INTERNET OF THINGS, BIG DATA AND THE LAW

Written by ***Aprajita Tyagi* & Ankit Bajpai*****

* Senior Manager (Legal), Aditya Birla Idea Payments Bank Ltd.

** Business Consultant, ZS Associates

INTRODUCTION

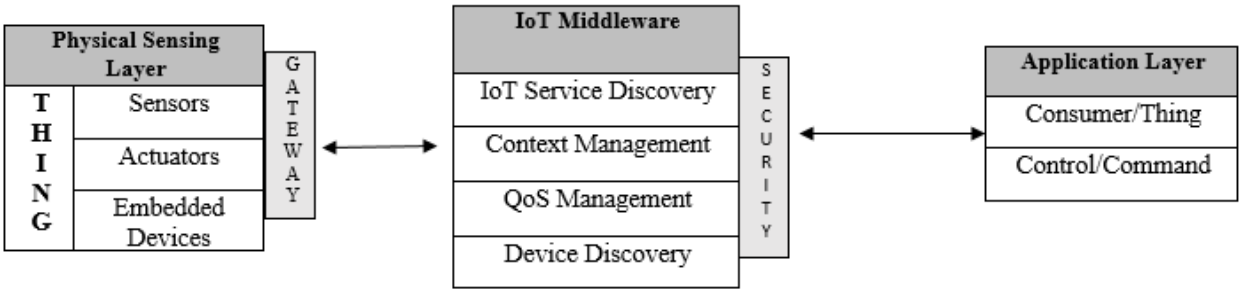
The term Internet of Things (IoT), first used by Kevin Ashton in 1999, refers to integration of 'Things' through sensors and network, enabling communication amongst them. 'Things' in IoT context refer to any person or man-made object/device (atoms) that can be assigned an IP address and provided with the ability to transfer data (bits), and to interoperate within the existing Internet infrastructure.[1] Simply put, IoT connects objects of the real world with the virtual world, enabling activities useful for humans, thus, blurring the lines between atoms and bits in the process.

BASIC IoT ARCHITECTURE

A basic IoT system architecture consists of three layers:

- The physical sensing layer- contains embedded devices that make use of sensors to gather real world data. It provides the mechanism and protocols for devices to expose their sensed data to the Internet.
- The middle-ware layer- facilitates and manages the communication between the real world sensed activities and the application layer.
- The application layer- medium that can be used by the consumer to send commands to real word objects over the Internet via mobile applications, webapps, etc.

[1] John A. Stankovic (2014): Research Directions for the Internet of Things. IEEE Internet of Things Journal 1(1), p. 3–9, oi:10.1109/jiot.2014.2312291

