IoT & Convergence: Is It Risk Free?

Published on Wed, Aug 05,2015 | 16:13, Updated at Wed, Aug 05 at 16:23Source : Moneycontrol.com

By: Huzefa Tavawalla, Co-Head, International Commercial Practice and Smitha Prasad, Senior Associate, Nishith Desai Associates

Constant developments in technology, along with an incredible growth in the form and use of the internet over the past few decades has led to a convergence of the internet and service providers.

Simultaneously, the world has seen immeasurable progress on the hardware front over the past century, from supercomputers the size of a large room, to a watch that can check your text messages, and clothes that can check your pulse and heart rate.

The result – **'IoT'**, a world where every 'thing', phones, kitchen appliances, cars, watches, clothes, shoes, streetlights, highway toll booths, can be connected to the internet, and to multiple other 'things' via the internet.

With predictions that IoT technology market will accrue a value of around $1.9 trillion by 2020 , the past few months have seen a torrent of announcements made by global leaders such as Cisco, Google, Samsung, Apple, Qualcomm, Freescale – *whether engaged in the business of manufacturing devices, providing network solutions or software development* – on setting up incubators, research centres and undertaking large investments to further develop the IoT.

With the rapid growth of the internet along with its convergence, the Indian government also realized the requirement of a policy framework associated with this sector. Thus, in April 2015, the Department of Electronics and Information Technology released a draft policy on the 'Internet of Things' ("**IoT**").

Additionally, recent Government initiatives towards the 'Digital India Program', which aims to transform India into a '*digital empowered society and knowledge economy', and the draft IoT policy looks to "develop connected and smart IoT based system for [India's] economy, society, environment and global needs*". The allocation, during the announcement of the Budget 2015, of INR 1000 crores to the self-employment and talent utilisation program – a techno-financial, incubation and facilitation program to support all aspects of start-up businesses, and other self-employment activities, particularly in technology-driven areas will no doubt add to the array of initiatives taken up by the industry, to spur greater growth in the area of IoT.

Every new technology brings along with itself new legal and tax issues! IoT also comes with its own range of nuances that the legal world must keep up with.

In this article, we have highlighted some of the significant legal issues and challenges related to IoT along with providing insights on the regulatory framework associated with this sector.

1. Privacy and Security

The use of smart / wearable devices and the IoT is resulting in huge amounts of 'Big Data'. With multiple devices communicating with each other, personal information of users will be

shared between devices, service providers and users, thereby raising security concerns.

Stakes are even higher, for example in the context of e-health, the collection and rapid exchange of sensitive personal information in an interconnected and open environment not only increases risks in respect of patient confidentiality, but also has the far more alarming potential to endanger life if one takes the example of implanted medical devices administering drugs on the basis of autonomous data inputs.

A system failure or more sinister malicious attack on such device could have dire consequences.

The European Commission's draft Data Protection Regulation 2012 ("**Draft Regulation**"), which is currently going through the EU legislative process and is expected to be adopted in 2015 tries to address some privacy and security issues in relation to IoT.

The Draft Regulation provides that, the data controller must, '*implement appropriate technical and organisational measures in such a way that processing information will ensure the protection of the rights of the data subject'.* The Draft Regulation also provides for additional data security measures, including requirements for companies to notify their respective national authorities of any incidences of hacking / data breaches, in order to allow users to undertake appropriate measures .

Although, Indian privacy laws do provide for security measures in relation to data, they would need to evolve further to tackle security issues associated with the IoT space.

On the privacy front, the primary compliance that is required with privacy laws of most countries is informed consent. Obtaining an informed consent from the user in this context becomes difficult as many applications are running in the background and processing information autonomously. Consequently, an individual's ability to control the use of his / her personal information could be compromised.

Indian data protection laws have only been recently introduced, and only protect a limited sub-set of personal information under specific circumstances. These laws however, do not always encompass the varied situations surrounding the IoT environment. However, with the constant evolution in technology, it is hoped that laws would accordingly evolve to address such concerns arising from modern electronic computing in this e-world.

