COUNTERBALANCING THE INTERESTS OF INNOVATION AND CONSUMERS' DATA: SETTING THE REGULATORY STANDARDS FOR IOT STAKEHOLDERS

[*] *Aryan Babele and Abhijeet Vaishnav*

ABSTRACT

The advent of technologies as everyday utilities, more commonly referred to as smart objects, connected over an online network, are the Internet of Things (IoT). The dependency on IoT applications have increased manifold rapidly due to them facilitating ease into the lives of humans. IoT industry has the great potential in tremendously bringing value creation as well as innovation in a variety of sectors, ranging from human interaction to healthcare sector, and from transportation to the way of banking. However, the popularity of these applications may also transmit risks of potential disruptions to the existing state of the market, ranging from consumers' data protection issues to targeted broad-scale shutdown of systems, Therefore, the wide usage of IoT like devices and services calls for a new set of IoT specific regulatory standards on data protection and cyber-security. Since the regulations and technological advancements often become adversaries, there arises a need to have a regulatory framework which should be technology-friendly to maintain the right balance between technological

[*] Aryan Babele is Research Fellow (Fintech) at Vidhi Centre for Legal Policy. Abhijeet Vaishnav is a 5th Year B.A. LL.B. (Hons.) student at Rajiv Gandhi National University of Law, Punjab.

innovation, commercial consumption and consumer protection in respect of IoT. This paper deals with the understanding of IoT in light of protection of data related to consumers. Further, the paper examines various data protection concerns associated with proliferation of IoT such as manipulation of consumers' data, non-transparency in data-transfers, unethical data collection and dissemination, information security, consent-tracking models, among others. The paper also studies the need of regulatory framework in the national vis-a-vis international scenario in respect of IoT. The paper seeks to bring forth suggestions to balance the interests of the consumers as well as the IoT industry.

1. INTRODUCTION

The Internet of Things ("**IoT**") marks a major transformation in the evolution of Internet. It has not only expanded the scope of facilitating interaction between humans through machine-to-machine communications, but has also facilitated collection of data and sending of instructions, to or from, everyday objects that interface with, or form part, of the world. As IoT's functions have begun to extend to collection and processing of real-time data as well, it would not be wrong to derive a new notion that the 'society is majorly based on information and ideas more than the physical things.' In the digitalized era, with machine-to-machine interaction, IoT helps in bridging gaps not only between different technologies themselves

but also between technology and people, connecting them all to the platform of the Internet.

In simpler terms, IoT refers to all those everyday physical 'utilities' or 'things' that have the capability to interact with the environment, people and other devices in real time. When a 'thing' is connected to the Internet, it has the capability to send and/or receive information. Such processing capabilities make 'things' smarter, without a need for inherent super storage. IoT involves a network that connects various technologies over the same, for them, to interact and share their data. For instance, a smartphone user can listen to any song on demand over the music streaming apps. This is not because one has every song stored in that phone, but is due to the smart phone's capability to connect to the Internet to send information (asking for the music) and receive information (streaming the music) from the cloud storage that is stored somewhere else in the world.

IoT is increasingly penetrating into our everyday lives. It is growing at such a rapid rate that the experts have calculated that the number of Internet connected devices in the world might reach 43 billion by 2023[1]. In the US itself, the

[1] Fredrik Dahlqvist, Mark Patel, Alexander Rajko, & Jonathan Shulman, *Growing opportunities in the Internet of Things*, McKinsey & Company, (Sep. 01, 2021), https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things.

number of connected devices per person has doubled to 25 in 2021 from 11 in 2019, according to a report by Deloitte.[2] As the society is becoming more informed and aware of these technologies and IoT, there arises an urgent need for people to be self-aware as well. In an increasingly IoT dependable society, flip side of such technology should also be recognized. Being one of the most disruptive technologies of our time, IoT has globally emerged as an Internet-based infrastructure. It, in an absolute manner, integrates multiple numbers of connections such that numerous devices get engaged in processing, collecting and sharing the data, for specific tasks. Such advancement could also translate into the drastic improvements and unprecedented growth in diverse markets like the healthcare, energy, transportation, and logistics.[3]

This paper seeks to analyse how ubiquitous IoT is in various sectors, highlighting its advancement in those sectors. On the other hand, it also highlights upon incidents that have innately shaken the consumer

[2] 2021 Connectivity and Mobile Trends Survey, Deloitte, (Sep. 1,2021), https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html.

[3] Sanford Reback & Tony Costello, *Deconstructing the Internet of Things,* Bloomberg Government, (Sep. 1,2021), https://www.multivu.com/players/English/7371431-bloomberg-visa-the-digital-trust securingcommerce/flexSwf/impAsset/document/166030bd-bc8d-40ed-97c2-5f60a0270bbd.pdf.

protection related regulatory structure and increased concerns of data protection. The IoT industry has for long thrived largely upon the non-personal data, which is now being called for regulation by concerned policymakers. Against this backdrop, the paper ultimately attempts to put forth points for the need of regulations to control the expansive IoT applications and balance the outlook of the consumers' data interests as well as that of IoT manufacturers/ service providers. The recommendations presented in the paper are the broad based principles as well as the best practices that may be considered for implementation by the regulators, as well as the IoT industry stakeholders for self-regulation.

2. UNDERSTANDING 'INTERNET OF THINGS' ("IOT")

The term 'IoT' when used in 1999 by Kevin Ashton, was originally used to indicate those technological objects that embody tiny wireless chips that could be sensed so that each 'thing' could be tracked in space and time via the Internet.[4] Mostly, it has been described as the 'world of interconnected, sensor-laden devices and objects.'[5]

[4] Sidney Perkovitz, *The Internet of Things: Totally New and A Hundred Years Old*, Jstor Daily, (Sep. 1,2021), https://daily.jstor.org/internet-things-totally-new-hundred-years-old/.

[5] FTC Staff Report, Internet of Things: Privacy & Security in a Connected World, FTC 1 (2015) https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/ 150127iotrpt.pdf [*hereinafter* FTC IoT Report].

Despite an increasing dependency on the IoT, there is yet to be evolved a single, uniform and universally accepted definition. The consultancy-firm, McKinsey, provides a broad definition of IoT, which includes 'sensors and actuators' in physical objects that are connected to each other through Internet networks (wired or wireless), in return, which produces big volume of data for computers to analyze.[6] Another attempt was made under the EU's project on Coordination and Support Action for Global RFID-related Activities and Standardization ("**CASAGRAS**"), which defined IoT to be

> *'a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.* [7]

[6] Michael Chui, Markus Löffler, & Roger Roberts, *The Internet of Things*, McKinsey, (Sep. 1,2021), http://www.mckinsey.com/industries/high-tech/our-insights/the-intemet-of-things.

[7] *Final Report: RFID and the Inclusive Model for the Internet of Things; EU Project (216803)*, European Commission: London, UK, (Sep. 4, 2021), https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/low%20resolut

India's Ministry of Electronics and Information Technology ("**MeitY**") attempted to define IoT as,

> "*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.' - Phones, Tablets and PCs are not included as part of IoT.*"[8]

As per this definition, IoT devices include all those technologies which can interact with each other with minimal human intervention. It attempts to identify IoT as all those devices which practice machine-to-machine ("**M2M**") interaction and are interoperable. Phones, tablets, and personal computers ("**PCs**") are excluded from the definition of IoT, which brings out a major fallacy in the definition of failure to recognize M2M communication of these three 'things' with other smart things. For instance, communication between the smartphone with other smart devices like the printer, air-conditioner, etc. However, a plausible argument for such classification maybe due to these things not fulfilling the

ion/www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf.

[8] *IoT Policy Document*, Ministry of Electronics and Information Technology, (Sep. 1,2021), http://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

one of the prescribed parameters to be identified as IoT. All the three gadgets mentioned require the human involvement in various steps to facilitate interaction between humans and them and their interaction with other smart things.

To further elucidate and for purposes of this paper, IoT, essentially, can be explained as a 3-step process. First- ability of the sensors to detect and capture data from the real-time environment, just like a human being. Second- continuous data transmission through Internet-network connected to a cloud-storage application for data storage. Third- analysis of the data, which further helps in expediting the organisational processes, enabling the customisation of products and services, automatically decreasing unused information and increasing efficiency with safety and security.[9]

> *'IoT deployments will generate large quantities of data that need to be processed and analysed in real time… Processing large quantities of IoT data in real time will increase as a proportion of workloads of data centres, leaving providers facing new security, capacity and analytics challenges.'*[10]

[9] *Internet of Things*, *Patent Landscape Analysis*, WIPO, (Sep. 1,2021), http://www.wipo.intlexport/sites/www/patentscope/en/programs/patentlandscapes/documents/internetofthings.pdf.

[10] *Gartner says the Internet of Things will transform the Data Center,* Gartner, (Sep. 1,2021), http://www.gartner.com/newsroom/id/2684616.

Thus, it is imperative to note the underlying essence of all the attempted definitions, some which have been discussed, that IoT thrives on data. In the digital age where technology is changing facets of industries, human interaction as well as its own foundation on a daily basis, a universally accepted definition of IoT may take time to come along and be seamlessly accepted. While a universal definition of IoT continues to be worked upon, one of its essential functions of data collection and/ or ability of processing the same remain undisputed. This level of data collection and ability of IoT to manipulate the same for advancement of human-kind and technology is what makes such technologies disruptive as well. This calls for regulations and a system of checks and balances to be introduced for IoT to continue to yield common good and prevent them from turning pervasive, intrusive or destructive.