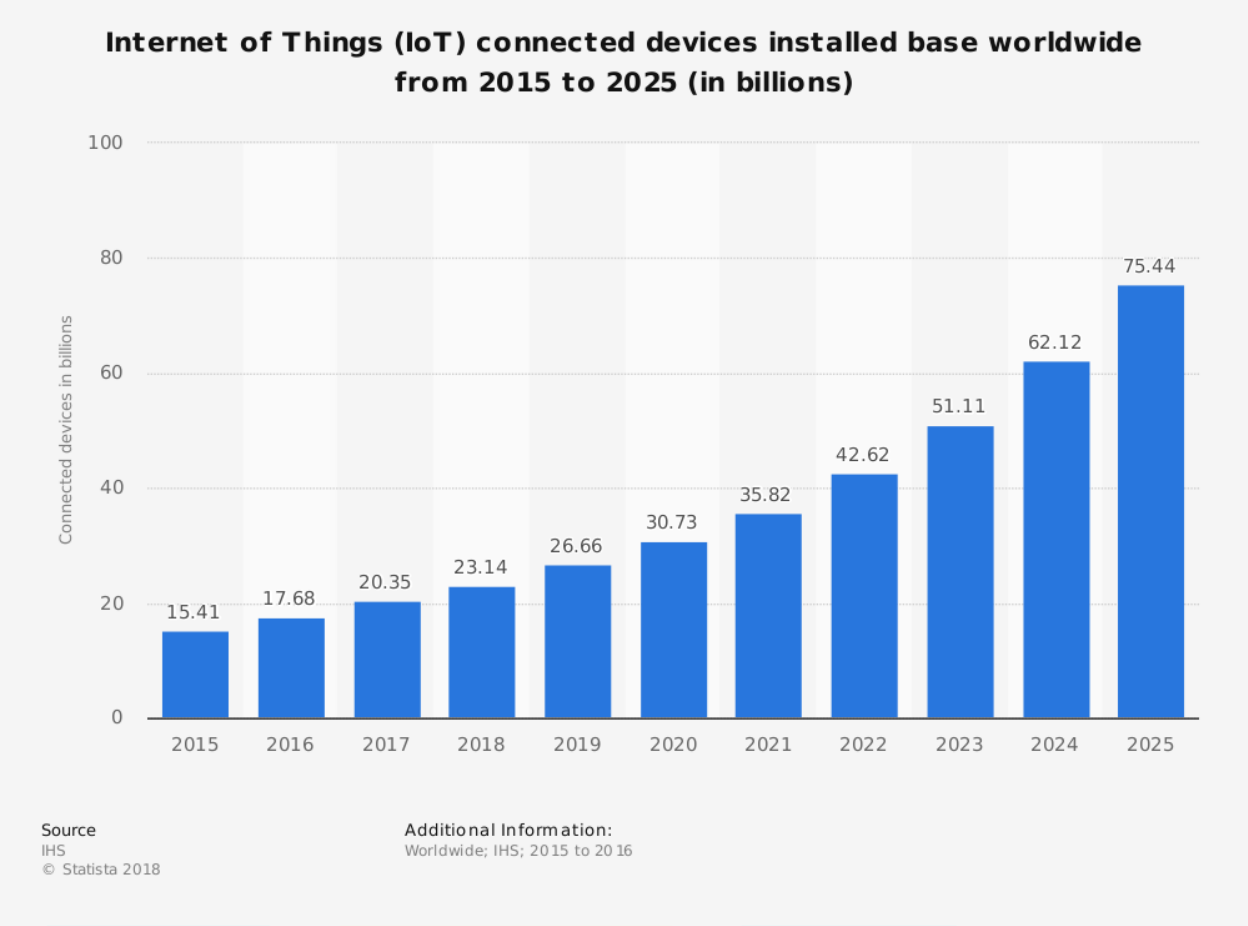


IoT- basic architecture[2]

IoT, BIG DATA AND ANALYTICS

What started as a simple exercise of installing sensors in the Coca-Cola machine to track availability of cool drinks at Carnegie Mellon University (1970), has led to integration of devices to build smart cities of tomorrow, smart wearables, power grids, medical devices etc. It is predicted that by 2020, the installed base of sensors/devices in India is expected to grow to 1.9 billion units[3] and globally, to 30.73 billion. All of these devices will gather, analyze, share, and transmit data in real time.

[2] IoT Architectural Framework: Connection and Integration: Framework for IoT Systems, Onoriode Uviase Gerald Kotonya, School of Computer Science and Communication, Lancaster University, Lancaster, UK
[3] IoT: Landscape and Nasscom Initiatives, 2017 (Source: GoI draft policy on IoT, Industry reports) https://www.wfeo.org/wp-content/uploads/stc-information/L3-IoT_Landscape-by-S_Malhotra.pdf



