Comments by Amcham India on draft Internet of Things (IoT) Policy released by the Department of Electronics & Information Technology (DeitY), on October 16, 2014

Standards

The Draft IoT Policy already acknowledges the importance of technical standards to ensure the growth of IoT industry in India. We believe that the role of the Government of India should be to develop initiatives that support IoT innovation and facilitate the growth of IoT industry and ecosystem with voluntary global standards. Hence, Amcham agrees with the objective stated in Draft IoT Policy that the Government of India should encourage and prioritize participation in worldwide standards related efforts addressing IoT market needs including ISO/IEC JTC1, IEEE, the Industrial Internet Consortium, and other global standards and industry organizations.

We would however urge the Government of India to be cautious with respect to any proposals to develop IoT standards exclusively for India. We appreciate that concerns of health and national security are paramount and there would be circumstances where the Government must step in to ensure that IoT related goods sold in India conform to specific Indian standards mandated to ensure the health and safety of Indian citizens. However, as DeitY has observed, the technology sector has benefited from the global standardization process developed in a variety of international Standard Setting Organizations (SSO), which are open for participation by all interested parties – these organizations range from formal international bodies to global industry-led standards organizations. Technical standards developed in these SSOs facilitate interoperability between devices which follow these standards and implementation of communication standards also enable devices to connect with communications networks.

As the Draft IoT Policy rightly states, IoT is essentially a "*seamless connected network* of *embedded objects*". For this network to operate it is important to ensure that IoT devices (i.e., the embedded objects) are in accordance to global standards so that they can 'talk' to each other across borders and over the global communications network. This is best achieved by supporting Indian participation in the development and adoption of global standards. In cases, where the Government determines there is a justified need for local standards development, it would be a mistake for India to develop standards that do not interoperate globally, as this would limit India's ability to profit from IoT innovations outside its borders or for local industry to participate in global IoT ecoystems.

We would also point out that excessive mandatory Indian standards with regard to IoT devices can potentially make India as an unattractive hub to manufacture and deploy IoT products. Global companies establish manufacturing facilities in a small number of countries and then ship the products globally. IoT enabled devices manufactured in India while following the '*Value Up' and 'Cost Down'* model can have tremendous market across the developing world. In the event the Government of India imposes Indian specific standards on IoT products, companies might not be able to sell products made for India in the global market. Also, global and local manufacturers will not be able to market IoT products specially manufactured for Indian market to other countries and jurisdictions. Hence even if manufacturing facilities are set up in India, such manufacturing facilities will never be able to reap benefits of economies of scale from ability to access the global IoT marketplace. Indeed, ultimately India might not be able to integrate itself to the global supply chain which is important for India's continued economic growth.

Hence, we request that rather than following a path of 'top down' approach of mandating standards, the Government of India should rather increase participation in the variety of global SSOs and increase public/private cooperation for development of voluntary global standards. Further the Government should encourage Indian companies and academics to get more active in the global SSOs.

We believe increased participation in global standardization forums will ensure that India is able to influence and contribute to emerging IoT related standards and application markets. Mandatory country specific standards should be put in place only when their need can be scientifically provable and there are justified unique Indian concerns regarding a particular technology.

In short, Amcham would request the Government to support the open participation of global standards and interoperability necessary to achieve a successful IoT ecosystem. In the emerging IoT economy, voluntary global standards can accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. Furthermore, open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology evolution path.

Amcham believes that industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges, with the Government as a key participant. DeitY should encourage industry to collaborate in open participation global standardization efforts to develop technological best practices and standards. The Government should also encourage the use of commercially available solutions, which implement global standards and best practices, to accelerate innovation and adoption of IoT deployments. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.

Privacy and Security

We commend DeitY for appreciating that for an IoT ecosystem to be successful, "*data needs to be openly collected and shared between cross functions to bring out maximum benefits*". The Draft IoT policy also rightly underscores the importance of analytics in a successful IoT ecosystem. In order for Government, consumers and business to reap the full benefits of the IoT, devices must be able to connect to the 'cloud' and the 'edge,' and able to both upload and download data from the 'cloud'.

In such a connected environment, it is important to ensure that the users are able to have trust in the ICT infrastructure. As the draft IoT policy rightly points out there is an urgent need to discuss and debate these issues in various forums. Often a 'one size fits all' approach does not work in an ecosystem as diverse as the IoT. For example, encryption key lengths considered appropriate in one device might not be adequate for another device.

Considering the cyber security is an ever evolving challenge, all stakeholders- the Governments, industry and academics- must cooperate and coordinate efforts to proactively mitigate cyber security risks. We appreciate DeitY's efforts to ensure such a collaborative environment where all stakeholders can cooperate to develop an appropriate cyber security environment.

We understand that the Government of India is drafting a privacy law for India. Through DeitY, we request the Government of India to consider issues concerning the emerging IoT industry while drafting the Privacy law for the country. While some of the traditional privacy principles developed in the 1970s may still be relevant, the applicability of some specific principles will need to evolve to be nuanced inappropriate for an IoT ecosystem.

For example, it might be difficult to obtain and document traditional 'consumer notice and consent' in an IoT environment. However, other principles, such as accountability principle, continue to be very relevant in an IoT environment. Amcham looks forward to discussing the privacy and security issues with the Advisory Committee which will be established by DeitY as well with the other departments of the Government of India.

