Internet of Things: Legal and Regulatory Challenges

Mani K. Madala

***Abstract*—**This paper discusses as to what is IoT, advantages of the same for human kind, identifies the risks and concerns connected with IoT, discusses the need for legislation and regulation and recommends suitable approaches for the same. Finally recommends the setting up of World IoT Organisation (WIoTO) on the same footing as World Trade Organisation to get the various jurisdictions to sign plurilateral treaties to obtain harmonization of legislations.

***Keywords*—** IoT, Risks, legislation , World Internet of Things Organization.

I. Introduction

THE "Internet of Things" (IoT) is a phrase that refers to every day products that are connected to the internet that can send and/ or receive communications from other devices. IoT is a network of Physical objects or things embedded with electronics software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing internet infra-structure.It includes internet enabled products such as thermostats, fitness trackers, watches, cars light bulbs, washers and dryers and even tooth brushes. Beyond direct consumer applications many traditional businesses are seeking to utilize IoT to improve their operations by capturing huge data and subject the same to Big Data Analytics to gain insights about consumer behavior to obtain competitive advantage-radically different way of doing business thus making IoT a disruptive technology. IoT enables a very broad range of applications- from more efficient agriculture, manufacturing, logistics, counterfeit detection, monitoring of people, stock, vehicles, equipment and infra-structure, to improved health care, retailing, traffic management, product development, hydrocarbon exploration. It also enables new m new business models.

Goldman Sachs commissioned a research report into the IoT, which concluded that the IoT wave of computing would be larger than the previous two computing waves; the fixed Internet wave and the mobile wave. The report posits that the IoT will lead to the creation of new technology winners and losers, which will be based on the ability of companies to adapt to an increasingly integrated and interconnected world. The direction of technology adoption and development will be tilted by the S-E-N-S-E framework proposed by the report; sensing, efficient, networked, specialized, and everywhere. (Goldman Sachs, 2014)

Cisco estimates that some 50 billion by 2020. IDC the analyst firm makes an even bolder prediction: 212 billion connected devices by 2020. According to CISCO estimates this massive increase in connectedness will drive a wave of innovation and could generate up to 19 trillion dollars in savings over the next decade.

II. Advantages of IoT

IoT can enrich our lives. These miniaturized electronics, computers or robots transform into data gathering objects. These devices interact with their environment and report information on whatever it is programmed for on a real time basis and thereby enhance operational optimization and efficiencies. Consumers share the benefits by employing such reporting and analytic intelligence. For instance waiting for repairs on white goods might become a thing of the past thanks to remote diagnostics and programming while meter reading could not only be carried out from afar but also be used to help home owners to avoid over spending on utilities.

Product developers could easily assess the ways in which people a actually use the things and implement this information to get rid of useless information in favor of more useful ones. IoT can be great boon in the care and health care of elderly living alone. Doctors could see at a glance if their medical tests are a cause for concern and can remotely check their medicine consumption to see if they are taking their medicines correctly in right doses. The IoT is expected to have an economic impact of $3.9 trillion to $11.1 trillion per year by 2025 which will represent up to 11 percent of world's economy. The largest manufacturer have already jumped on to the bandwagon of IoT. But there are many hiccups on the way to realize the full potential of IoT.

III. IoT : Risks and Concerns

IoT suffers from various vulnerabilities. The IOT creates a greater attack surface by forming more access points to the internet that need to be securely monitored. The greater the attack surface the more vulnerabilities that exist which can be exploited. These new threats were identified by Europol in 2014: "With more objects being connected to the internet the

Mani K. Madala is professor with National Institute for Training in Industrial Engineering, Vihar Lake Road, Mumbai

creation of new types of critical infra-structure we can expect to see more targeted attacks on existing and emerging infra structures including new for4ms of blackmailing and extortion schemes. IoT is subject to many threats like data theft, physical injury and possible death" (Europol,2014)

The vulnerabilities could be of various kinds:

• Loss of privacy and data protection: The difficulties of complying with the principles of privacy and data protection, such as informed consent and data minimization, are likely to grow considerably. The EU Commission has stated in its Report that "It can reasonably be forecast, that if IoT is not designed from the start to meet suitable detailed requirements that underpin the right of deletion, right to be forgotten, data portability, privacy and data protection principles, then we will face the problem of misuse of IoT systems and consumer detriment."