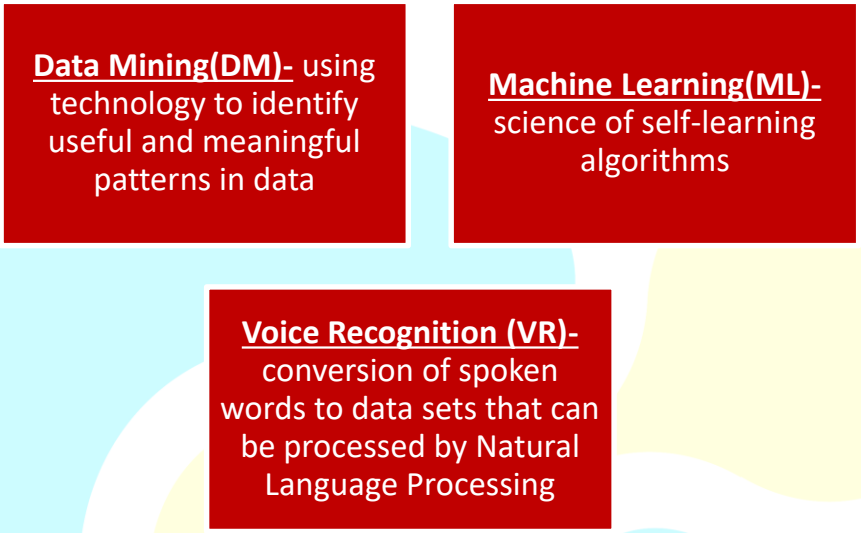
(IoT connected devices installed base worldwide from 2015 to 2025)

Information generated by these IoT devices can be categorized as 'Big data', where, the term 'Big data' is defined as a large amount of structured, unstructured or semi-structured data, and includes sensitive information like behavioral patterns (likes, dislikes, daily routines etc.).

IoT big data analysis involves a large amount of unstructured information generated by IoT devices, which is collected in the big data system (a shared distributed database) and stored within the big data architecture. This information is analyzed using analytic tools and concluded with generation of reports of such analyzed raw input. This holds huge potential for sectors like healthcare, retails, home solutions, where data analytics cannot just help reduce human dependency and eliminate human error in the process, but also help entities analyze human interests to assess market trends, enable supply chain management and improve customer experience.

ROLE OF ARTIFICIAL INTELLEGENCE IN INTERNET OF THINGS

IoT offers multiple opportunities across industries including better stock management, marketing and promotion, handling complaints etc. Artificial intelligence techniques play pivotal role in enabling the aforementioned. Some of the techniques being used are:



- Data Mining: Since devices in an IoT framework generate huge amount of data, data mining is used to manage this data through extraction (selection of wanted data from the huge volume generated), cleaning (repeated data or junk data is removed) and transformation (transforming the cleaned data into a standard format which can be read across workstations and sending it out to the network), as well as to reduce the storage space. Data mining helps one discover trends and patterns within big data.
- Voice recognition: to enable control of device as well as to enhance customer experience.
- Machine learning: to find patterns, correlations and anomalies in the data generated by IoT which will enable better decision making and help improve various facet of our daily lives.

NEED FOR INTEROPERABILITY AND STANDARDIZATION

Interaction amongst devices is at the heart of IoT. Since devices forming part of the IoT ecosystem are manufactured by various manufacturers, they may use different operating systems, data communication protocols etc. As a consequence, interoperability becomes an

issue. For successful integration, devices need to be compatible with each other i.e, convergence at a macro level. This requires global standard, common architecture and open source software frameworks, in addition to low cost, high efficiency connectivity.

IoT AND LAW

From European Union to US Federal Trade Commission to Government of India, agencies/entities around the globe have joined the IoT bandwagon. However, the existing legal framework is far from equipped to address issues related to IoT.

IoT presents many legal challenges, including:

- Jurisdiction issues
- Data privacy, liability and risk allocation
- Data ownership and intellectual property rights
- Formation and validity of online contracts (e-contract)
- Consumer protection and product liability

JURISDICTION

In a traditional scheme of things, the courts in a country have jurisdiction over individuals who are within the country and/or to the transactions and events that occur within the borders of the country. However, in an IoT scheme of things, there is a huge possibility that the entities/users who are part of the IoT framework, are present in multiple jurisdictions. In such scenarios, the question of jurisdiction assumes importance. Parties need to decide where they go to seek justice, which is the right forum, etc.

In scenarios where manufacturers sell device/software across nations, they may be required to defend any litigation that may result in the country of sale. As a result, the device manufacturer should review the local laws before marketing or selling its products or services, as they may run the risk of being sued in any jurisdiction where the goods are bought or where the services are availed. Further, the local statutes of a country may provide for a 'long arm jurisdiction' whereby the operation of such local laws have extra-territorial application if an act or omission results in some illegal or prejudicial effect within the territory of the country (under Indian law,

the Information Technology Act, (ITA) 2000 and Indian Penal code provide for such extra territorial jurisdiction).