In summary, security and privacy are critical building blocks for the IoT ecosystem – and capabilities that must be designed into IoT systems from the outset using the best known Privacy-by-Design methodologies.1 To maximize the potential of an IoT ecosystem, India's IoT policy must have a clear and implementable privacy and security strategy. This strategy must contemplate the range of purposes and risks among the various market applications, sectors, and domains, and create a logical and implementable framework that encourages industry innovation for appropriate solutions. For trusted data exchange in the IoT ecosystem, data generated by devices and existing infrastructure must be able to be shared between the cloud, the network, and Intelligent devices for analysis – enabling users to aggregate, filter, and share data from the edge to the cloud with robust protection. Moreover, data must be accurate to be beneficial.

So DeitY's IoT policy must promote the importance of accuracy and integrity of data in all market sectors, but especially in the industrial domain where the safeguarding of critical infrastructure can be vital to economic and social stability. India's IoT policy also must evoke consumer and industry trust through hardened privacy and security solutions in order to motivate adoption and participation in the IoT marketplace. With respect to privacy, Amcham recognizes that the IoT presents new challenges for traditional privacy principles.

Consumer notice and consent will continue to be important, however other privacy principles also must be emphasized to ensure consumer privacy is adequately protected. For example, focusing on accountability for the appropriate collection, use, and protection of the consumer's data. Optimal privacy and security methods must be developed as required for different IoT solutions. Use cases should be used to proactively identify privacy and security risks and to develop robust strategies to mitigate those risks.

Spectrum

The Draft IoT Policy already notes the need to discuss spectrum related issues for a successful IoT ecosystem. Ubiquitous, affordable, high speed broadband connection over both the licensed and unlicensed airwaves is critical for a successful IoT ecosystem. It is also critical to ensure that IoT devices enjoy connectivity and interoperability with legacy systems. Amcham looks forward to discussing the spectrum related issues with the Advisory Committee which will be established by DeitY as well with DoT and other departments of the Government of India.

Some Specific Parawise Suggestinons

Under 'BACKGROUND', the IoT opportunity information is good. However, the three distinct stages of IoT are not highlighting the key phases adequately. IoT is a data centric opportunity and includes Big Data and Analytics/Insight. The 3 key stages are – data capture, data collection/ ingestion and data analytics. We need to change point no 2 in particular as 'data collection' will typically happen at the edge of the enterprise (DZM) and this layer will need to handle security and scalability in particular. We suggest the following change –

Background

Contents currently in there

Internet of Things involves three distinct stages:

1. The sensors which collect data (including identification and addressing the sensor/device),
2. An application which collects and analyzes this data for further consolidation and,
3. Decision making and the transmission of data to the decision-making server. Analytical engines and Big data may be used for the decision making process.

Recommended changes

Internet of Things involves three distinct stages:

(i) 'instrumentation' or data capture at the sensors;

(ii) ''data ingestion' using a scalable, secure and reliable gateway at the edge of the enterprise, capable of handling growing number of connections and consuming the data at massive scale;

(iii) 'deriving intelligence' or capability of consuming the Big Data and performing real time analytics to enable predictive decision making.

Page 4

The definition gives the policy document a M2M specific flavor rather than Internet of Things. This will likely limit the scope and reach of the program. The explicit mention that 'Phones, Tablets and PCs are not included as part of IoT' has a restrictive implication. If this has been done to ensure that the policy for these devices is separate and should not be confused with IoT, we could explicitly mention the same rather than making the definition restrictive. We suggest the following change –

Definition

Contents currently in there

> "IoT is a seamless connected network of embedded objects/ devices, with identifiers, in which M2M communication without any human intervention is possible using standard and inter operable communication protocols." - Phones, Tablets and PCs are not included as part of IoT.

Recommended changes

> Recommend dropping the line - - ~~Phones, Tablets and PCs are not included as part of IoT~~
>
> Instead of this adding... Such interactions can be augmented with context such as geo-location, time and so on by leveraging devices such as phones/ tablets/ hand-helds and using these to enable communication between 'devices' and 'people'.
> Its important to note that though these devices can participate in IoT scenarios, the policy governing such devices (Phones, Tablets and PCs) will be separately laid out.

Page 5 onwards… Pillars of IoT and plan details

The details talk about investment plans but a holistic business model is not coming across. It will give a clearer view if we can add information around how are these investments going to yield the returns or what opportunities does it open up.

Some additional details can be included to make this complete –

1. An in depth analysis of the partner ecosystem in the context of where India has both strengths and gaps.

2. More on how to use the local opportunity to build a base for the global opportunity.

3. Some level of details around commercialization and business analysis.

Page 10

Standards

This is an important topic and it needs to be addressed carefully. We need to be cautious around too much emphasis on standards. This is a fragmented space and moving quickly. Standards will catch up with the real work, so its important to be aware and involved as these standards take shape and be agile in adopting to them. We should be careful not to create any India specific standards here which have a restrictive impact.

Page 11

Attention will be needed on how to commercialize the R&D investment. This will attract industry participation.

Page 12

Suggest that we re-title 'incentive and engagement' to 'Business Enablement'. Use of venture capital and accelerators, business training for start-ups.and also some of the sections already covered should still be included.

Page 15

Governance structure misses participation from vertical industry consumers of the technology unless that is what the Industry Experts are expected to bring.

Amcham India 01.12.2014
New Delhi