• Autonomous communication: One of the most significant IoT-related data privacy risks stems from the fact that devices are able, and intended, to communicate with each other and transfer data autonomously. With applications operating in the background, individuals may not be aware of any processing taking place, and the ability for data subjects to exercise their data privacy/protection rights may therefore be substantially impaired.

• Traceability and unlawful profiling: Incredibly accurate estimates of race, age, IQ, sexuality, personality, substance use and political views could be inferred from automated analysis of their Facebook "Likes" alone. Similarly, although the objects within the IoT might individually collect seemingly innocuous fragments of data, when that data is collated and analyzed, it could potentially expose far more than intended by the individual to whom it relates, and indeed more than those Facebook Likes. The data collected, in combination with data from other sources, may reveal information on individuals' habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling. This in turn increases the risk of authentication issues, failure of electronic identification and identity theft.

• Malicious attacks: The IoT provides hackers with more vulnerabilities to exploit and creates significant security risks. Such risks could take a variety of forms, depending on the nature of the data and device in question. 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. Take, for example, the remote programming of a heart pacemaker, or a drug dispenser configured to administer medication in response to a patient's condition. A system failure or more sinister malicious attack on such device could have dire consequences. In the context of energy, hackers could target smart meters to cause major blackouts, and in the context of home security, it takes little imagination to contemplate the potential effects of a system failure or malicious attack. Such threats to security and privacy vary considerably and the breadth of challenges presented means that a onesize-fits-all approach to policy and/or regulation is unlikely to work.

Denial of Service attacks on the IoT can bring down the systems with disastrous results. Zorzi et al (Zorzi,2010)found that physical jamming of communications channels could also be used to launch DoS attacks Using large amounts of packets to flood the network can also disrupt the network availability. Resource exhaustion attacks does not call for a lot of intelligence.

Routing attacks can occur where data relay and forwarding exist in the perceptual data collection process, it can be arranged that the intermediate nodes may attack the data during the forwarding. Eavesdropping to steal the information can also be another threat. Data Control must be considered but must not be confused with data ownership (Tan and Wang,2010)

Attackers can also adopt a guerilla strategy to take control of small portions of the network but affecting the entire system. Sensors can be stolen destroyed, disabled and the entire sensor network can be brought down.

Physical attacks are also possible when an attacker could enter a house where the sensor is kept and detect where the electronic signals are coming from through the detection equipment and based on the properties of the received signals- they can manage to steal disable or destroy the IoT. Attackers who know the default pass words of the devices can exploit the back doors and change critical settings or replace the firmware altogether. Depending on the devices these actions can cause serious illnesses, injuries or even death.

• Repurposing of data: The risk that data may be used for purposes in addition to or other than those originally contemplated and specified by the data subject becomes even greater in the IoT. Repurposing of data may be contemplated even before data collection begins. For example, regulatory bodies, insurance companies and advertising agencies, among others, may seek access to data collected by others. Controls are needed to ensure that such data is only used in the manner consented to by the data subject. Whilst an individual Client Alert might be happy for his fridge to know how many pizzas he eats each week, he might be less comfortable if he knew that that information was being passed on to his health insurance provider.

• User lock-in: As is the case for existing technologies, the IoT increases the risk that consumers may become locked-in to a specific IoT service provider, thereby impeding their ability to retain control over their data and their right to move from one provider to another.

• Applicable law: With IoT devices, systems, users and service providers located in any number of jurisdictions, the global nature of the IoT means that various national laws may be applicable, each providing different levels of protection. This may give rise to questions of conflict, difficulties in enforcement and confusion among consumer Standards and Inter-operability

The great heterogeneity in Application Programming Interfaces and middleware (software components) makes it difficult to write applications that will run on different

systems – therefore users often have to rely on a single set of applications for a single set of IoT components. More standardization would enable more innovation, and enable information to flow between industry verticals like consumer electronics and the automotive industry. There is a need for interoperability, connectivity, access control, service discovery, and privacy services, built on IoT- optimized protocols where necessary. Governments should facilitate the industry to evolve standards.

