US Commerce Department IoT Questions

About ARM

ARM welcomes this opportunity to offer some short points on the question posed by the Commerce Department. Our responses are in italics below.

ARM is a UK Headquartered company with extensive operations worldwide including in the US (where we are listed on NASDAQ). Our main business is the design of microprocessors. We have been particularly successful in mobile, and other areas where energy efficiency is important. IoT is one of big priorities.

We would be happy to amplify our points, or discuss other issues with you at your convenience.

The Questions and our Responses

1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?
   a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

      The technological challenges for IoT can in general terms be summarised as:

- *Energy efficiency. If IoT means lots of objects having sensors, including embedded in infrastructure and motor vehicles, they will need to have very long battery lives, or be able to harvest energy from their environment. New technology needs to deliver this.*
- *Compute power in constrained environments. IoT sensors will be small. Some of them will only be required to perform relatively simple tasks, others sophisticated edge processing. But even so if they are to provide adequate security, including a capability to receive upgrades, they will need adequate computing power. Latest generation 32-bit processors can deliver this.*

- *Security. Arguably, this is the biggest challenge. More is said about security below.*
- *Communications. IoT will need adequate Local Area and Wide Area communications capabilities. Again, more is said about this below.*

b. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?

- *Data security and Data protection. Data security is about making sure hackers cannot access your data in transit or in storage. Data protection is about ensuring that those who are authorized to receive your data only process it in ways you are content with.*
- *The data challenge is important because most observers believe that the real benefit of IoT (including the business benefit) derives from using the data the sensors collect. This value is increased in particular by aggregating and combining data, so that data can be used to offer individuals more personalised services and to provide more substantial insights into human behaviour for a variety of public policy and market research objectives.*
- *In an IoT world citizens (and businesses) will find more of their data captured by IoT devices. Even data that at present would not be classified as personal data could be used in ways which would reveal sensitive information about individuals or businesses.*
- *At present the public are inclined to be wary of how business (and public bodies) might use their data. For IoT to succeed, people need to have confidence in it. Unless IoT is seen as empowering people it will not deliver the full range of its potential benefits.*
- *There is at present no single answer to this. Some argue that the key is to provide greater transparency about data usage since at present very few people read lengthy Terms and Conditions. This would need to be an industry led effort. Other aspects of this include making clearer to people the benefits from letting their data be used in various ways.*

- *There may also be policy challenges around security (see below).*

c. What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

- *Broadly speaking IoT will enable us as a society to use resources more efficiently and to deliver services more effectively. It will do this by providing more data, more sophisticated analysis and the ability to respond to the data more quickly.*
- *Some key sectors likely to be transformed include:*

  (i) Health
  (ii) Smart cities
  (iii) Transport
  (iv) Energy
  (v) Manufacturing
  (vi) Agriculture

- *Realising the full benefits of this will require a mix of public and private sector activity*.
- *IoT will also offer the possibility of developing new business models. Businesses which have hitherto offered physical goods will be able to offer physical goods plus a range of services based on the data collected from those goods.*

2. The term ‘‘Internet of Things’’ and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures.8 What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

- *The simplest starting point for a definition of IoT is the idea that many objects will become intelligent and managed, i.e. able to gather information about that object, its performance or its environment, which will be processed and analysed locally or remotely, and as a result of which judgments can be made about different courses of action.*
- *There are some key points about this model:*

(i) It does not even mention the Internet. It is of course likely that information will be sent online. But this is not necessarily the case. In some cases machine to machine communication will suffice. Some recent predictions of the size and structure of the IoT market suggest a growing expectation that non-Cellular M2M will

constitute a bigger category than previously thought, and bigger than mobile phone connections.

(ii) It makes clear that so called 'big data' starts with collecting little data through the placement of IoT sensors.

(iii) It is critical that devices are actively managed, security setup correctly, software updates performed, and status monitored.

(iv) Open Internet standards, such as IPv6, will be critical for the growth and manageability of the IoT both for remote and machine to machine communications.

3. With respect to current or planned laws, regulations, and/or policies that apply to IoT: a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies? b. Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

    - Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to device vs. human interfacing.

- *It may be easier to think first in terms of the generic IoT challenges, which may be more or less important depending on the different IoT applications.*
- *For example, security will be a generic issue. But it may be that not all IoT applications need to have the same level of security protection. Clearly certain crucial areas - infrastructure, transport, health - will need high level protection.*
- *The Federal Government needs to have thought about IoT security even if in the end it decides that it is not an appropriate area for direct or detailed Government regulation.*
- *As seen by ARM, the following elements are crucial:*

(i) The need for an end to end multi-layered security architecture.