3. AN OVERVIEW OF THE MARKET OF IOT APPLICATIONS AND SOLUTIONS

As has been widely recognized, IoT has well penetrated into various aspects of our lives; impacting industries as well. It is estimated that IoT's vast expanse in key industrial sectors may even lead to increase in efficiency by 15-40%

in developed nations.[11] Increasing usage of IoT has provided humans with unimagined richness in their interaction processes and contribution to the lives medically, socially and technologically. IoT's vast expanse in various industries has encouraged Indian Government to plan for 100 smart cities with key features of smart urban lighting, transport system, smart parking, amongst other smart initiatives.[12] In December 2019, the Ministry of Electronics and Information Technology approved over INR 4 billion for the implementation of 'FutureSkills Prime', a program aimed at 'up-skilling ecosystem for B2C in emerging and futuristic technologies', including IoT.[13] In the recent times, its usage has increased so much so that it may be equated to be as a backbone of almost all industrial sectors, some of which are discussed below.

Automotive and transport industry is seen to be realising the potential of IoT in their domain with real-time monitoring and accurate information of critical data in the operations of public transportation, traffic and public

[11] *Australia's IoT Opportunity: Driving Future Growth- An ACS Report*, Australian Computer Society, (Sep. 1,2021), https://www.acs.org.au/content/dam/acs/acs-publications/ACS-PwC-IoT-report-web.pdf.

[12] Supra 8.

[13] 16th Law Commission of India Report, *Action Taken by the Government on the Observations/Recommendations of the Committee contained in their Fourth Report (Seventeenth Lok Sabha) on 'Demands for Grants (2019-20)*, (Sep. 1,2021), http://164.100.47.193/lsscommittee/Information%20Technology/17_Information_Technology_16.pdf.

bikes. With increased usage of telematics hardware and software in vehicles, spending on IoT in automobile sector globally was around USD 32 billion in 2020, and expected to reach USD 100 billion by 2026, at a Compound Annual Growth Rate ("**CAGR**") of 21.12%.[14]

Global Positioning System ("**GPS**") is an IoT device that has become an essential technological solution for many problems in the transportation industry. IoT not only caters to the ground level of transportation but also to waterways and airways. Few examples of successful IoT implementation in transport industry are GoDirect's Fuel Efficiency software, Rolls Royce autonomous freight shipping, Honeywell's IoT connected aircrafts, etc.[15] All the automated processes such as fleet management, public transit management, smart inventory management, geo-fencing, etc. requires continuous capture and analysis of mission-critical data.

[14] These data points claimed to be used by companies including KPMG, Deloitte, Accenture and more. *Automotive IoT Market Research Report by Component, by Connectivity, by Communication, by Application, by Region - Global Forecast to 2026 - Cumulative Impact of COVID-19*, ReportLinker, (Sep. 1,2021), https://www.reportlinker.com/p06081367/Automotive-IoT-Market-Research-Report-by-Component-by-Connectivity-by-Communication-by-Application-by-Region-Global-Forecast-to-Cumulative-Impact-of-COVID-19.html?utm_source=GNW.

[15] Vivian Zhang, *Why the transportations sector needs data scientists,* VentureBeat, (Sep. 1,2021), https://venturebeat.com/2018/04/20/why-the-transportation-sector-needs-data-scientists/.

Application of IoT has led to lesser risks and reduced costs of transportation, real-time communication of the roadside messages like the toll rates, lane closures, speed limits, ability of the vehicle to communicate to its environment, surveillance, etc. Advent of technologies connected via Internet has led to the development of various automated vehicles. These can be put to use by accessing them through the virtual network rather than being present with/in them in the real-time world. Examples of evolution of the smart transport can be found in the automated cars; Audi's launch of Vehicle-to-Infrastructure technologically equipped car[16] (the car is equipped to communicate with traffic light information in select cities), as a step to smarter and safer cities, etc.

Some of the advancements made in India under smart transport industry include the anti-lock braking system and electronic stability program, which is estimated to save 10,000 lives in India from car accidents.[17] With such rapid penetration of IoT in the transport and automotive sector,

---

[16] *Audi launches first Vehicle-to-Infrastructure (V2I) technology in the U.S. starting in Las Vegas*, Audi Newsroom, (Sep. 1,2021), https://media.audiusa.com/en-us/releases/92#:~:text=Press%20releases-,Audi%20launches%20first%20Vehicle-to-Infrastructure%20(V2I)%20technology,U.S.%20starting%20in%20Las%20Vegas&text=Las%20Vegas%20continues%20its%20leadership,traffic%20signal%20network%20to%20vehicles.

[17] *Smart Transportation - transforming Indian cities*, Grant Thorton, (Sep. 1,2021), https://www.grantthornton.in/globalassets/1.-member-firms/india/assets/pdfs/smart-transportation-report.pdf.

the industry may soon introduce technology that is able to communicate vehicle-to-vehicle, and contribute towards smart road transportation. Such transformation of hardware-oriented industry to software-oriented industry has opened arenas for the transport and automotive industry to explore and contribute in boosting IoT in the future.

In **Healthcare**, it has been estimated that by 2020, 40% of IoT-related technology will be health-related, more than any other category, making up a USD 117 billion IoT market in healthcare.[18] As per Grand View Research, IoT market in healthcare, by 2025, is expected to reach USD 534.3 billion (CAGR 19.9%).[19] Induction of wearable biosensors and wireless communication technologies (fitness tracking devices, wellness bands, etc.) have facilitated healthcare significantly around the world during the ongoing Covid-19 pandemic situation. The combination of personal health technologies and the IoT suggests the rise of powerful Internet of Medical Things ("**IoMT**") that features expanded abilities to exchange useful data, improvements in context awareness, and the

[18] Harald Bauer, Mark Patel, & Jan Veira, *The Internet of Things: sizing up the opportunity,* McKinsey & Company, (Sep. 1,2021), http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity.

[19] *IoT in Healthcare Market Worth $534.3 Billion By 2025 | CAGR: 19.9%,* Grand View Research, (Sep. 1,2021), https://www.grandviewresearch.com/press-release/global-iot-in-healthcare-market.

ability to initiate actions based on data that are collected and analysed.[20] Health-related IoT applications allow researchers to collect rich and accurate data to an extent which was not possible in conventional physician-patient interactions.

Another stepping stone with convergence of technology and medicine is the evolution of certain applications which help in personalised healthcare of the patients and easier communication between the patients and doctors. In India, this comes with the recognition of 'telemedicine' by government in the face of social distancing measures during Covid-19 situation.[21] Also, IoT is being increasingly employed for medical surveillance. While increasing number of medical devices are introduced in the market which are digitally enabled and connected, regulations too need to be imposed to keep such technology from becoming disruptive. In lieu of this, the US Food and Drug Administration, in 2013, released a system of unique

[20] Nichola P Terry, *Will the Internet of Things Transform Healthcare?,* 19 VJE & TL 329 (2016), https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1121&context=jetlaw.

[21] Telemedicine is defined as "the delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities". *Telemedicine Practice Guidelines*, Ministry of Health and Family Welfare, (Sep. 1,2021), https://www.mohfw.gov.in/pdf/Telemedicine.pdf

identification of the medical devices which the companies can recall in case of an adverse event, to improve patient care.[22]

Some of the examples of IoT's health-related applications are IBM's 'Watson for Oncology', Google's DeepMind Project etc. IoT's inclusion in healthcare witnessed a sudden increase during the COVID-19 pandemic, where 5G thermometers were used to screen patients for fever[23], smart bracelets and rings were worn by patients in China.[24] These bracelets and rings are synced with CloudMind's AI to check temperature, Blood pressure, and oxygen level, at regular intervals.[25] Hospitals have now started to deploy 'smart-beds' which can detect when it is occupied by a patient and send appropriate information to doctors/ nurses in case the patient is trying to get up from the bed.[26] Conventional healthcare sector is disrupted, but the path to transform the model of care through influx of

[22] *FDA finalizes new system to identify medical devices*, US Food & Drug Administration, (Sep. 1,2021), https://wayback.archive-it.org/7993/20170112084527/http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm369276.html.

[23] Tim Hornyak, *What America can learn from China's use of robots and telemedicine to combat the coronavirus* , CNBC, (Sep. 1,2021), https://www.cnbc.com/2020/03/18/how-china-is-using-robots-and-telemedicine-to-combat-the-coronavirus.html.

[24] Charles Arthur & Ruan Shuhui, *In China, robot delivery vehicles deployed to help with COVID-19 emergency*, United Nations Industrial Development Organization, (Sep. 1,2021), https://www.unido.org/stories/china-robot-delivery-vehicles-deployed-help-covid-19-emergency

[25] Ibid.

[26] R. Babu & K Jayashree, *A Survey on the Role of IoT and Cloud in Health Care*, 4 IJST Research 2217 (2015), http://ijsetr.com/uploads/624351IJSETR4609-407.pdf,.

technology is difficult. In India, usage of IoMT and IoT is widely seen in care delivery cases to pre-detect symptoms of breast cancer and treatment options, in delivery of better patient care and in smart ambulances to periodically capture data and vitals automatically.[27]

A revolutionizing step of technology into medicine is introduction of Electronic Health Records ("**EHRs**"). It is a repository of information regarding the health of a subject of care in computer-processable form that is able to be stored and transmitted securely, and is accessible by multiple authorized users.[28] Indian government has introduced standards for EHR in India which can be adopted by healthcare institutions on voluntary basis. An example of how IoT in healthcare will improve facilitation of ease can be explained. While it usually takes two hours on an average for Indian hospitals to decide to which department a patient has to be taken to, IoMT can dramatically improve healthcare.[29] Therefore, with time

[27] *Reimagining the possible in the Indian healthcare ecosystem with emerging technologies*, PWC India, (Sep. 1,2021), pwc.in/industries/healthcare/reimagining-the-possible-in-the-indian-healthcare-ecosystem-with-emerging-technologies.html.