Adequacy of Unique identifiers: In terms of unique identifiers our previous IP address system Ipv4 can generate approx. 4.2 billion IP addresses, deficient in what's required for upcoming device demands. The next generation IP address system IPv6 by combining Ipv4 with each devices unique physical address can generate 340 trillion trillion trillion addresses. According to Google Ipv6 adoption rate among Google users reached 8.24 per cent as Dec 11, 2015. Legislation is required to move all manufacturers to IPv6 IP address system.

Concerns for the development of IoT include: costs need to fall, reliability needs to improve, Issues of connectivity, user interfaces and addressing. For IoT to become a truly ubiquitous technology, the cost of tags, sensors and communications systems needs to fall to a level where they are a very small fraction of the total cost of the objects they are attached to. The governments should endeavor through legislation and regulation to help the industry to accomplish this.

IoT security also requires penal legislation. Companies which have lax security practices and which mislead the consumers need to be penalized. In USA a hacker exploited a flaw in the software of TRENDnet security cameras and posted live feeds of approx. 700 consumer a cameras. The authorities fixed the responsibility on the manufacturer and levied penalties.

Access control systems, strong authentication measures, security safe guards should be built into the devices. Active firewalls, anti-virus, anti spyware software intrusion detection systems and intrusion prevention systems are needed to protect IoT devices.

IV. Legislation and Regulation for IoT

Legislation and regulation needs to look at the potential issues for each category of stakeholders: The potential issues for industry and service providers could be business model interoperability,, standards, numbering plan issues spectrum allocation policy. For content providers and controllers the issue could be net neutrality. For government and law enforcement the issue could be cyber security and mandatory data retention. The issues for community could be digital divide, discrimination, privacy risk, and consumer law and product liability among many others.

Is the existing legislation adequate to handle the vulnerabilities or new legislation required? Which kind of new laws are required and what should be their time frame? These legal challenges should be embedded into the constitution of every jurisdiction. In 2008 the German Supreme Court constituted an independent fundamental right of confidentiality and integrity related to info – technical systems and every jurisdiction has a lesson in this. Privacy is recognized as a fundamental human right in the 1948 Universal Declaration of Human Rights and is anchored in the constitutional law of most countries today. The first major piece of legislation on information privacy was passed with the 1974 US Privacy Act, which established the fair information practices (FIPs). The FIPs comprise the principles of notice, consent, individual access and control, data minimization, purposeful use, adequate security and accountability. They have been taken up in by the Organization for Economic Co-operation and Development (OECD), which anticipated trade barriers from the increasingly diverse national privacy legislation.

Objectives to be attained Based on the vulnerabilities discussed here

The main objectives should be -effective personal data protection which entails the application of the legal principles, as well as effective information security (confidentiality, integrity, availability) of services, with a view to provide better IoT services for the citizens. Another interesting element is the issue of universality of personal data protection which is going to be very relevant in an IoT environment. Apart from the obvious legal problems, the issue of scope of users' choices and data portability also needs to be considered. Due to the international / global nature of the Internet of Things it is important, to increase the level of harmonization of data protection legislation and to ensure a high level of enforcement. It can reasonably be forecast, that if IoT is not designed from the start to meet suitable detailed requirements that underpin 〉 the right of deletion 〉 the right to be forgotten 〉 data portability 〉 privacy and 〉 data protection principles then we will face the problem of misuse of IoT systems and consumer detriment. To achieve these goals various kinds of legislation need to be worked on such as: Right-to-know-legislation; Prohibition-legislation; IT-security-legislation; Utilization-legislation; Task-force-legislation.

The right-to-know-legislation has the purpose to keep the customer informed about which data are collected and should also have the possibility to deacti- vate the tags after a purchase.The prohibition-legislation introduces provisions

Both for the service providers as well as common men as what is allowed and what is not allowed.