(ii) Start with the principle that connected devices need security partitioning built into the hardware of the device. Trustzone ™ - for example, creates a specially secure area to help isolate sensitive assets/operations, thus protecting the integrity of the device's systems. It is now possible to provide this level of security even in tiny, low cost sensors.

(iii) *But security should not become an excuse for promoting closed, proprietary systems. We need an open hardware root of trust which provides trust credentials for devices without locking in any particular service provider.*

(iv) *Communications security: IoT must be built around security by design i.e. security has to be factored into the design of IoT devices from the start. This means encouraging device developers to use software platforms (like ARM's mbed OS) which tackles security for them. In this way secure communications becomes part of the embedded IoT device.*

(v) *Upgrade security. We need to think about lifecycle security. We need secure firmware updates, secure provisioning, to be deliverable over the air.*

- *Another generic issue may be autonomy. Where machines are taking autonomous decisions new considerations may apply. For example, in Robotics we may need to think about an approach which is 'ethical by design' in the same way in which we are thinking of ' security by design' as the underlining principle of IoT design.*

4. Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant?

   Technology: Technology is at the heart of IoT and its applications. IoT development is being driven by a very diverse set of stakeholders whose expertise in science, research, development, deployment, measurements and standards are enabling rapid advances in technologies for IoT. It is important to understand what technological hurdles still exist, or may arise, in the development and deployment of IoT, and if the government can play a role in mitigating these hurdles.

5. What technological issues may hinder the development of IoT, if any? a. Examples of possible technical issues could include: i. Interoperability ii. Insufficient/contradictory/proprietary standards/platforms iii. Spectrum availability and potential congestion/interference iv. Availability of network infrastructure v. Other

   b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

- *IoT spectrum availability is important. IoT will need spectrum which provides low latency and good penetration. In some cases ensuring reliable Quality of Service*

will be crucially important. Both license exempt and unlicensed models will have a role to play.

- *The ability to have dedicated licensed spectrum in the sub-Ghz bands will help operators build deployment and business cases around this and allow them to effectively ring fence the IoT portion of their business from the mobile portion. This approach allows operators to make use of the 'narrow' bands of licensed spectrum for IoT and avoid further loading of their already 'stressed' mobile networks.*
- *We are seeing the emergence of technologies such as NB-IoT that can be deployed in traditional mobile licensed spectrum.*
- *We are also seeing huge interest in license exempt band wide area networks for IoT. Technologies such as LoRA, Sigfox, Weightless and others are all competing to use the same blocks of sub-GHz ISM band spectrum. Much of this is in ISM bands which may not provide adequate WAN connectivity. The issues around capacity, interference and coverage will be hugely complex to manage in these bands which we expect may limit the business case for deployments in the future.*
- *The notion of 'managed license exempt' bands which are reserved only for specific IoT applications/protocols would allow a balance of maintaining the advantages of license exempt access whilst going someway to help manage the capacity and interference issues and thus help bring new services and investment.*
- *The use of licensed bands would allow operators to provide a service and design a business model around it. This may turn out to be the preferred option for high value IoT cases.*
- *Interoperability is also important.*
- *Three key aspects of interoperability are:*

(i) Internet Protocol (IP) communications capability is key to the success of interoperable IoT. IP needs to go to the end/edge device.

(ii) Edge processing. Lots of processing of data is now possible close to where the data is collected, without the need to pass data through 'gateways' – where there is a risk of proprietary control. 32 bit architecture is already available to do processing even at the edge. So we need an ICT infrastructure which is flexible, enabling processing to be carried out wherever it is most appropriate: at the edge or in the cloud or in between! A model for this is already emerging in eg FOG. (A further advantage of which is that it may help contain the energy footprint of the ICT infrastructure.)

(iii) Open Standards. The development of proprietary silos will damage the growth of IoT and its ability to deliver the full range of commercial and public benefits. The Federal Government should not aim to pick favourites. But it should encourage the widespread use of a variety eg IPv6, 5G, LoRA, Bluetooth, Weightless.

