play out. This is a departure from the inward-focused "regulator as referee" paradigm which dominates existing segments of the economy. Policy makers must carefully assess what the past tells us: history's lesson is not "impose what worked last time", but "watch for known warning signals and apply small corrections earlier". Thus, the work underway across the policy landscape to create a

framework for privacy norms is an example of an area where much good can be done. Recognizing that society as a whole benefits when data is shared is a foundational element of IoT. Privacy is a trade-off between the individual and the public good, and crafting policy in this area is a necessary condition for IoT's long-term success. In a similar vein, data-stewardship (as opposed to ownership) is an area where policy-makers can play a role by building a framework around which industry participants can align, though efforts in this area are lagging.

Policies that wade deep into technical implementations and architectures are far less useful and likely to slow innovation and derail beneficial impacts. Thus, while security will be another fundamental component for IoT success, policy makers are simply one more participant in the multi-stakeholder approach to securing the network. The best role for government is in its role as technology buyer - specifying rather than legislating the minimum standards for system security. Thus, rapid IoT adoption by the government is a powerful lever to encourage rapid innovation in IoT security.

Finally, by treating IoT as a monolithic technology that passes beneath the shadow of nearly every existing regulatory body, we are setting the stage for overlap and fragmentation in those cases where regulation could be truly beneficial. It is only natural for an entity to seek growth, so we must be on our guard against mission creep. No federal agency anticipated IoT when its charter was drawn, and so we are relying on policy-makers to figure out where things should fit. The lesson from the digital economy is that the value of data is in what it represents, not in where it is housed, how it is handled, or who owns it. Likewise, smart devices are by definition multi-purpose and subject to change, meaning that they may cross regulatory boundaries even after they've been deployed in the field. Frameworks that transcend regulatory silos are more aligned with how IoT is likely to evolve, just as a multi-stakeholder policy development process is in keeping with the constituency involved in IoT's creation.

Question 4

Breaking down the definition of IoT into smaller parts could be highly beneficial for policy makers. As NTIA suggests, some of these characterizations could be overlapping, but as long as they enable simpler policy making they should be explored.

Industrial/private IoT versus Consumer/public IoT is a very useful distinction in discussions about privacy and data stewardship, and in government's role as part of the ecosystem. These definitions allow us to focus on issues internal and external to the two domains, and on the connection points where they interact.

Infrastructure versus data-structure would also be a useful distinction. By separating IoT into its physical and logical components, policy discussions can deal with narrower sets of issues. Infrastructure policy might focus on standardization, interface compatibility, interoperability, device authentication, device stewardship, energy standards, etc. and be very industry-centric. The IoT data-structure would be the focus for policies around privacy, data security, jurisdiction and legal processes, encryption, data stewardship, and other information-centric issues, where public policy makers might have a larger role.

Question 5

While we offer no specific citations to policy research, we would highlight that discussion of data stewardship/ownership might prove to be a critical IoT policy weakness as systems proliferate. Likewise, data authentication, and online anonymity/trust models are areas where greater discussion is required.

Technology Questions

Questions 6 & 7

While there are many technological issues to be resolved for IoT to thrive, the private sector is ideally suited to working through these. Industry has a

track-record of creating complex technology ecosystems, and the fora exist for collective agreement on the various parameters in play. The reality is that industrial innovation is a darwinian process, and there is no value in trying to preselect winners or prevent failures from occurring. Government has a role as one of many participants, as previously discussed.

Where government's role is key, is where government controls resources critical to the IoT community, like spectrum or real estate. IoT will increase spectrum demands in every possible dimension, as many devices will connect wirelessly to the larger network. Likewise, there will be pressure to increase bandwidth and computing penetration towards the network edge. This may implicate public rights-of-way or public buildings as jumping-off points for IoT systems.

Infrastructure Questions

Questions 8, 9 & 10

There is little doubt that IoT will increase network traffic loads, but at the same time the industry is actively exploring new architectures, new wireless technologies, and is pushing high bandwidth systems closer and closer to the edge. And while there was a historical shift in how the industry thought about resiliency as we moved from switched to routed networks (an assumption that redundancy would solve any problems), architectures are now more sophisticated, taking advantage of public networks when possible, while using private networks when appropriate. But while many industrial and private IoT systems will be purpose-built to accommodate outages and failures, infrastructure resiliency will remain key in the supporting systems, like the energy grid, that will serve to enable many of the consumer IoT implementations.

Economy Questions

Questions 11 & 12

Whether or not to measure IoT as an economic sector depends on the timeframe and purpose of the program. At some point, IoT will morph from a sector to an enabler embedded across the entire digital economy, just as IT or the internet are today. Any measurement systems contemplated should take into account these challenges.