IT-security-legislation encompasses initiatives that demand the establishment of certain IT-security standards which should protect that application of IoT.The Utilization-legislation intends to support the use of IoT.And lastly the task-force-legislation covers legal provisions supporting the technical community to invest into the research of the legal challenges of IoT

Net neutrality which means- 1.No blocking – ISPs must not block access to legal content, applications, services or non-harmful devices. 2. No throttling – ISPs must not impair or degrade lawful internet traffic on the basis of content, applications, services or non-harmful devices. 3. No paid

prioritisation – ISPs must not favour some lawful internet traffic over other lawful traffic in exchange for consideration of any kind (including from their affiliates) can be achieved with penal legislation.

IoT challenges centre around globality – across all jurisdictions- IoT is supposed to be universal, verticality- across the life cycle of Iot product including wste management, ubiquity across the human, plant animal kingdoms and technicity- technical community best knows that technical challenges and how to provide solutions for the same.Legislation in one jusrisdiction for one sector is not going to solve the problem.

It is not unrealistic to expect that there will be different IoT regulations in different jurisdictions just as happened with cloud, data privacy and other technologies. With IoT devices systems users and service providers located in many jurisdictions the global nature of IoT means that various national laws may be applicable each providing different levels of protection. This may give rise to questions of conflict, difficulties in enforcement and confusion among consumers.

The specific problem in view of security and privacy consists in the appreciation that privacy concerns are not identical in the different regions of the world which makes the application of general principles difficult in cross border business activities.

Therefore a basic legal framework should be introduced by an international legislator. A new body would be in a position to take into account all the characteristics of IoT. It should have the necessary capacity as well as the expertise.

An international organization -let's call it - World Internet Organization should be created and put on the same footing as World trade Organization. Plurilateral treaties need to be signed by the countries for cooperation and collaboration on all issues connected with IoT.There is need for harmonization of legislation.

REFERENCES

[1] Europol,THE INTERNET ORGANISED CRIME THREAT ASSESSMENT (iOCTA), European Cybercrime Centre 2014 https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf

[2] Goldman Sachs. The Internet of Things: Making sense of the next mega-trend. 2014, Available http://www.goldmansachs.com/our-thinking/outlook/Internet-of-things/iot-report.pdf.

[3] L. Tan and N. Wang, Future Internet: The Internet of Things. Advanced Computer Theory and Engineering (ICACTE), 5(1), 376-380, 2010

[4] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, From today's INTRAnet of things to a future Internet of things: A wireless- and mobility-related view. Ieee Wireless Communications, 17(6), 44-51, 2010. http://dx.doi.org/10.1109/MWC.2010.5675777

Mani K. Madala (M'76–SM'81–F'87) and the other authors may include biographies at the end of regular papers. Biographies are often not included in conference-related papers. This author became a Member (M) of **IEEE** in 1976, a Senior Member (SM) in 1981, and a Fellow (F) in 1987. The first paragraph may contain a place and/or date of birth (list place, then date). Next, the author's educational background is listed. The degrees should be listed with type of degree in what field, which institution, city, state or country, and year degree was earned. The author's major field of study should be lower-cased.

The second paragraph uses the pronoun of the person (he or she) and not the author's last name. It lists military and work experience, including summer and fellowship jobs. Job titles are capitalized. The current job must have a location; previous positions may be listed without one. Information concerning previous publications may be included. Try not to list more than three books or published articles. The format for listing publishers of a book within the biography is: title of book (city, state: publisher name, year) similar to a reference. Current and previous research interests ends the paragraph.

The third paragraph begins with the author's title and last name (e.g., Dr. Smith, Prof. Jones, Mr. Kajor, Ms. Hunter). List any memberships in professional societies other than the **IEEE**. Finally, list any awards and work for **IEEE** committees and publications. If a photograph is provided, the biography will be indented around it. The photograph is placed at the top left of the biography. Personal hobbies will be deleted from the biographyy.