[28] *Electronic Health Record (EHR) Standards for India - 2016*, Ministry of Health and Family Welfare, (Sep. 1,2021), https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf.

[29] Ravi Ramaswamy, *Riding technology: The role of IoT in healthcare surveillance*, The Economic Times (22/07/2017), (Sep. 1,2021), https://economictimes.indiatimes.com/small-biz/security-tech/technology/riding-technology-the-role-of-iot-in-healthcare-surveillance/articleshow/59710658.cms.

and effort reduction, IoMT is helping more in providing preventive mechanisms than the curative.

In **Manufacturing**, the sensors-embedded devices are used to track the status of machinery and monitor the flow of inventory, which implement real-time updates to further reduce downtime; such IoT applications are estimated to achieve gains of USD 53.8 billion by 2025, from around USD 33 billion in 2020.[30] Manufacturers utilising IoT solutions in 2014 saw an average 28.5% increase in revenues between 2013 and 2014, according to a TCS survey.[31] Several leading global manufacturers- including the likes of Bosch, Harley Davidson, GE, and Siemens- are early adopters of smart manufacturing.[32]

However, such expansive deployment of IoT will require more electricity to sustain an IoT environment of data centres and data storages.[33] It is remarkable to note that in

---

[30] *IoT in Manufacturing Market by Component (Solutions (Network Management and Data Management) and Services (Professional and Managed)), Deployment Mode, Organization Size, Application, Vertical (Process and Discrete), and Region - Global Forecast to 2025*, Markets and Markets, (Sep. 1,2021), https://www.marketsandmarkets.com/Market-Reports/iot-manufacturing-market-129197408.html.

[31] John Greenough, *Internet of Things in Manufacturing*, Insider, (Sep. 1,2021), https://www.businessinsider.com/internet-of-things-in-manufacturing-2016-10?IR=T.

[32] Kevin O' Marah & Pierfrancesco Manenti, *The IoT will Make Manufacturing smarter,* Industry Week, (Sep. 1,2021), https://www.industryweek.com/manufacturing-smarter.

[33] Robin Kester*, Demystifying the Internet of Things: Industry Impact, Standardisation Problems, and Legal Considerations*, 8 ELR 205, (2016), https://www.elon.edu/u/law/wp-content/uploads/sites/996/2019/07/V8_No1_Kester.pdf.

the past two decades, India has witnessed an exponential increase in the demand for digital storage, from 1 petabyte in 2001 to more than 34 petabytes which then continuously increased by 25-30% every year.[34] It is the predictions of researchers that data centres of the world will even consume 1/5th of Earth's power by 2025.[35] Due to such statistics, IoT developers are focussing on making IoT a right solution for excessive energy consumption rather than making it a disruptive agent for **Energy sector.** The IoT market with respect to energy sector is predicted to reach USD 35.2 billion by 2025, at a CAGR of 11.8% (2020-2025)[36]**.**

As a greater number of households are getting connected to the 'smart grids' and 'smart meters', better are the consumers adjusting their patterns of energy consumption. With increasing number of IoT devices that are connecting to the households, consumers can monitor their behaviour of consuming energy. An example of this is the Zigbee

[34] Avinash Aslekar & Pramod Damle, *Improving Efficiency of Data Centres in India: A Review,* 8 IJST REV.1, 44-49 (2015), https://indjst.org/articles/improving-efficiency-of-data-centres-in-india-a-review.

[35] Joao Marques Lima, *Data centres of the world will consume 1/5 of Earth's Power by 2025*, BroadGroup, (Sep. 1,2021), https://data-economy.com/data-centres-world-will-consume-1-5-earths-power-2025/.

[36] *Internet of Things (IoT) in Energy Market by Solution (Asset Management, Data Management and Analytics, SCADA, Energy Management), Service, Platform, Application (Oil and Gas, Smart Grid, Coal Mining), and Region - Global Forecast to 2025*, Markets and Markets, (Sep. 1,2021), https://www.marketsandmarkets.com/Market-Reports/iot-energy-market-251659593.html.

technology. This application, which majorly caters to personal area network, can be applied for building and street lighting, smart grids, electric meters, home automation systems, resulting in efficient use of energy for the consumer.[37]

Fintech or Financial Technology includes the market of those companies which use technology to introduce innovative financial services. There always have been identified privacy concerns in the financial sector, thus, it remained content with the traditional ways of business to protect data from looming threat of data leak. However, fintech sector seems to be gaining a footing in the present-day scenario. According to Jim Marous, a fintech expert and publisher of 'The Financial Brand', IoT is set to improve the customer experience and consequently, its relationship with its customers, by increasing agility and response time towards changing market needs.[38] Hence, in future, the financial sector may not accept its position at a lower end of employing IoT and venture more into it.

As IoT penetrates our everyday lives, IoT has not remained at bay from education sector. **Education**, no

---

[37] Erol-Kantarci & Hussein Mouftah, *H.T. Wireless Sensor Networks for Cost-Efficient Residential Energy Management in the Smart Grid*, 2 IEEE Communication Surveys and Tutorials 314–325 (2011), (Sep. 1,2021), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6861946.

[38] *Security and Privacy Concerns Need to be Addressed When it Comes to IoT in the Financial Industry*, Fintech News Singapore, (Sep. 1,2021), http://fintechnews.sg/9235/iot/iot-security-privacy-concerns-need-addressed-comes-iot-financial-industry/.

doubt, plays a rooting role in any society. The rigid education system has become a thing of a past with the introduction of 'fun and creative learning' processes introduced in the school. Such systems not only enable one to learn meaningfully but also apply the creative part of their mind to inculcate abilities of innovation in students. In a developing country like India, where all resources are not equally and readily accessible, IoT in education will lead to uniformity in providing education with resources being outsourced through audio-visual provisions.

IoT is also making the information sharing more accessible in **law enforcement**, providing policing authorities with real-time language interpretation, virtual criminal records etc.[39] IoT has proved its potential in law enforcement with applications such as 'Shot Spotter' (helps detecting perpetrator in shorter span of time by locating gun and firing pattern)[40], electronic driving licenses (introduced in France to reduce counterfeit of licenses)[41], connected fleet

[39] Brian Chidester, 7 ways that IoT is transforming law enforcement, (Sep. 4,2021), https://blogs.opentext.com/7-ways-that-iot-is-transforming-law-enforcement/.

[40] *About ShotSpotter*, Shot Spotter, (Sep. 1,2021), https://www.shotspotter.com/company/; Elizabeth MacBride, *The Scientist, The Investor And The CEO: How 'Shots Fired!' Technology Turned A Profit*, Forbes, (Sep. 1,2021), https://www.forbes.com/sites/elizabethmacbride/2018/10/30/the-scientist-the-investor-and-the-ceo-how-shotspotter-turned-a-profit-after-22-years/#197a3cc9468c.

[41] *The new French electronic driving license*, Thales, (Sep. 1,2021), https://www.thalesgroup.com/sites/default/files/gemalto/gov-new-driving-license.pdf.

systems (including license plate readers, dashcams, gun sensors to enhance connectivity and coordination among the fleet and speed tracking, location and fuel consumption monitoring for patrol cars)[42], etc. Again, the challenge remains the same, notwithstanding the separate vulnerable points of cyber security, that is understanding the use of cloud analytics to make collection and analysis of the data an effective and secure mechanism.

4. PROFOUND DATA PROTECTION RELATED CONCERNS FOR CONSUMERS USING IOT

The IoT applications involve numerous smart devices connected to each other over the Internet, enabling the aggregation of unparalleled amounts of information-data. Such collection of data means that devices connected in an individual's home are, in a frequent manner, providing millions of discrete vulnerable data points. This increases the possibility of an ambient data collection by the IoT devices, of which an individual-consumer is not aware. The ubiquitous application of these devices is also what intensifies the volume and variety of non-personal and personal data which can be exploited in unauthorised ways, raising concerns about the huge task of maintaining

[42] Shilpa Kolhatkar, *Super Vehicles: Connected Fleet IoT Solutions for Fire, Police, and Emergency Services*, Cisco Blogs, (Sep. 1,2021), https://blogs.cisco.com/digital/connected-fleet-iot-solutions.

integrity of consumers' data in the data-driven era of IoT.[43] Therefore, while the IoT devices are providing the greater efficiency in processes like automating tasks, collecting and disseminating information-data, updating performance, etc., it is also amplifying the traditional legal risks for consumers as inherently associated with the usage of Internet-technology enabled services.

1. The consumer related privacy concerns and the popularity of IoT applications

The companies are gleaning large amount of information-data from consumers' devices to make certain inferences about consumers' behaviour and plan economic decisions accordingly. This leads to increasing concerns of privacy. One of the serious privacy concerns associated with IoT devices is the possibility of different kinds of data related to an individual somehow ending up in the hands of unauthorised persons, which could be enriched by such persons by combining data sets from myriad of IoT devices. Even if such data is non-personal data, the combination of such data from different sources could lead to identification of personal data or personal profile of a consumer.[44] For instance, sensors generally present in

[43] Supra note 3.