DATA PRIVACY, LIABILITY AND RISK ALLOCATION

Data privacy, liability for breach as well as allocating risks amongst the parties that are a part of the IoT framework, present pressing legal issues. These issues warrant due attention since the majority data that these IoT devices generate/use, is personal data, some of which is highly sensitive (like medical information).

Consent: Under the current law, many jurisdictions (like EU General Data Protection Regulation (GDPR)), require express consent of the end user (data subject) for collection of their personal data. In an IoT framework where devices collect data in the background and transfer data to other connected devices, obtaining consent becomes a major concern.

In the Indian Context, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 cover companies (including firms, sole proprietorships, and associations of individuals), engaged in commercial/professional activities, within its ambit. Thus government bodies and individuals engaged in data processing are not covered under the rules. Further, the rules draw a distinction between 'sensitive personal information' and 'personal information'*, where sensitive personal data has been restrictively defined thus excluding information like individual habits, travel data etc., which in itself can be sensitive in nature if one looks at it from a privacy perspective.

Privacy: Even if the data collected is encrypted to ensure anonymization, since data is fed through multiple devices, and these devices interact with each other, a combination of data collected from multiple devices make user profiling easier than ever and anonymity loses significance. This again poses a huge risk to right to privacy of the data subjects. In India, right to privacy has been recently recognized as a fundamental right[4] and breach thereof will come with its own set of consequences. In such a scenario, it is important that device/software manufacturers address such privacy concerns at the manufacturing/coding stage itself.

[4] *JUSTICE K S PUTTASWAMY (RETD.), AND ANR*. V. *UNION OF INDIA AND ORS*., 2017

(*'Personal information' means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person[5]; 'Sensitive personal information' pertains to information sensitive in nature such as passwords, health conditions, sexual orientation, medical records and biometric information, etc.)

Regulations like EU GDPR, and ITA, require entities to inform the user of the purpose for which data has been collected, and allow control over personal data. Further in order to ensure transparency, Information Technology Rules[6] require body corporate across the chain of data processing that engage in the collection, storage, or otherwise deal with, or handle Personal information, to publish a privacy policy on their websites. The privacy policy is to clearly delineate their data processing practices, the type of personal information collected, the purpose of collection and usage, as well as details of disclosure made to third parties, and the reasonable security practices and procedures adopted. The ITA[7] provides penal liability for any wrongful disclosure of personal information secured while providing services under the terms of a lawful contract thus providing remedy to data subjects wherein their information is collected pursuant to a contract. Since multiple devices collect, transmit and process information in an IoT ecosystem to provide users with desired results, device manufacturers will not be in a position to enlist the exact purposes for which data will be used. Further, since the data, as originally collected from users, itself may undergo changes during its processing and generate new data, providing users control over the data collected from them, including deletion thereof, would have little significance.

Information Technology Rules[8] mandate that the body corporate obtain consent from data providers prior to any collection, disclosure, or transfer of data. Rule 5[9] also requires a body corporate to take steps to ensure that data subject knows that data is being collected, the purpose of collection, intended recipients of information, the particulars of the collecting agency, and

[5] 2(i) of ITA
[6] Rule 4, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[7] Section 72A of the ITA
[8] Rule 5,6 and 7, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[9] Rule 5(1) and 5(3), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

where the collected information will be stored. These stipulations are again limited in their applicability to sensitive personal information.

While availing the service/product, from a body corporate, data subjects may at any time withdraw their consent to share their data with the body corporate. Such withdrawal is to be indicated to the body corporate in writing. Once a data subject has opted out, the body corporate has the option to cease provision of the service/product for which the impugned data had been sought.[10] The Information Technology Rules do specify that the body corporate holding sensitive personal information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law[11], however, this concept of data deletion is limited to sensitive personal information. Also, no provision has been made to allow data subjects access to the data shared by them in the past which is stored by the data collectors, so that they may switch service providers. In view of the existing provisions, the data controller (manufacturer/service provider in Indian context), needs to lay down the data that is being collected and its proposed usage, covering all foreseeable scenarios. Also, since data is collected by/shared/processed by multiple entities in IoT construct, each manufacturer/service provider needs to clearly limit its liability and allocate risk through the agreements executed amongst such entities as well as in the end user licensing agreements/terms and conditions, executed with the end users.