2. Data Ownership

As multiple devices connect with each other and communicate in a seamless manner, we see two types of data being used to enable IoT applications – data that is specifically provided by a user, and data that is generated as a result of the use of the application, for example data generated as a result of a user profiling exercise.

In the latter case, where multiple devices and service providers interact to create certain data related to a user's preferences, the question of ownership of such data becomes difficult to answer, especially in a situation where there is no proper contractual relationship between the various parties that touches on this aspect.

One argument that can be made is that the mere fact that two entities let their devices interact with each other and create data could reflect the intention of the parties to create joint ownership.

Typically, under Indian law, the data so created would be protected as copyrighted work. Indian copyright law provides that the author of a work is generally the first owner of the copyright in such work. While it would be difficult to identify the "author" of the data in the above mentioned circumstances, it is also important to note here that with the exception of certain limited circumstances (such as an employer-employee relationship), Indian copyright law does not recognise the concept of 'work-made-for-hire'. In certain instances, a work produced by two or more authors, can also be considered a work of joint ownership where the contribution of the authors is not distinct from one another, Therefore it would be pertinent not only to identify the author(s) and first owner(s) of any data, but also evaluate means to address situations where assignments / licenses would be required to use such data.

With the passage of time it is hoped that there would be jurisprudence which would provide insights on the nuances associated with data ownership in the IoT space.

3. Net Neutrality

Network neutrality is the principle that all internet traffic is treated the same, regardless of its nature or destination. Under this principle no data can be prioritized over another. It means Internet Service Provider's **("ISP")** can't discriminate between different kinds of content i.e. without net neutrality users can be charged more to watch a video clip on Netflix than send a message over Whatsapp.

One of the most critical aspects for the success of IoT is the convergence of different services, networks and applications which are integrated seamlessly. Without Net neutrality, this will be a big challenge, as service providers will have control over what services, applications and devices can use their networks to communicate with others. Also, what needs to be considered is how IoT and its convergence would be affected if there is no Net Neutrality.

Net neutrality has been a bone of contention in the United States between consumer groups, government regulators and ISPs for over a decade. The Federal Communications Commission in the United States recently voted to propose strong 'open internet' rules, which will regulate and prevent ISPs from favouring one content provider over the other. However, it is likely that if enforced, these rules will be brought before the courts in the United States, and it remains to be seen if they will then be upheld.

In India, there are no specific laws that deal with net neutrality. However, the Department of Telecom, Government of India does place an obligation on all telecom operators to provide telecom services in a non-discriminatory manner unless the government directs otherwise.

Recently, Bharti Airtel, one of the biggest mobile service providers in India, introduced a differential pricing model based on the type of mobile internet usage i.e. internet browsing versus voice over internet protocol (VoIP) based usage. This move was widely reported in the Indian media, and became a controversial topic among net neutrality activists in India. As a result, the telecom regulator indicated that a process would be initiated to define the concept of 'network neutrality' in India, and provide adequate regulations. The telecom regulator issued a consultation paper on net neutrality and over the top services[1], receiving an overwhelming response from the public, largely as a result of a public campaign mounted by activists, and backed by a number of popular local businesses in India.

Over the past couple of months, representatives of the Indian government have made various statements indicating that the government supports a freely accessible internet, and will maintain net neutrality[2]. A formal report form the telecom regulator is expected soon, and it remains to be seen how the debate on net neutrality will move forward, and how IoT will be affected by its outcome, especially from an Indian perspective.

4. Formation & Validity of e-contracts

Data ownership, security and privacy issues plaguing IoT can be adequately addressed to an extent by way of contracts between the device manufactures and the users and in many scenarios the contracts will be entered between the users and the manufacturers by way of e-contracts such as click wrap / shrink-wrap contracts.

In case of a shrink-wrap agreement the contracting party can read the terms and conditions only after opening the box within which the product (commonly a license) is packed.

In some jurisdictions, certain types of contract may be required to be physically signed. Further, many jurisdictions also have developed jurisprudence on whether standard form contracts, where one party has a dominant position over the other, would be considered 'unconscionable'. Additional requirements under contract laws of various jurisdictions, such as the requirement for privity of contract, or lawful consideration under Indian law would also need to be examined on a case to case basis.