[44] *Personal Data Protection for Internet of Things Deployments*, European Large-Scale Pilot Programme, (Sep. 1,2021), https://european-iot-pilots.eu/wp-content/uploads/2020/06/Personal-Data-Protection-for-IoT-Deployments_2020.pdf.

an IoT enabled room, like temperature monitors, air quality and CO2 sensors, humidity sensor and light sensors can work in coordination to track the presence and number of occupants in that room with surprising precision.[45] More specifically, companies like Amazon, by combining a number of data inputs from sources like various Alexa enabled devices and devices connected to such Alexa enabled devices, cameras, its streaming services, internet browsing and other web services, can easily create a virtual profile of the user, who can then be targeted with personalized recommendations and advertisements.[46]

Further, the IP addresses of the multiple IoT devices can be linked together to create a unique 'digital fingerprint' that is attributable to a single individual.[47] In other words, the significant personal data pertaining to an individual may be derived through collection of different sets of non-personal data as processed by different IoT devices used by the individual. Such personal data may lead to

[45] Nashreen Nesa & Indrajit Banerjee, *IoT-based sensor data fusion for occupancy sensing using Dempster–Shafer evidence theory for smart buildings*, (Sep. 1,2021), https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/#easy-footnote-bottom-5-22883.

[46] Matt Burgess, *All the Ways Amazon Tracks You—and How to Stop It*, (Sep. 1,2021), https://www.wired.com/story/amazon-tracking-how-to-stop-it/.

[47] Northern Kentucky Law Review, Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 NKLR 29 (2016), https://heinonline.org/HOL/LandingPage?handle=hein.journals/nkenlr43&div=6&id=&page=.

manipulation in the hands of unauthorised persons, and data losing the value it was originally collected for. More specifically, the concept of 'quantified self' could expand enormously to create rich behavioural profiles.[48] Hence, the *sui generis* concern related to the application of IoT applications is the massive aggregation of data that can lead to the database of behavioural profiles storing the sensitive details about patterns, preferences, habits, and other information that are unique to an individual.

Issues of privacy arise when the data is shared between sources without the consent or information of the person. Adding to the complexity and novelty of IoT is the fact that traditional approach to the 'Notice and Consent' is difficult for service providers to be adopted in the context of IoT enabled devices. Each end-point of the IoT environment, things, sends data automatically and communicates with other endpoints and works in conjunction.[49] For instance, there are devices such as Fitbit Tracker that does not have interface or if there is one, then it is a small display which makes the incorporation of digital notification and consent, a difficult concept according to the traditional approach. Similarly, as noted before there are numerous stakeholders in an IoT

[48] *Id.*

ecosystem- sensors manufacturer, device assembler, third-party applications, data centre, and cloud service providers, inter alia - which makes it more difficult, in the absence of any standardization, to discern which stakeholder's privacy policy is applicable to the contentious piece of data.

2. The increasing number of novel Internet-related cyber-security issues

As the number of Internet-connected objects expand, the more serious issues of interoperability and interdependence develop as potential attacks surface. Since, IoT industry has begun to thrive on personal information, security concerns in the recent times have increased manifold. According to the Hewlett Packard's ("**HP**") study, one IoT device has an average of 25 vulnerabilities.[50] The threats such vulnerabilities pose can be illustrated through an incident that occurred in the US, exposing the vulnerability of IoT devices. White supremacists in 2017 hacked into networked printers and fax machines at numerous of universities, including the University of California, Berkeley, causing the machines to print out racist propaganda.[51] Some of the other infamous

[50] K. Rawlinson, *Hp study reveals 70 percent of internet of things devices vulnerable to attack*, HP, (Sep. 1,2021), https://www.hp.com/us-en/hp-news/press-release.html%3Fid=1744676#.YS9sS05R3IU.

[51] Carl Straumsheim, *More Anti-Semitic Fliers Printed at Universities*, Inside Higher Ed, (Sep. 1,2021), https://www.insidehighered.com/quicktakes/2017/01/27/more-anti-semitic-fliers-printed-universities.

incidents include the Tesla car accident in 2016[52], NotPetya attack in the transport industry causing a loss of over USD 300 million[53], etc. such incidents have confirmed that people's control over environment has become subdued with increased dependency on IoT that are vulnerable and prone to hacking.

Such vulnerabilities as associated with IoT applications coupled with the fragile state of the Indian cyber-security infrastructure portends the need of initiating an informed public conversation among consumers about the responsible use of IoT solutions. Indian Computer Emergency Response Team ("**CERT-in**") reported almost 4 lacs cyber security incidents in 2019, which rose to around 11.5 lacs in 2020. James Cook, sales director South Asia, upon analysis of India-specific data, stated

---

[52] Anjali Singhvi & Karl Russell, *Inside the Self-Driving Tesla Fatal Accident*, The New York Times, (Sep. 1,2021), https://www.nytimes.com/interactive/2016/07/01/business/inside-tesla-accident.html. [See also, Ashley Thomas, *States Take the Lead on Securing IoT,* Law Journal Newsletters (01/04/2020) https://www.lawjournalnewsletters.com/2020/04/01/states-take-the-lead-on-securing-iot/ last seen on 01/10/2021. Amazon introduced Ring Camera with made news headlines after hackers breached the devices. There were numerous accounts of hackers obtaining access to the cameras and taunting and yelling obscenities at children, and threatening adults for bitcoin ransomware through the cameras. As a result of these hacks, Amazon is now facing a **class action lawsuit** claiming that the Ring camera security vulnerabilities were a result of Amazon's negligence and that it led to an invasion of privacy. *See*, *John Baker Orange v. Ring LLC and Amazon .Com LLC*, No. 2:19-cv-10899 (2019)]

[53] Lee Mathews, *NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million*, Forbes (16/08/2017), (Sep. 1,2021), https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#5e7b5ef84f9a.

wrong channelizing of resources to be the reason for such occurrences-

> '*Security breach is higher in India because they have been spending their budget either at wrong places or were more focussed only at the end points. According to the study, 81% respondents lay emphasis on endpoint or mobile defences - which is ranked at the top in terms of spending plans, while data-at-rest stood at the bottom with 54%.* [54]

3. The curious case of 'dark patterns'

The term 'dark pattern' was coined by Harry Brignull, who defines them as interface designs that *'trick users into doing things that they might not want to do, but which benefit the business in question*'[55]. For instance, until recently it was common for online travel booking portals to use the pre-checked consent boxes at the payment stage to default the users into buying insurance cover, even when the user had no active interest in purchasing the product. Insurance and Regulatory Development Authority of India ("**IRDAI**") raised concerns that such clever in-app defaults impede

[54] *Data breach incidents in India higher than global average*, The Economic Times (23/07/2018), (Sep. 1,2021), https://economictimes.indiatimes.com/articleshow/65107118.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[55] Harry Brignull, *About Us*, Dark Patterns, (Sep. 1,2021), https://www.darkpatterns.org/about-us..

consumers' *'informed choice'*.[56] In the example, the use of 'pre-checked boxes' is a classic example of a dark pattern. The dark pattern assumes the user's default preference as to purchase an add-on financial service even when it is not the case. Here the users are expected to be attentive to uncheck the box and opt-out. But as the UK's Financial Conduct Authority has submitted[57], often consumers use digital services under time constraints and are less likely to opt-out or be aware of existing defaults.

Beset by their cognitive vulnerabilities, limited rationality and the constraints on the time and attention, a sizeable proportion of consumers' end-up buying services without an informed consent. Therefore, dark patterns-based interfaces are manipulative in sharp contrast to persuasive marketing efforts. More worryingly, research suggests that individuals with lower levels of education and in urgent need of money make for easy targets for clever service providers.[58] This has significant implications for India, which is characterized by low income, low levels of digital

[56] Insurance Regulatory and Development Authority of India*, Circular on Travel Insurance Products and operational matters*, IRDAI (Sep. 1,2021), https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo3913&flag=1.

[57] *General Insurance Add-Ons Market Study – Remedies: banning opt-out selling across financial services and supporting informed decision-making for add-on buyers*, Financial Conduct Authority, (Sep. 1,2021), https://www.fca.org.uk/publication/policy/policy-statement-15-22-general-insurance-add-ons.pdf.

[58] Journal of Legal Analysis, Jamie Luguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, 13 JLA 43 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205.

literacy and a sizeable proportion of first-time users of Internet. Such consumers having subscribed for services unintentionally and unknowingly also get severely exploited in terms of collection of data pertaining to them. These learnings are also significant in the cases of IoT and voice assistance and other device types.[59]

The distinction between personalization and manipulation has been at the heart of policy issues that stem from the use of personal information during supply of digital services. It is crucial that a legal framework must be incorporated to identify manipulative dark patterns in the context of consumer's choice, value-system, and socio-economic background.

4. Non-Personal Data Generation and Associated Risks

Non-personal data may be defined in a negative sense as the set of data which excludes personally identifiable information is non-personal data.[60] In general, in contrast to personal data, non-personal data is anonymous. It can

[59] *Dark Patterns Workshop Transcript*, Federal Trade Commission, (Sep. 1, 2021), https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf.

[60] Government of India, *Report by the Committee of Experts on Non-Personal Data Governance Framework*, Ministry of Electronics and Information Technology, (Dec 2020), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf; The Indian Express, Aashish Aryan, Explained: What is non-personal data?, (Sep. 26,2021), https://indianexpress.com/article/explained/non-personal-data-explained-6506613/.

also include the data that has been converted from personal to anonymous data.[61]

Non-personal data can be either public, community, or private.[62] The data collected by the government or other authorities based on surveys, sampling, and similar collected methods is public non-personal data. Regular censuses, data regarding air pollution of a particular area, etc. are good examples. Community non-personal data relates to any data in its raw form, collected from a community of persons. Finally, private non-personal data is anonymous data collected from a particular individual. This can include anonymous data collected by fitness apps, an automobile company collecting data about the condition of its vehicle through sensors, etc. It can thus be concluded that the data generated as a by-product of use of IoT is primarily private non-personal data.

