HSA ADVOCATES
HEMANT SAHAI ASSOCIATES

LAW & POLICY UPDATE

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Internet of Things (IoT) – Policy and challenges in India

By: Gaurav Sahay, Partner & Shreya Pola, Associate

Internet of Things (**IoT**) is essentially a seamless connected network of embedded objects/devices, with identifiers, in which M2M communication without any human intervention is possible using standard and interoperable communication protocols. The IoT ecosystem is booming exponentially, not only in India, but across the word.

The IoT ecosystem comprises of a close relationship between software, electronic hardware and telecommunication industries. The number of Internet-connected devices (12.5 billion) surpassed the number of human beings (7 billion) on the planet in 2011, and by end of 2020, Internet-connected devices are expected to number between 26 billion and 50 billion globally. It is predicted to offer outstanding scope and opportunities to many industries in India.

In 2015, the Government of India had formulated a Draft IoT Policy with a vision to develop connected and smart IoT based system for our country's economy, society, environment and global needs. This Policy launched a Smart City project, with a plan of developing 100 smart cities in the country, by allocating INR 7,060 crores for the same. In continuation of this endeavor, the launch of the Digital India Program aims to transform the Indian society into a digitally empowered society and boost the IoT industry. The proposed smart cities shall consist of smart homes, smart parking, smart phone detection, smart transportation, smart roads and smart lighting.

Draft IoT policy adapts a multi-modal approach, comprising of five vertical pillars: Demonstration Centres, Capacity Building & Incubation, R&D and Innovation, Incentives and Engagements, Human Resource Development, which focuses on areas that promote engagement and awareness with IoT in India and two horizontal supports, Standards and Governance structure, which are essentially the regulatory functions to govern IoT in India.

The government has laid down the policy to form an effective structure for appropriate governance of IoT activities and its implementations. Firstly, it lays down provisions for setting up an Advisory Committee, which will have the responsibility of formulating guidelines concerning the emerging areas of IoT. Secondly, a Governance Committee shall be formed for implementing effective governance policies and projects in India. Lastly, a Program Management Unit will be formed, chaired by director of IoT operation with smart city support, to provide appropriate support to the detection of multifarious initiatives to operationalize IoT policy effectively and to review periodically the on-going IoT projects for their successful completion on time.

With its increasing usage, following concerns and challenges cannot be ignored and need to be addressed effectively:

- **Privacy**

  Privacy has always been a major concern in India. Through use of IoT and associated devices, large quantities of personal data and sensitive personal data in certain cases, are exchanged. The data networks are delicate and operation of storage in data clouds are still in development stage in India. Therefore, data stored in a cloud service and not protected adequately may result in unauthorized third-party access and information leaks, who may use and process it for unwarranted purposes. For example, data collected by a smart fridge can be used by insurance companies to detect food habits and health conditions of residents. Hence, there is a need to form strict regulations to keep a check on this. However, the Draft IoT policy fails to address this crucial issue and it warrants immediate attention.

- **Security**

  Ensuring effective security practices is an essential practice in the development and design stage of IoT devices. Principles such as confidentiality, reliability, safety, availability, robustness, survivability, authenticity, resilience, identity management, access control, accountability and utility play a key role in the development of security of the IoT connected devices. With an increase in the demand for IoT devices, developers and manufacturers have shifted their focus to increasing the quantity of devices instead of ensuring the quality of devices. This has resulted in mass manufacture of cheap and low standard designed devices, making its security vulnerable and weak. Since the IoT arrangements also include making of similar devices, the homogeneity expands the potential impact of any single security weakness to all the devices having the same features.

- **Infrastructure in India**

  The lack of an efficient infrastructure to support the growing usage of IoT devices is a major challenge faced by the industry. Currently, with unsteady and unstable accessibility of internet connection across the nation, India faces a big hurdle in ensuring strong internet connectivity across its boundaries, especially the rural areas. The use of IoT devices in areas where Internet availability/bandwidth is not adequate, would remain a major challenge.

- **Lack of standardization**

  The absence of standards or SOPs for the manufacture and design of IoT devices can result in low quality and cheaply designed/ configured devices, which may have undesirable consequences for the users. Without any standards to assist and guide the developers and manufacturers, the design products may result in troublesome operations. Therefore, there is a need to formulate a standard in order to ensure that the quality of the devices and the growth of the industry is effective, efficient and not disruptive.

An assessment of the recent market trends in the IoT sector shows that there is both awareness and the desire of the consumers to be connected and have smart and intelligent systems. Additionally, with the government's constant underlying efforts to improve infrastructure supporting IoT, this industry is expected to grow at an exponential pace in the coming decade. However, challenges such as privacy and security of the devices need to be addressed and regulated in order to ensure that the negative impacts of the IoT ecosystem do not override the potential positive changes it can bring about to the country.