The Indian Contract Act, 1872, the principle Indian legislation which governs contractual relationships in India, prescribes certain requirements for the formation of contracts as follows:

- *Valid offer and acceptance of the terms of the contract*
- *Presence of adequate consideration*
- *Purpose of the document being legal*
- *The parties should be competent to contract, and*
- *The contract should not have been induced by fraud and/or coercion.*

E-contracts are generally considered valid under Indian law, provided they fulfil the above requisites.

However, it is important to note that certain legislations in India do prescribe additional requirements for the formation of contracts – for example, Indian copyright law requires that any assignment of a copyright must be in writing and signed by the assignor.

In the world of IoT, there is typically very little or no scope for negotiations to be held between the device manufacturer and the users regarding the terms of e-contracts. Also, in most cases there is no privity of contract between multiple device manufacturers, hence what continues to remain a challenge is what terms would govern the inter–relations between the multiple device manufacturers who e-compute with each other while providing services to the user.

Thus, it becomes important to examine the validity of e-contracts, from the perspective of the form /substance along with its enforceability.

5. Product Liability and Consumer Protection

Manufacturers, distributors, suppliers, retailers – anyone who make products available to the public can be held responsible for any breach of warranties in relation to such products, and injuries those products cause whether to an individual itself, or to their property.

In the context of IoT, if a device fails or malfunctions, if devices fail to notify users in accordance with user settings, or if data or software is compromised or lost, the device manufacturers / service providers could face far reaching consequences. For example, in a situation where a wearable medical device fails or malfunctions, there could be instances where medical treatments are omitted, or wrong dosages of medicines are administered. The device manufacturer may be held responsible for bodily injury, or financial harm. Where home automation devices malfunction, the result could be liability for property damage.

In most common law jurisdictions, product liability is based on traditional principles of negligence or absolute liability or strict liability under tort law. A court in a product liability claim involving an IoT device will use these principles to determine liability of the manufacturer of the device.

In India, the Consumer Protection Act, 1986, is the primary law under which product liability and consumer claims may be brought – among other things, this legislation provides for special tribunals, and a redressal mechanism for complaints in relation to unfair trade practices and defective goods / services.

Industry players, especially device manufacturers could consider purchasing product liability insurance to cover any such instances. Also, insurance companies could offer tailor made product liability insurance to IoT device manufacturers, as in some scenarios traditional product liability insurance might not completely protect the IoT device manufacturers.

Considering the above and the number of players in the IoT field, it will be interesting to see how liability is divided and potential consumer disputes are resolved in this space.

Conclusion

With the constantly evolving use of the internet, a question which springs up is whether we need a new law at the state / national level or whether there is a requirement for an international legislation to address risks arising from an IoT environment.

Given the truly global state of the internet, the lines between national territories get more blurry by the day, making it difficult for state legislations to identify and enforce their laws.

With surveillance and interception programs undertaken by various countries providing an

additional stimulus to the growth in this debate, we now see an increasing demand for nations to work with each other, to ensure protection of privacy rights along with addressing security concerns.

With the passage of time we are bound to see legislative activity from the more technologically advanced nations, providing guiding principles for those trying to implement adequate legal mechanisms to deal with this field, leading to increased jurisprudence, both at an international and a national level.

[1] http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/ **(Last visited on June 25, 2015)**

[2]Article 23, Draft General Data Protection Regulation available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf **(last visited June 25, 2015)**

[3] http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm **(last visited June 25, 2015)**

[4] Rachel Ramsey, *What the Net Neutrality Ruling Means for The Internet of Things* available at *http://www.machinetomachinetechnologyworld.com/articles/366860-what-net-neutrality-ruling-means-the-internet-things.htm* **(last visited June 25, 2015)**

1] Consultation Paper No: 2/2015, available at http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/OTT-CP-27032015.pdf

[2] http://indianexpress.com/article/technology/social/govt-supports-non-discriminatory-access-to-internet-telecom-minister/