Therefore, the constant concern attached to non-personal data is the risk of re-identification of individuals through anonymous data. Re-identified data can pose a serious threat on various levels, prominent being the privacy

---

[61] *Report by the Committee of Experts on Non-Personal Data Governance Framework*, Ministry of Electronics and Information Technology, Government of India, (Sep. 26,2021), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

[62] Government of India*, Report by the Committee of Experts on Non-Personal Data Governance Framework*, Ministry of Electronics and Information Technology, (Dec 2020), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

concerns of an individual.[63] Non-personal data can also pose risks related to companies / government identifying or targeting specific communities based on the analysed community data in its anonymous form and using non-personal data for manipulative marketing or policies. The body corporates might deploy discriminatory policies based on such analysis[64], targeting selective highly profitable areas and leaving out others. It is unclear how such practices would be in line with goals like public or community benefit. This can take an even more aggravated form if the data is re-identified, opening ways to exploit the religious, political, economic, or other focal points in the community data.

5. REGULATORY APPROACH FOR BALANCING IOT AND DATA PROTECTION: INDIAN SCENARIO

At a grander-scale in IoT ecosystem there are different industries in coalition dedicated to promoting automated collection and dissemination of data as always available for analytics. It is a critical time now for these stakeholders to

[63] *Report Summary, Non-Personal Data Governance Framework*, PRS Legislative Framework, (Sep. 26,2021), https://prsindia.org/policy/report-summaries/non-personal-data-governance-framework.

[64] Aishwarya Girdhar, *Regulate non-personal data*, The Pioneer, (Sep. 26,2021), https://www.dailypioneer.com/2020/columnists/regulate-non-personal-data.html. ("Even seemingly benign data on communities can lead to collective harm, such as if data on average income is used to decide interest rates for those living in a certain area, or demographic census data is used to target communities based on social or religious lines")

work on uniform standards and flexible protocols that can harmonise collaborative development of the IoT technology without any prejudice to the private and public concerns. In a new world of IoT artefact design, it is necessary to follow an intensive participatory design approach that actively involves the data privacy and security needs of multiple users and stakeholders in the IoT design process.[65]

1. The proposed legal regime to govern IoT in India

Currently, Indian government's approach is not focussed on regulating the risks associated with expansive usage of IoT. It is rather focussed on scaling up the usage of IoT at the industrial level. It is also determined to involve IoT at the larger scale in its aspiring 'Smart Cities Mission'. In 2015, the MeitY formulated **the 'Draft IoT Policy'** to propose the plan of 'smart cities' that will be comprised of all kinds of smart facilities – parking, transportation, lighting, etc.[66] The Draft IoT Policy sets out the approaches for the development of the capacity building

[65] Rachelle Bosua, Megan Richardson, Karin Clark, Sean Maynard, Atif Ahmad & Jeb Webb, *Privacy in a world of the Internet of Things,* Networked Society Institute, University of Melbourne, (Sep. 9,2021), https://apo.org.au/sites/default/files/resource-files/2018-01/apo-nid131656.pdf.

[66] *IoT Policy Document*, Ministry of Electronics and Information Technology, (Sep. 9,2021), http://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

and incubation, R&D and innovation, incentives and engagements, demonstration centres, and human resources development, in relation to boost the IoT scaling. Apart from mentioning the 'requirement of standards' and 'governance structure', the Draft IoT Policy avoids charting out any further details in terms of regulatory approach of India to govern IoT.

Thus, the Draft IoT Policy clearly fails to take into account the need of basic regulations that any consumer-friendly ecosystem must have before the roll out of a disruptive technology like IoT. The privacy breach risks are the foremost concerns which most of the advanced international regulators are addressing in respect of IoT. The Draft IoT Policy does not mention anything about measures to protect integrity of consumers' data. This warrants immediate attention given the fact that India still does not have any comprehensive legislation on data protection. It is further important to note that the Draft IoT Policy is only at the draft stage which has not been finalised and, therefore, even after five years of its release, India has not recognised any standards or SOPs in respect of IoT.

In 2018, the Department of Telecommunications ("**DoT**") issued **guidelines for implementing restrictive features for SIM cards used only for M2M communication services and related KYC instructions for issuing**

M2M SIM cards to organizations providing M2M communication services.[67] These guidelines covered registration and technical requirements in respect of M2M service providers that are engaged in providing M2M services through SIM embedded M2M devices. Pursuant to this, the Department of Telecommunications has recently also put out a set of Draft Guidelines for Registration Process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Provider for M2M Services.[68]

It is important to note that the guidelines describe M2M services as the "services offered through a connected network of objects/devices with identifiers in which M2M communication is possible with predefined back-end platform(s)" collecting and analyzing the information from these devices / objects. These guidelines do not cover

[67] Government of India, *Instructions for implementing restrictive features for SIMs used only for Machine-to-Machine (M2M) communication services (M2M SIMs) and related You're your Customer (KYC) instructions for issuing M2M SIMs to entity/organisations providing M2M Communication Services under bulk category and instructions for Embedded-SIMs (e-SIMs)*, Department of Telecommunications, (June 2018), https://dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1%20.

[68] Government of India, Draft Guidelines for Registration Process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Provider for M2M Services, Department of Telecommunications, (June 2021), https://dot.gov.in/sites/default/files/Inviting%20Public%20comments%20on%20Draft%20Guidelines%20for%20Registration%20Process%20of%20M2M%20Service%20Providers%28M2MSP%29%20and%20WPANWLAN%20Connectivity%20Provider%20for%20M2M%20Services.pdf?download=1 .

precisely the IoT as they regulate specifically the communication among machines such as machines involved in supply chain management or fleet management, whereas the regulation of IoT entails the regulation of communication between machines as well as machines and humans, such as voice-controlled smart home features. Therefore, both the guidelines as discussed in the preceding paragraphs do not provide any guidance on security measures to be considered for the protection of data of consumers using commercial IoT services.

Against this background, it is noteworthy that a working group of Telecommunication Engineering Centre prepared a technical report on the subject of **IoT/M2M security** ("**TEC Report**") which also focused on the solutions pertaining to IoT.[69] This TEC Report was introduced in 2019. The TEC Report adequately recognized the need of having guidelines specific to IoT other than the M2M from the security point of view with respect to challenges posed by IoT in terms of ensuring data ownership and protection of sensitive data of consumers. As mentioned in this paper in the preceding chapters, the TEC Report specifies how the IoT will

[69] TEC is a technical body representing the interest of Department of Telecom, Government of India: *Technical Report Recommendations for IoT/M2M Security*, Telecommunication Engineering Centre, Government of India, (Sep. 26,2021) https://tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20Iot%20M2M%20Security.pdf.

"exacerbate the problem because many applications generate traceable signatures of the location and behavior of the individuals". It asserts the importance of balancing the 'anonymity' and the 'liability' in the context of IoT applications. It emphasizes that an application to be accepted, "the user requires the guarantee to have a certain degree of protection of its personal (or other) information". In furtherance to this, liability is a "deeply related requirement".

On the lines of the TEC Report, the TEC recently released a **'Code of Practice on Securing Consumer Internet of Things' ('TEC Code of Practice')** to provide a draft of the voluntary security standards and guidelines for manufacturers and service providers of consumer IoT devices.[70] The draft of the TEC Code of Practice largely incorporates the standards from the UK's 'Code of Practice on Consumer IoT Security' and the Australian 'Code of Practice on Security of Internet of Things for Consumers', as discussed in next part of this paper. Both the codes of practice are voluntary and, therefore, the TEC Code of Practice as well, and is due for implementation. The TEC Code of Practice acknowledges the possibility of leakage of data as a major threat due to ineffective and

[70] *'Code of Practice for Securing Consumer Internet of Things (IoT)'*, Telecommunication Engineering Center, (Oct. 1,2021), https://tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20 Code%20of%20pratice.pdf.

poor design of IoT devices and services. Therefore, the code as addressed to IoT device manufacturers, IoT service providers, mobile application developers and retailers suggests the standards that the IoT end points shall comply with in order to protect the users and the networks that connect these IoT devices. The TEC Code of Practice proposes to be applicable on consumer IoT devices that are connected to the internet such as watches, speakers, doorbells or baby monitors. It recognizes that different applications will require different security assurance levels, but does not provide a risk-based framework.

The TEC Code of Practice reiterates (moreover *clarifies*) that the IoT devices are required to "undergo mandatory testing & certification prior to sale, import or use in India, in compliance to the Mandatory Testing and Certification of Telecommunication Equipment (**"MTCTE"**) guidelines issued by Department of Telecommunications ("**DoT**"), Government of India under the Indian Telegraph (Amendment) Rules, 2017".[71] It proposes the

[71] *Mandatory Testing and Certification of Telecom Equipments (MTCTE)*, Telecommunication Engineering Centre, (Oct. 1,2021), https://www.tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments-mtcte. ["The Indian Telegraph (Amendment) Rules, 2017, provides that every telecom equipment must undergo mandatory testing and certification prior to sale, import of use in India. The final detailed procedure for Mandatory Testing and Certification of Telecom Equipments (MTCTE) under these rules has been notified separately. The testing is to be carried out for conformance to Essential Requirements for the equipment, by Indian Accredited Labs designated

guidelines such as the requirement of deploying the IoT devices in market with a default password that is unique per device and the need of providing a dedicated channel to the public for reporting security issues or vulnerabilities. The draft code covers the aspect of data protection as well such that it proposes to call out the manufacturer to disclose information about the personal data processing to consumers in clear and transparent manner. It further requires the consumers' consent obtained in "a valid way" with the capability to withdraw the same. Finally, the draft code suggests the collection of minimum data as necessary for IoT device functionality. As the TEC Code of Practice is still in its draft stage and due for implementation.