(iv) *Also, as suggested above, there will be a big role for standards based LANs and WANs, which can support Internet Protocol.*

- *The need for the Federal Government to take action on the details of these issues is not clear. It might be best for the Government not to get too specific, while aiming to identify a clear direction of travel.*

6. NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why?

- *Connectivity models for IoT may need to be considered further. The mobile industry has been focussed on delivering mobile broadband through LTE, but this may not serve the interests of IoT devices where factors such as low power, long range and low latency will be important.*
- *Some 'IoT' devices have emerged using 2G. These are effective. But reliance on 2G is coming to an end as carriers look to move away from 2G spectrum and move across to 4G broadband.*
- *There are broadly two models for how IoT conectivity can be provided:*

(i) *Devices connect to a short range radio (such as Zigbee), which in turn connects to a gateway for long range communications, often via a wired network provided by someone other than the IoT device provider;*

(ii) *Devices connect directly to a base station using Low Power WAN (LPWAN). The base station typically serves a large number of devices, thus reducing costs.*

- *Standards bodies have been relatively slow to focus on LWPAN, but we are now seeing the emergence for example of 802.11ah, from the Wi-Fi Alliance, ETSI LTN, and Weightless-N, Weightless-P,NB-IoT. The latter may turn out to have potential: it aims to make possible low cost modules and it may fit well with industry moves*

  to refarm GSM services to LTE.

- *The success of LPWAN will depend on eg: availability of end nodes, low cost and low power, open and accessible standards driven technology and interoperability*

between vendors. The early phase of LPWAN has been dominated by unlicensed use of the so called ISM band (around 900 MHz). It is unlikely that the market will move to a one size fits all: this will probably be different from what we have seen in cellular with the dominance of LTE.

Infrastructure: Infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services.

7. How will IoT place demands on existing infrastructure architectures, business models, or stability?
8. Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?
9. What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?

Economy: IoT has already begun to alter the U.S. economy by enabling the development of innovative consumer products and entirely new economic sectors, enhancing a variety of existing products and services, and facilitating new manufacturing and delivery systems.

In light of this, how should we think of and assess IoT and its effects?

The questions below are an effort to understand both the potential economic implications of IoT for the U.S. economy, as well as how to quantify and analyze the economic impact of IoT in the future. The Department is interested in both the likely implications of IoT on the U.S. economy and society, as well as the tools that could be used to quantify that impact.

10. Should the government quantify and measure the IoT sector? If so, how? a. As devices manufactured or sold (in value or volume)? b. As industrial/manufacturing components? c. As part of the digital economy? i. In providing services ii. In the commerce of digital goods d. In enabling more advanced manufacturing and supply chains? e. What other metrics would be useful, if any? What new data collection tools might be necessary, if any? f. How might IoT fit within the existing industry classification systems? What new sector codes are necessary, if any?

- *Measuring IoT in a meaningful way is not straightforward. The big advantage of the Federal Government measuring it would be to show the pace of take up of IoT,*

thus encouraging businesses and others to consider how IoT can help them maintain and improve services, competitiveness and productivity.

- *One measurement would be of the number of microcontrollers circulating in the market. This is not fool proof: but it would be a measure of how much intelligence and connectivity is being embedded in products and infrastructure.*
- *Measuring industry's investment in IoT could be particularly helpful as a demonstration of how industry is adopting technologies to help improve their business performance. Some of the industrial applications of IoT for example include the ability to provide early diagnosis of failure in capital goods, and other key infrastructure components, and thus allow preventive maintenance which minimises the down time and disruption caused by such failures.*

11. Should the government measure the economic impact of IoT? If so, how? a. Are there novel analytical tools that should be applied? b. Does IoT create unique challenges for impact measurement?
12. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture? a. What will be the benefits, if any? b. What will be the challenges, if any? c. What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?
13. What impact (positive or negative) might the growth of IoT have on the U.S. workforce? What are the potential benefits of IoT for employees and/or employers? What role or actions should the government take in response to workforce challenges raised by IoT, if any?

- *IoT will have an impact on manufacturing. The so called 'smart manufacturing' or Industry 4.0 offers a vision of factories of the future. These will display maximum use of automation, including robotics, the ability to use sensors for better analysis of performance of equipment, including the ability to self diagnose future failures and even, self repair. 3-D printing will offer the prospect of greater versatility, so that factories can respond to changes in demand quickly, and to the trend towards personalisation of products and services. Some operations could be controlled*

  remotely, from a distant HQ.

- *The consequences of this are hard to predict with confidence. Some argue that greater automation will result in a need for fewer workers, thus reducing the*

element of labour in the cost of running a factory. This might mean that we see a trend to repatriate manufacturing from low labour cost markets back to the US , thus creating more factories, which if they don't all need production line workers will need a range of ancillary staff, logistics and delivery staff, suppliers etc

- *Others have argued that the introduction of robots has not in fact resulted in major job losses, since the robots at present work alongside human workers.*
- *One likely consequence is that the workers of the future will need to be comfortable operating in a high tech environment. Equipping them with the necessary skills – whether at school, or afterwards, is going to be a key challenge.*

Policy Issues: A growing dependence on embedded devices in all aspects of life raises questions about the confidentiality of personal data, the integrity of operations, and the availability and resiliency of critical services.

14. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

- *Privacy (see below), security (see below), liability (see below) and skills.*

15. How should the government address or respond to cybersecurity concerns about IoT? a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns? b. How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)? c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

- *If we were to highlight a defining characteristic of IoT security it might focus on:*
- *The need to provide sufficient computing capability for small, embedded devices to be able eg to provide for encryption and receive upgrades over the air in a constrained setting, where energy efficiency is key and where small size matters.*
- *This can be achieved through eg*

(i) providing a hardware root of trust in the microprocessor itself, to create a secure operating environment for sensitive operations.

(ii) Providing even in small scale devices sufficient computing power to be able to generate encryption and to receive over the air upgrades.

- *Secure Identity authentication may be even more important in an IoT world. Latest developments in single (or dual) factor authentication using asymmetric cryptography (see the work of the FIDO Alliance) are important.*

16. How should the government address or respond to privacy concerns about IoT? a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns? b. Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)? c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

- *Since IoT will involve many more sensors collecting and sending much more data there is a risk that the perception will be that it constitutes a greater threat to privacy. This needs to be addressed, but probably by industry rather than the Federal Government. The tools required to address it are well known:*

(i) *companies need to commit to using state of the art security technology to protect data in transit and in storage, including from insider attacks by disgruntled employees or former employees.*

(ii) *Companies who handle data need to find ways to reassure customers about how they will use that data. Key to this is the need for transparency, probably expressed in simpler terms than current Ts&Cs.*

(iii) *Serious sanctions may need to be introduced to discourage any attempt at reidentifying anonymised data, particularly where customers have been told that their data will only be used in anonymised form.*

17. Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?
    - *It is not yet clear whether IoT will raise new issues around liability for product safety etc.*
    - *Although IoT products will be complex, involving hardware, software and service providers, they may not necessarily pose conceptually new liability issues. Existing liability law has developed a practised framework for allocating liability . But in Europe, the Commission is asking whether existing approaches to liability will provide for a sufficiently rapid redress in IoT cases.*

18. In what ways could IoT affect and be affected by questions of economic equity? a. In what ways could IoT potentially help disadvantaged communities or groups? Rural communities? b. In what ways might IoT create obstacles for these communities or groups? c. What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access? d. What role, if any, should the government play in ensuring that the positive impacts of IoT reach all Americans and keep the negatives from disproportionately impacting disadvantaged communities or groups?

International Engagement: As mentioned earlier, efforts have begun in foreign jurisdictions, standards organizations, and intergovernmental bodies to explore the potential of, and develop standards, specifications, and best practices for IoT. The Department is seeking input on how to best monitor and/or engage in various international fora as part of the government's ongoing efforts to encourage innovation and growth of the digital economy.

19. What factors should the Department consider in its international engagement in: a. Standards and specification organizations? b. Bilateral and multilateral engagement? c. Industry alliances? d. Other?

- *As indicated above there are many standards bodies looking at different aspects of IoT. The challenge is to encourage the emergence of effective standards which do not compromise interoperability.*

20. What issues, if any, regarding IoT should the Department focus on through international engagement?

21. Are there Internet governance issues now or in the foreseeable future specific to IoT?

22. Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?

- *The manufacture of IoT sensors is likely to be a global business. Support for open trading arrangements across regions will help.*

24. What factors can impede the growth of the IoT outside the U. S. (e.g., data or service localization requirements or other barriers to trade), or otherwise constrain the ability of U.S. companies to provide those services on a global basis? How can the government help to alleviate these factors?

Additional Issues:

25. Are there IoT policy areas that could be appropriate for multistakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity?

26. What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the Department of Commerce best collaborate with stakeholders on IoT matters?

- *It might be useful to set up some sort of IoT forum where industry can exchange ideas with the Commerce Department. The agenda of such a group would not be primarily technical, or focus on standards etc. It would focus on how to stimulate IoT take up, how to realise its wider societal benefits, and how to build public confidence in it. It would also look at areas where a market failure might impede take up.*

27. How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would an overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?

- *This might be usefully discussed in the sort of group suggested above.*

28. What are any additional relevant issues not raised above, and what role, if any, should the Department of Commerce and, more generally, the federal government play in addressing them?

Contact:

Stephen Pattison, VP Public Affairs, ARM, Stephen.Pattison@arm.com

110 Fulbourn Rd , Cambridge, UK CB1 9NJ

ARM May 2016