DATA OWNERSHIP AND INTELLECTUAL PROPERTY RIGHTS

As regards the data ownership, due to multiplicity of entities, Machine to Machine (M2M) communication and consequent data generation, the ownership over data collected/generated in IoT framework is difficult to determine.

Going through the prevailing copyright principles in United States, joint ownership in a copyright work is created when a work is prepared by two or more authors with an intention

[10] Rule 5(7), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[11] Rule 5(4), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

that their contributions should be merged together[12]. Section 2(z) of Copyright Act, 1957 of India defines 'work of joint authorship' as a work produced by the collaboration of two or more authors in which the contribution of one author is not distinct from the contribution of the other author or authors; Therefore, in the absence of a contract to the contrary, when entities allow interaction of their devices and generation of data therefrom, joint ownership can be presumed.

Further, for expansion of IoT framework on a global level, interoperability is an important factor. However, in scenarios where the underlying standard technology is patented by an entity, interoperability and standardization becomes a challenge, since any party adopting standardized technology will end up infringing patents of such third party patent owners. Therefore, there is a need for global cooperation to ensure that such patents are declared as standard essential patents* and are licensed on reasonable terms in a non-discriminatory manner.

(*Standard essential patents are patents essential to implement a specific industry standard. Standards are technical requirements or specifications that seek to provide a common design for a product or process. Patents which are essential to a standard and have been adopted by a Standard Setting Organization (SSO) are known as SEPs).

E- CONTRACTS

For IoT systems, the users and manufacturers usually enter into e-contracts (click wrap/shrink wrap). Concerns surrounding liability, ownership and privacy can be addressed by executing such contracts sufficiently laying down the rights and obligations of the parties involved. Various jurisdictions, including India, give recognition to such e contracts[13]. To be enforceable, e-contracts need to fulfill basic requirements laid down under contract laws for formation of valid contract (Offer, Acceptance, Free consent, consideration and legal object).

Data controllers will need to ensure that the terms of such e-contracts are not one sided (i.e., all terms in favor of the controller) to ensure that the validity is not challenged on the grounds

[12] Section 101 of Copyright Act of 1976
[13] Section 10A, ITA

of lack of free consent or undue influence. Further, in most IoT cases there is no privity of contract amongst multiple device manufacturers forming part of the IoT ecosystem, hence defining the relations and obligations between such parties will remain a challenge.

CONSUMER PROTECTION AND PRODUCT LIABILITY

Imagine a scenario where a medical device malfunctions and dosage for a critical ailment is skipped or a scenario where communication failure results in non-communication of smoke detected in a manufacturing plant. These are just some of the examples of far-reaching effects a device or network failure can cause in IoT framework.

Courts across jurisdictions are adopting consumer friendly approach of strict liability in cases involving product liability, as against the traditional principal requiring proof of negligence of a manufacturer. Further, India has multiple consumer oriented laws (like Consumer Protection Act, 1986, the Legal Metrology Act, 2009 etc.), which provide for special courts/forums that work on a fast track basis and protect and allow consumers to sue and obtain remedies easily when sold defective products. The manufacturers can guard themselves by way of product liability insurance against such scenarios and additional cost could be distributed amongst their consumers.

CONCLUSION

Sectors across the globe are in early stages of IoT adoption but IoT is also making its way into our everyday lives. Though IoT presents the world with plethora of opportunities yet there remain multiple technical and legal issues which need to be addressed to avoid catastrophic consequences. What's unique in this case, is the requirement for global co-operation both in terms of standardization of underlying technology as well as the law regulating the technology, to enable both innovation and for safeguarding human rights. Further, law needs to keep up with the pace at which technologies are evolving, and at the same time, be drafted in such a fashion that it lays down the basic principles, in addition to addressing specific scenarios, so as not to become obsolete in a short span of time.