2. Applicable legal framework for protection of consumers' data

The Information Technology Act, 2000 ("**ITA**")[72] and the 'Reasonable practices and procedures and sensitive personal data or information rules, 2011'[73] ("**IT Rules**") therein, provide the legal provisions that are currently applicable on the 'body corporates' in respect of data

by TEC and based upon their test reports, certificate shall be issued by TEC"]

[72] The Information Technology Act, 2000.

[73] Reasonable Practices and Procedures and Sensitive Personal Data or Information Rules, 2011.

protection. Section 43A[74] of ITA read with the IT Rules provides the basic protection against mishandling of sensitive data by a body corporate.[75] It aims at providing compensation to the affected persons for the negligence or failure of the body corporate in '*implementing reasonable security practices and procedures*' in handling sensitive data or information. However, being a generally worded provision, this provision does not effectively cover the concept of IoT and related issues. This highlights the need for a comprehensive privacy legislation that can catch up with the speeding technological advancements.

3. Status of data protection legislation for India

The Indian government had set up the Committee of Experts on a Data Protection Framework for India ("**Srikrishna Committee**") in 2017, which was chaired by Justice B. N. Srikrishna. The Srikrishna Committee released its report titled 'A Free and Fair Digital Economy' in 2018 along with the draft of the Personal Data Protection Bill, 2018. However, the proposed bill lapsed in the Parliament and the Personal Data Protection Bill, 2019

[74] S. 43(A), he Information Technology Act, 2000; R. 4, Reasonable Practices and Procedures and Sensitive Personal Data or Information Rules, 2011.

[75] *Internet of Things Legal & Tax Issues*, Nishith Desai Associates, (Sep. 9,2021), https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Internet_of_Things.pdf.

(**the 'Bill'**) thereafter was introduced. The Bill not only addresses the concerns which earlier were not covered under existing law that provides data protection in India but also brings into the picture certain pre-requirements that are required before any firm begins to collect, analyse and disseminate data in India. It also seeks to establish a Data Protection Authority. However, there are certain aspects of the Bill which require attention of legislators so as to pass a privacy legislation that is comprehensive enough to adequately regulate disruptive technologies like IoT.

The bill explicitly defines validity of '*consent*' as one which is 'free, informed, clear, specific and capable of being withdrawn'. Section 11[76] also lays down conditions under which consent will not be held to be a valid consent and expressly states that the burden of proof to prove consent is on data fiduciary. However, in case of IoT devices, which continuously communicate with the environment in its functioning, the systems do not obtain the consent every time while initiating any actions. Moreover, the procedure for consent is a fatigue process. The procedure as specified in the Bill could deter in smooth functioning of IoT due to lack of consent at various occasions or lag in functioning due to waiting period for the obtainment of consent. As emphasised in the paper above, the traditional

[76] S. 11, The Personal Data Protection Bill, 2019 (Pending).

consent model will not work and there is a need to propose an IoT specific procedure. Such a procedure must allow manufacturers and service providers with flexibility to collect data for the purposes of enhancing provision of services and it must be strict enough to deter them from collecting excessive data.

Another obscure provision with respect to firms engaging in provision of data-driven services is the definition of '*harm*'.[77] Amongst various parameters as written down in the Bill as to what causes 'harm', it further includes 'any observation or surveillance that is not reasonably expected by the data principal.'[78] The use of the word 'reasonably' creates a grey area for the IoT solutions provider to decipher and may also be at times subjected to very different interpretations by the users or the manufacturers of IoT. The use of word 'reasonably' is one such instance in the Bill which leaves the same to be interpreted over a period of time by judiciary or complementing regulations and rules. Hence, it creates a dwindling standard for the IoT stakeholders. This requires more specific and certain regulatory guidelines with respect to IoT and similar type of other services where data is collected, processed and analysed continuously.

[77] S.3(20), The Personal Data Protection Bill, 2019 (Pending).
[78] S. 3(20)(x), The Personal Data Protection Bill, 2019 (Pending).

Section 15 of the Bill gives the power to the Central Government to classify any other personal data as '*sensitive personal data*' apart from what already has been listed down under section 3(36).[79] The firms dealing with sensitive personal data has more stringent provisions to be adhered to as they are considered 'significant data fiduciaries' ("**SDFs**"). The Bill envisages the framework where firms are categorized as SDFs if engaged in processing of sensitive personal data or significant volume of personal data.[80] SDFs are subject to additional compliance requirements and higher fines for violations.[81] However, there lies no provision for the firms to appeal to another authority regarding their stance if the categorisation is in fact appropriate or not. Hence, small firms may hesitate from venturing into the IoT industry due to subjective norms and immediate compliances needed after

[79] Ss. 93, 15 & 3(36), The Personal Data Protection Bill, 2019 (Pending). S. 93 read with s. 15 lays down factors to be considered while categorizing data as 'sensitive personal data', which are, the risk of significant harm, the expectation of confidentiality attached to such category of personal data; whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and the adequacy of protection afforded by ordinary provisions applicable to personal data.

[80] S. 26, The Personal Data Protection Bill, 2019 (Pending); S. 38, The Personal Data Protection Bill, 2018 (Pending). The criteria for categorization of SDFs are to be determined by DPA by taking into account following factors: (a) volume of personal data processed; (b) sensitivity of personal data processed; (c) turnover of the data fiduciary; (d) risk of harm by processing by the data fiduciary; (e) use of new technologies for processing; and (f) any other factor causing harm from such processing.

[81] Ch. VII, XI, The Personal Data Protection Bill, 2019 (Pending); Ch. VI, X, The Personal Data Protection Bill, 2018 (Pending).

categorisation as SDFs to save themselves from the strict penalties. The Bill also nowhere explains the meaning of 'critical personal data' but categorises the same as data which is notified so by the Central Government.[82] This leaves an arbitrary vacuum for the government to fill in as per what it deems fit rather than a judicial authority.

MeitY appointed a committee of experts to recommend a **framework to regulate the flow of non-personal data** in India. Since then, the Committee has released two **reports** on the topic of regulation of non-personal data, with the later one[83] (the 'Revised Non-personal Data Framework') being the revision of the original report.[84] However, the stakeholders have voiced major concerns in relation to framework on the governance of non-personal data. The concerns are around the existing lack of regulations on personal data in India that leads to the ambiguity about the appropriate authorities and the scope of their powers. For example, the proposed non-personal data Authority in the revised report might conflict with the regulatory purview of the proposed Data Protection

[82] S.33(2), The Personal Data Protection Bill, 2019 (Pending).
[83] *Report by the Committee of Experts on Non-Personal Data Governance Framework*, Ministry of Electronics and Information Technology, Government of India, (Sep. 26,2021), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.
[84] The Original Report: *Report by the Committee of Experts on Non-Personal Data Governance Framework*, Ministry of Electronics and Information Technology, Government of India, (Sep. 26,2021), https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.

Authority of India or the Competition Commission of India on different subject-matters of data usage and its nature.[85] Finally, another challenge to the successful implementation of the proposed non-personal data regulation is allowing corporations to become 'data trustees.' Such trustees are responsible for 'creation, maintenance, and data-sharing of HVDs (High-Value Datasets).' Not having ample restrictions on the eligibility might put such HVDs at risk.[86] It goes without saying that a well-balanced regulation is required for effective utilization of non-personal data to achieve the twin objectives of public good and economic profitability. However, the aforementioned challenges need to be addressed and their elimination is a prerequisite to rolling out any successful regulation on the subject.

4. Other applicable legislations to safeguard consumers' data protection interests

The inadequate definition of *'harm'* and *'consent'* pose similar challenges in other applicable legislations as well. The Consumer Protection Act 2019 includes the concept

[85] Nikhil Pahwa, *Event Report: Governance Of Non Personal Data*, Medianama, (Sep. 26,2021), https://www.medianama.com/2021/01/223-event-report-governance-of-non-personal-data/.

[86] Ayush Tripathi & Gautam Kathuria, *Changes and challenges in the revised regulatory framework for non-personal data*, The Print. (Sep. 26,2021), https://theprint.in/theprint-valuead-initiative/changes-and-challenges-in-the-revised-regulatory-framework-for-non-personal-data/586117/.

of '*product liability*'[87], and for an action to be raised under the provision, some '*harm*' must be caused to the consumer. However, both the definitions of '*harm*'[88] and '*injury*'[89] miss out breach or leak of sensitive non-personal or personal data, and, hence, doesn't explicitly cover harm to privacy by IoT related devices and services. It is important to note that the Consumer Protection Act 2019 also includes "disclosing to other person any personal information given in confidence by the consumer" as an unfair trade practice, except otherwise mandated under law.[90] This raises the concern of having regulatory overlaps once a comprehensive data protection legislation comes into force. This leaves the judicial authority with the task to determine the regulatory purview of the Consumer Protection Act 2019 in comparison to other regulators.

6. REGULATORY APPROACHES IN INTERNATIONAL ARENA: BEST PRACTICES

Concerns regarding the usage of the IoT technology and the policy that governs it, call into question key norms of established regulatory regimes, globally. This also presents a question over the objective of achieving interoperability and universal networking, and the aim to avoid Internet

[87] Ss. 2(34), 2(35), 82-87, The Consumer Protection Act, 2019.
[88] S. 2(22), The Consumer Protection Act, 2019.
[89] Ss. 2(23), The Consumer Protection Act, 2019.
[90] Ss. 2(47)(ix), The Consumer Protection Act, 2019.

fragmentation. Given that the cyber-threat landscape is continuously evolving and adapting in a dynamic and unpredictable manner, there arises a concern whether regulators should continue in near term to commit with comprehensive cyber-security legislations or not.[91] The IoT is redrawing the boundaries of what constitutes 'personally identifiable information' and, fundamentally, challenges the way we address to cope with this evolution.[92] In order to understand the needed legal requirements, it is important to identify the best practices that have been adopted around the world to maintain the integrity of data of consumers using IoT.