Questions 13 & 14

Like all technological change, the deployment of IoT will both create opportunities and change current patterns, sometimes in profound ways. Like the agriculture example used earlier, some industrial sectors will be re-engineered to take advantage of the wealth of real-time data and local control systems that make up IoT. In general, any system which embodies large numbers of discrete real-world data points capable of local measurement could be revolutionized by IoT, so fields as disparate as health care, traffic control, weather measurement, energy generation and transmission, agriculture, government, and so on are looking at IoT with great optimism. The social benefits of improving these systems include, among others, better health, greater energy efficiency, reduced waste, a reduced carbon footprint, lower prices, improved safety, and if managed well, a new industrial base from which to build American jobs and increase exports. These benefits will not come without economic disruption, however.

Research into longer-term impacts as systems go from limited to complete knowledge might benefit from government support. For example, as transportation systems gain in knowledge and complexity, the day may arise where traffic is evenly spread across all the surface streets in an urban environment, changing the character of once “busy” versus “quiet” neighborhoods. Changes to speed limits or road restrictions would not need simulation, but might become dynamic elements in the system, with suburban speed limits falling in the evening hours, and rising again to accommodate

traffic balancing during a busy morning commute. Streets leading to schools and playgrounds could be restricted such that "through traffic" was never routed into these areas. Government-sponsored research into those areas of infrastructure management under their control might be a wise course sooner rather than later, essentially posing the question, "how will the world be different when we have perfect information and perfect control of this system?"

Policy Questions

Question 15

Policy areas that will affect IoT are not new, and include areas such as consumer privacy, lawful access and intercept, cybersecurity / data stewardship, and any segment-specific policies which tend to prevent new business models from disrupting the status-quo (eg taxi or hotel regulations vs AirBnB and Uber). In turn, IoT is likely to affect policy areas which today are impacted by the size and complexity of the datasets involved, including areas like public health. In general, industry is approaching IoT as a set of incremental experiments - testing products and services in focused applications and then expanding to more general applications. Government would do well to accommodate this modern development process by mirroring it in the policy arena unless the challenges involved are universally applicable across the various IoT segments: thus privacy, cybersecurity / data stewardship and lawful access and intercept deserve continued and focused attention.

The privacy challenge is not unique to IoT, but emerges from the general digital economy debate; only the scale will change as IoT accelerates. On the one hand, large datasets provide tremendous insight into complex systems, especially when combined with other contextual information. These insights are driving a new wave of exploration and discovery in fields such as public health. The policy response has been to encourage the removal of personally identifiable information from data in the belief that this will protect individual privacy. The challenge is that when multiple "anonymous" datasets are

combined with even generic public information, it can be possible to re-attach individuals to the underlying information. As a simple example, knowing where you work and where you live would allow the re-identification of an anonymous GPS track from your mobile phone. Significant research is underway to create reliably anonymous datasets, but the effort involved highlights the immense challenge of truly de-identifying data (and keeping it that way). Government has a role in promoting research in this area, as well as in trust models which promote good stewardship of any private information collected.

Given the incredible benefits that arise from accurately measuring the world in real-time, policy discussions must shift from the absolutes of perfect privacy versus complete transparency, and explore how best to implement a model that allows users to independently balance the tradeoffs involved. We are beginning to see this emerge with IoT applications such as mapping applications where users can volunteer their GPS information in exchange for traffic advice. Myriad other applications abound, with both lesser and greater transparency and awareness of how the data is used and how the benefits are allocated. What we know is that consumers are willing to make tradeoffs if the advantages are clear.

Question 16

While cybersecurity is a critically important issue that is amplified as networks grow and IoT emerges, cybersecurity policy is somewhat independent of IoT generally. We would recommend looking at cybersecurity separately, and to segment cybersecurity policy issues so that we can independently examine: 1) bad actors accessing networks/data illegally, 2) data/network stewards failing to secure assets under their control, and 3) state actors operating under the umbrella of national security.

Question 17

Privacy, or data stewardship more generally, is becoming an active area for innovation, with the emergence of blockchain technologies coupled with

strong encryption and distributed computing providing the building blocks for trust models for everything from cryptocurrencies to apartment sharing. These capabilities can be complex and have spawned a dynamic and competitive race to develop and implement commercial systems which may re-energize segments of the economy which have seen little fundamental innovation for decades. IoT policy is independent of these innovations, but will no doubt exploit them as they emerge.