1. European Union

The **European Union** ("**EU**") passed the **General Data Protection Guidelines** ("**GDPR**")[93] in 2016, replacing

[91] Allison Grande, *House Republicans urge FCC to curb Cybersecurity Measures*, Law360, (Sep. 9,2021), http://www.1aw360.com/articles/549350/house-republicans-urge-fcc-to-curb-cybersecuritymeasures.

[92] Carl Straumsheim, *More Anti-Semitic Fliers Printed at Universities*, Inside Higher Ed, (Sep. 9,2021), https://www.insidehighered.com/quicktakes/2017/01/27/more-anti-semitic-fliers-printed-universities.

[93] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Communities*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, last seen on 01/09/2021 (hereinafter 'GDPR').

the EU Data Protection Directive 95/46/EC.[94] The GDPR went into effect from May 2018. Though GDPR is not free of loopholes, it leaves IoT industries in water-tight compartments for its loopholes to be as little exploited as possible. It has come as a revolutionizing step for the data-thriving industries, empowering the users alongside creating awareness among them regarding their data. It is interesting to note is that GDPR was passed in the year 2016, it took two years to come into enforcement, and the time given to the companies to adjust their policies. This left a whole new scenario and a formalised channel of benchmarks in the IoT industry. GDPR harmonizes with the EU data protection laws and provides the institution of a single comprehensive legislation that is applicable to all the members of the EU.

Most of the legal compliances laid down in the GDPR are going to raise a significant burden over the IoT entities. Among the compliances for IoT entities, one is the 'right to be forgotten' under Article 17[95] of the GDPR, which provides strict requirement for data controllers to erase any personal data of a consumer that is unnecessarily being processed and when there are no overriding legitimate

[94] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal of the European Communities, (Sep. 9,2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.
[95] See GDPR, Article 17.

grounds to do so by the IoT entities. Further, the 'right to portability', under Article 18[96] of the proposed GDPR, for example, gives data-subjects the right to receive from data controllers their personal data in a commonly used electronic and structured format that allows for further use by other data controllers.[97] Further, the Article 25(1)[98] of the GDPR obliges the data controller to take appropriate technical and organizational measures for the protection of personal data into account during the development of the product.

All the above-mentioned principles related to data protection are already being followed in the Bill 2019 as it follows the GDPR as template. The most significant takeaway from the EU regime is the IoT specific regulatory approach. The EU has introduced the draft of **the regulations supplementing the Radio Equipment Directive 2014/53/EU** ("**RED**")[99] **to provide regulations in respect of 'Internet-connected radio equipment and wearable radio equipment'** ("**Draft**

[96] See GDPR, Article 18.
[97] Omar Tene & Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, Future of Privacy Forum, (Sep. 9,2021), https://fpf.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-WhitePaper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf.
[98] See GDPR, Article 25(1).
[99] *Radio Equipment Directive (RED)*, European Commission, (Sep. 9,2021), https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en.

RED Law").[100] This draft of the regulations aims at strengthening the security of internet-connected devices, most of which are expected to be part of the IoT, and of wearable radio equipment. The draft once passed shall act as the delegated act required to enforce article 3.3(e) of the RED[101], which lays down essential requirement of incorporating safeguards to ensure that the personal data and privacy of the user and of the subscriber of the device are protected. The draft covers a wide range of IoT enabled devices, from wearables to childcare devices and all internet connected radio equipment, if that radio equipment is capable of processing, trafficking and locating personal data.[102] The proposed delegated act suggests the approach of introducing a primary law i.e., GDPR, that provides the broad based principles and a secondary law that provides the substantive provisions for

[100] *Internet-connected radio equipment and wearable radio equipment*, European Commission, (Sep. 9,2021) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Internet-connected-radio-equipment-and-wearable-radio-equipment_en.

[101] *Radio Equipment Directive (RED)*, European Commission, (Sep. 9,2021), https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en.

[102] *Internet-connected radio equipment and wearable radio equipment*, European Commission, (Sep. 9,2021) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2018-Internet-connected-radio-equipment-and-wearable-radio-equipment_en, (The delegated act ensures that RED provide certain essential market access requirements for "smart appliances, smart cameras and a number of other connected radio equipment like mobile phones, laptops, dongles, alarm systems and home automation systems" or other such equipment that is at risk of "hacking and of privacy issues when they are connected to the internet".)

implementation of the given principles i.e., Draft RED Law.

2. United Kingdom

In addition to the GDPR like data protection regulations, the additional step that the United Kingdom ("**UK**") regime has taken is the introduction of the code of practice applicable to IoT specific industry stakeholders. The Code of Practice for Consumer IoT Security[103] requires manufacturers and IoT service providers within the UK to comply with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world. The Code of Practice outlines following key principles that such entities must comply with:

1) IoT devices must not be sold with universal default usernames;

2) The service providers must have a vulnerability disclosure policy;

3) The IoT software must be kept updated;

[103] *Code of Practice for Consumer IoT Security*, Department for Digital, Culture, Media and Sport, (Sep. 9,2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.

4) Ensure secured storage of credentials and security-sensitive data;

5) All communication, including remote management and control, must be encrypted;

6) Risk minimising measures must be adopted when attack surfaces including unused ports and superfluous code;

7) Ensure software integrity; and

8) Compliance with GDPR if any personal data is processed by IoT devices.

3. United States

In the United States ("**US**"), there is no single and comprehensive self-regulating legislation related to the protection of privacy or personal data, generally. However, the US has a collection of separate federal and state laws and regulations, with the common-law principles. A thing to be noted from privacy regulations in the US is that the laws and regulations in the country are specific to the industries which use processing of data in their facilities. **The Gramm-Leach Bliley Act, 1999**[104] governs the regulation of the financial institutions that collect public information. At the same time for regulating flow of health

[104] 15 U.S.C. Ss. 6801-09 (United States); 16 C.F.R. Ss. 313.1-.18 (United States); 16 C.F.R. Ss. 314.1-.5 (United States).

data of consumers, there is the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"),[105] as amended by the **Health Information Technology for Economic and Clinical Health Act of 2009** ("**HITECH**")[106], which protects the personal data-information held by healthcare sector and certain entities. The industries which do not come in the ambit of the specific limits of the aforesaid statutes, but collect and process consumer personal data, falls under the **Federal Trade Commission Act of 1914** ("**FTC Act**"), in furtherance to prohibiting unfair or deceptive commercial practices.[107]

The US law understands that it is practically unrealistic for the businesses to provide consumers with notice and choice every time they want to change their use of data, particularly in the age of constantly connected devices and ever-shifting consumers. As it is not possible to control the interaction of myriad objects or create virtual boundaries, it will be equally impossible to control data flows and subsequent uses of data.[108] Therefore, section 5 of the FTC

[105] 45 C.F.R. Ss. 160.101-.552 (United States); 45 C.F.R. Ss. 162.100-.1902 (United States); 45 C.F.R. Ss. 164.102-534 (United States).
[106] 42 U.S.C. Ss. 300jj-jj5l (United States); 42 U.S.C. Ss. 17921-53 (United States).
[107] 15 U.S.C. Ss. 41-58 (United States).
[108] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Federal Trade Commission, (Sep. 9,2021), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

is an authority as it seeks to prevent potential violations of data privacy that are the result of 'unfair or deceptive acts or practices in or affecting commerce'.[109] The language of section 5 although does not refer to data privacy, but the FTC is using it as a statutory instrument to police potential data privacy violations. The US is also one of the few jurisdictions that has understood the need to regulate dark patterns. FTC also regulates dark patterns by using its power to punish *'unfair and deceptive practices'* under section 5 of the Federal Trade Commission Act. *AMG Capital Management v. FTC*[110] is an important ruling on dark patterns where AMG, a payday lender, deployed dark patterns in its digital loan agreement to auto-renew (instead of close) expensive payday loans as a default option. The FTC found AMG Capital Management guilty of unfair and deceptive practices.

Recently in the US**,** the Internet of Things Cybersecurity Improvement Act of 2020 was enacted. It lays down certain mandatory provisions and guidelines to be followed by the federal government for the use of IoT enabled devices.[111] However, the Act only aims at regulating the

[109] Branden Ly, *Never Home Alone: Data Privacy Regulations for the Internet of Things*, 2017 Journal of Law, Technology and Policy 539 (2017), (Sep. 9,2021), http://illinoisjltp.com/journal/wp-content/uploads/2017/12/Ly.pdf.

[110] *AMG Capital Management v. FTC*, No. 19-508 (U.S. April 22, 2021).

[111] *H.R.1668 - Internet of Things Cybersecurity Improvement Act of 2020*, Congress.gov, (Sep. 9,2021), https://www.congress.gov/bill/116th-congress/house-bill/1668/text.

use of IoT devices by the government contractors manufacturing or providing IoT services to the federal government[112], i.e., it is not a comprehensive self-regulating legislation related to the protection of privacy or personal data generally. Further, the California's 'Security of Connected Devices' law, which became effective in January 2020, is a state legislation that focuses on providing obligations for manufacturers to equip the IoT devices or other connected devices with reasonable security measures.[113] It is worth noting that the law seeks to determine certain liability of the 'manufacturer' in case of mishap while also delimits the scope by creating exceptions to the same.

4. Australia

IoT in **Australia** is regulated through the **Privacy Act, 1988** and the **Telecommunications Act, 1997**. Under this regime, collectors of personal information are supposed to notify the concerned person about particular matters, including what information is being collected, how it is collected, and how it will be used and disclosed.[114]

---

[112] Brian G. Cesaratto & Alexander J. Franchilli, *New Internet Of Things (IoT) Cybersecurity Law's Far Reaching Impacts*, Mondaq, (Sep. 9,2021), https://www.mondaq.com/unitedstates/security/1047166/new-internet-of-things-iot-cybersecurity-law39s-far-reaching-impacts-.

[113] "Security of Connected Devices," Cal. Civil Code §§ 1798.91.04-1798.91.05(b).

[114] *The Internet of Things and Australian Privacy Law*, Primerus, (Sep. 9,2021), http://www.primerus.com/wp-content/uploads/2016/06/HHG-IoT-article.pdf.

However, the reality differs from the idealised laws. Though the Telecommunications Act mandate all the firms to comply with the privacy provision (unlike Privacy Act which mandates only those firms with turnover more than USD 3 million), the Act is not as detailed as the Privacy Act is. Moreover, it does not regulate collection and storage of personal information. The Telecommunications Act is now being realised to not be flexible enough to include in itself the wide arena of IoT. However, Australia has recognised protection of personal data, there still remains ambiguity regarding what pertains to be 'privacy' and how IoT would be regulated.

The **Code of Practice**[115] (Securing the Internet of Things for Consumers) is a voluntary set of guidelines set out by the Australian government in 2020 with the objective of providing manufacturers and service providers with information regarding appropriate cybersecurity features and measures that must be complied with by their IoT devices. Principle 5 of the same lays down essential guidelines for device manufacturers, IoT service providers, mobile application developers and retailers. It provides that in case where the consent is an essential requirement for the processing of user's data, the same should be obtained in a legal and express manner, with the option to

[115] *Code of Practice (Securing the Internet of Things for Consumers)*, Australian Government, (Sep. 9,2021) https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf.

cancel and withdraw the same at any time. A year after the release of the voluntary guidelines, the government of Australia published a discussion paper[116] which aimed at achieving domestication of international standards for privacy and data protection, especially the European ones, suggesting government's plan to roll out a full-fledged IoT specific legislation and replacing the voluntary one.

7. BALANCING THE INTERESTS: RECOMMENDATIONS

The open and ubiquitous nature of the IoT technology may significantly increase its vulnerability to suspicious attacks that target private or personal data / information. This is a challenge for IoT service providers to maintain the integrity of consumers' data during the provision of data-driven services. As the gap exists in respect of public conversation about the IoT stakeholders' accountability in India, the government intervention is important to provide a mechanism to correct for market failure and ensure accountability. Therefore, a specific regulatory policy, model or framework ("**Proposed Law**") is needed to guide the stakeholders to guarantee trust and liability determination in respect of the consumers' data-information or private information as recorded by the IoT

[116] *Strengthening Australia's Cyber Security Regulations and Incentives (A Call for Views)*, (Sep. 9,2021), https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf.

devices. The same has been observed as the best practice in the international jurisdictions that have started to regulate IoT. Although, India is considering to introduce the TEC Code of Practice for IoT stakeholders, it remains voluntary and at a draft stage. Further, the standards in it mostly are taken from the existing code of practices of the UK and Australia that are themselves is intending to build on these code of practices with a set of legally binding requirements.

The long-established norms of Internet governance are now required to be placed on the table for reconsideration. Following are the certain measures that may be considered by the appropriate regulator alongwith the standards provided under the TEC Code of Practice to regulate and, also, the industry stakeholders to self-regulate.

i. The primary legal measure that is needed to be standardised in the application of IoT technology is that to have **unambiguous 'terms of use'** or **'terms of service'** ("**ToS**") as well as privacy policies that are enforceable against the end-users of the IoT devices. If the product does not have a user interface where the end-user can check a box or otherwise agree to terms i.e., in click-wrap agreements, then such agreement should be provided on a website to be agreed before enabling the functionality of the IoT product i.e.,

browse-wrap agreements. The need to have proper disclosure – specifically, about the possible additional data collection, data sharing with third parties, vulnerabilities and liabilities – is required to be introduced as a substantive provision in for the implementation of the broad-based principle of informed consent. The law may suggest specifics for privacy policy such that it should delineate details of personal data retention and time-period.

ii. The Proposed Law may also require an IoT service provider to report the efforts it is making in following 'privacy by design' principle so as to design interfaces that are better for in respect of privacy. It is suggested that the appropriate regulator may conduct a yearly review of IoT device manufacturers / service providers to assess whether they are investing in designs of IoT devices that are useful and convenient with respect to privacy controls.

iii. The TEC Code of Practice does not reflect the risk-based approach. There is a requirement for improved notification practice in respect of networked toys, devices and services that collect children's data. The tighter regulatory scrutiny may be implemented for child-specific products where the data subject is itself not competent

enough to understand the kind of data it is sharing during an interaction with a device. While there may be flexibility in other cases given the IoT service provider is transparent and open about its processing of data and the use of same is for the better provision of services to the data subject that is major and to the great extent aware about what it is sharing.

iv. The essence of the IoT technology is to gain the access to and analyse the voluminous data recorded by IoT devices. The ownership of that data then vests in the consumer who owns the device or the service provider who has gained the access to the data recorded. Therefore, an aspect worth noting is that since there are numerous channels of dissemination of the data / information and multiple stakeholders involved, the IoT service provider (data controller) at all times should ensure that the line between data controller and data processor does not get obscured.[117] It is required that the Proposed Law mandate the IoT service providers to specifically state the '**allocation of risk**' such that a certain

[117] Anirudh Sarin, *India: Legal issues pertaining to the IoT*, Mondaq, (Sep. 9,2021), http://www.mondaq.com/india/x/691560/Data+Protection+Privacy/Legal+Issues+Pertaining+To+Internet+of+Things+IOT.

party will bear the responsibility / liability for any breach of data protection obligations that IoT services assure to a consumer.

v. The corporate entities that are leading IoT ventures are facing strong challenge to manage the processing, storing, and securing the consumer related data. As the IoT technology is growing in its reach, the enterprises are outsourcing the data-management to the different cloud service providers.[118] To some extent, ceding the management of the 'sensitive' data of consumers to the third parties poses questions with respect to the current legal framework. In the absence of any contract, the liability for any data protection violations will remain with the contracting company, even if the third party is at fault. In such transactions there is a need to carefully define **legal obligations** of stakeholders involved in IoT value chain in a broad manner in the Proposed Law but without the use of vague words. Another obligation could be of providing clarity to the consumer in any manner possible in respect security measures that

[118] Mike Kavis, *The Internet of Things Will Radically Change Your Big Data Strategy*, Forbes, (Sep. 9,2021), https://www.forbes.com/sites/mikekavis/2014/06/26/the-internet-of-things-will-radically-change-your-big-data-strategy/?sh=43c893c61d45, l

will be implemented throughout the product lifecycle. This will provide clarity to consumers about when the device will no longer receive security updates or the user will fail to update the device.

vi. The Proposed Law must envisage the need of providing a collaborative space for innovators, manufacturers or service providers to test their products under the supervision of regulators and identify vulnerabilities. Such a cooperation between the regulator and stakeholders will ensure that the pre-launch of a product must be done along with the proper disclosure about the possible vulnerabilities. When the TEC Code of Practice talks about the proper disclosure of vulnerabilities, it is a broad-based principle which must be strengthened by providing substantive provisions for implementation of such a disclosure practice.

vii. The Proposed Law must be technology friendly such that it must be futuristic enough to comprehensively govern the advancements in the field of IoT. There must bea review mechanism for reassessing and amending the existing policies specific to IoT as the technology evolves and new products are introduced.

viii. In India, dark patterns such as *hidden costs* or *hidden contractual terms* could fall under the remit of the Consumer Protection Act 2019 and the Central Consumer Protection Authority ("**CCPA**") to redress such issues. The consumer protection legislation could be amended to allow CCPA to regulate dark patterns comprehensively within the scope of the term *'unfair and deceptive practices'*. The Proposed Law must provide that such issues related to dark patterns will be specifically dealt with by the CCPA in order to avoid the possibility of regulatory arbitrage or overlapse.

These recommendations are meant to provide standards to nudge companies to take a meaningful first step towards greater transparency regarding how they manage consumers' data and the degree to which consumers have any say in how their data is used.

8. CONCLUSION

The IoT technology is a very complex and unexplored phenomenon when viewed in the context of legal and policy challenges. IoT is contributing remarkably in the transformation and upgradation of standard of lives of people as a technological innovation. However, IoT is facing strong challenges against it due to lacunae in the legal frameworks. It is in the best interest of concerned

stakeholders to create a proper regulatory regime to ensure a balance between the interests of IoT stakeholders and data-privacy concerns of consumers of IoT products. The paper sought to explore and classify sector-specific policy challenges associated with IoT technology and its application in industry, with an aim to provide standards that can be followed as a solution to the challenges interface of law and IoT face in India.

IoT devices are rapidly integrating as indispensable architectures into different industries' infrastructure such as Healthcare, Transport, Education Sector, Fintech and Banking, Energy Sector, Law-enforcement etc. IoT technology has contributed heavily in the aforesaid sectors which is going to have a big impact on these industries. Therefore, it is imperative to find out the issues as well as solutions as soon as possible and keep the interests of stakeholders in balance.

There is no doubt that legal framework is lagging behind than the growth of application of IoT technology. There is a dire need for standardizing the process such that to have a comprehensive privacy policy in order to have a proper liability management in consequences in respect of data protection breach. The standards are needed to balance the interests of innovators as well as consumers at the same time. IoT, along with numerous benefits, will realize its potential to transform the lives in a uniform manner only

when the legal framework for it will evolve dynamically, keeping the incentive-promoting approach.