Consumer privacy is a unique area where IoT policy could be implicated, at least until true trust systems come online. Privacy regulators in other jurisdictions are already wrestling with this question, and no doubt considerable learning will take place in the near future as commercial IoT experiments take place and are evaluated, but in the meantime the focus is more on the potential for misuse over what might reasonably be expected. Our recommendation to US policymakers is two-fold. First, we'd encourage regulators to resist setting rules in advance based on a "parade of horribles'. It is easy to create the phantom of a dystopian world where privacy is lost and big brother, either elected or commercial, sets the rules. The very fact that this is universally rejected in the U.S. shines a bright light on any steps in this direction, with plenty of time to assess and react as experiments take place. Second, we'd encourage policy makers to consider consolidating privacy expertise rather than establishing a privacy branch inside every federal agency. Advances in this area will take place across many domains, and the questions will be common despite the regulatory silos.

Questions 18 & 19

Questions of consumer protection and economic equality are not unique to IoT, and we see no imperative for breaking out IoT as a focus in these areas. IoT is a technology capable of bringing great benefit to everybody, from reducing the costs of transportation or our food supply, to reducing the environmental impacts of our modern society. We'd encourage everyone to invest in harnessing IoT to aid the disadvantaged. In the area of consumer protection, IoT holds no special place, but is simply one of many innovative

technologies that existing systems will need to explore and accommodate as the digital economy evolves.

International Engagement Questions

Questions 20 through 24

The evolution of communications and networking from localized to globalized was well developed before IoT emerged as the next wave of innovation. We anticipate that many of the existing structures, and many new ones, will compete to play a role in the eventual interconnection of IoT networks into an interoperating whole. But while we can envision a harmonized global IoT network as one possible future, we should not assume that the internet model is the best or only possible outcome, and thus we must leave room for the market to experiment with alternative approaches while recognizing that existing networks will form much of the foundation of the future IoT.

NTIA asks after the various issues and factors that might emerge in the international development of IoT, and how best the U.S. should monitor and engage. This is a very big question. We would encourage the Department to consider IoT as simply one example of the many emerging innovations that could have global significance now that the internet is in place, and to conceptualize an engagement model that is not so much specific to IoT as it is a possible structure for any future digital innovation. This is by definition a much larger question, but using IoT as a case study in this regard, while keeping this question slightly decoupled from IoT specifically, would be a positive starting point.

Additional Questions

Question 25 & 26

We would encourage the U.S. government, as a potential major ecosystem participant in public IoT infrastructure, to remain engaged as the IoT community evolves. To the extent that the Department is already

participating in well developed multi-stakeholder engagement models, we'd simply suggest keeping IoT in mind as digital economy processes are developed. In terms of the Department's specific role within the federal government community we would simply encourage the current overarching information gathering and community engagement activities.

Questions 27 & 28

In general, the IoT ecosystem is developing well, with broad participation and robust experimentation well underway. To the extent that there are fundamental shared research questions, we would encourage federal government participation in identifying answers and supporting basic research. In terms of a comprehensive technology policy like those seen in Europe and other regions, there is a risk that in the current international climate this could actually disadvantage American competitors as they seek to globalize their IoT solutions. We would encourage great care and a light hand should the Department decide to intervene this actively in the market.

Conclusion

The very fact that the Department is asking questions and gathering information around IoT is tremendously encouraging. Ill-informed intervention is always bad intervention, and the many references to "engagement" and "multi-stakeholder" are strong signals that there is a true will to participate, rather than to dominate. We encourage the Department to continue down this path, and to focus on educating policy makers based on hard data and actual market activities. Above all, we encourage the department to help fight the fear of change that all significant innovations inspire.

The IoT industry recognizes that, alongside the tremendous opportunities this new technology will bring, there will also be disruption. Our national focus on education, investment, and entrepreneurship add tremendously to our global competitiveness, but we must remain diligent to ensure that opportunities are available for everyone to benefit and accrue to all corners of our society. The ongoing buildout of broadband infrastructure will be a

fundamental part of the nation's future prosperity, and government plays a key role in supporting and encouraging this critical area. IoT, for its part, will provide tremendous payback for that investment in the year's to come.

Our advice to policy maker's remains simple: moderate course corrections where evidence identifies a real-world need, coupled with a government focus on removing roadblocks and providing clarity and simplicity where agencies choose to intervene; and government participation as an equal partner, with a primary role of analyzing and addressing the social and economic changes that a fully digital society will face.

The IoT Policy Network would like to thank the Department and appreciates the opportunity to comment in this proceeding. If you would like to discuss anything referenced in this filing, please contact Bruce Gustafson at 202-735-7333 or bruce@loquiturgroup.com

The IoT Policy Network was founded in 2016 by Bruce Gustafson and Christopher Guttman-McCabe. Our website is iotpolicynetwork.com