CWS/WP/200/46

WORKING PAPER

INTERFACE BETWEEN TECHNOLOGY, LAW AND POLICY IN THE DIGITAL WORLD: PROMISES AND UNCERTAINTIES

MONIKA[1]

RESEARCH FELLOW (LEGAL)

FEBRUARY 2018

CENTRE FOR WTO STUDIES

INDIAN INSTITUTE OF FOREIGN TRADE, NEW DELHI

1 All views and opinions expressed in this paper are personal, and do not necessarily reflect the views of the Centre, or the IIFT, or the Government of India. The author may be contacted at monikasingh@iift.edu

ACKNOWLEDGEMENT

I am grateful to Prof. Abhijit Das providing constant guidance and inputs which made this working paper possible. I would like to express my appreciation for Mr. Parminder Jeet Singh for his valuable comments which significantly improved the quality of the paper. I am also thankful to Aishwarya Atluri, Akanksha Bisoyi, Harita Putrevu, and Ridhish Rajvanshi for their assistance in the research for the paper.

TABLE OF CONTENTS

I. INTRODUCTION

Humankind is in the midst of a colossal technological revolution. Technology is rapidly evolving, and it in turn is shaping and getting increasingly embedded in our own lives, histories and futures. Recent advances in the areas such as information technology and telecommunications technology are changing lives by offering new means of exchanging information, transacting business and influencing the economic and social clusters of societies around the globe.[2] These revolutions are considerably different from the previous technological revolutions in terms of rate of development, degree of interconnectivity achieved between individuals and societies, and scale of impact on the society. Information technology and its uses have grown exponentially over a relatively short period of time. It has brought business, governance and societal components into a single interconnected ecosystem. Further, it has completely overhauled business practices, governance structures and cultural interactions.

One of the most remarkable elements of the knowledge based revolution is its limitless future possibilities. It has ushered in an age of rapid innovation. While it has raised the standard of living by allowing the governments to deliver public services more efficiently and effectively, at the same time it has also tested the limits of governmental control by creating new forms of inefficiencies. This struggle is particularly visible when it comes to rule making. Inherent natures of legal systems and present technologically driven society and business are diametrically opposite. Laws and regulations are tailored to be stable and long-serving whereas current technologically driven global environment is in a constant flux. This dichotomy is manifested in number of areas and it adds to the uncertainty wrought by technological revolution.

Disruptive nature of the current technological revolution has made already uncertain future even more difficult to predict. For instance, information technology enabled e-commerce is projected to be the future of global trade, but the form of this commerce and its repercussions on job structure, poverty, standard of living, industry etc., are unclear. Another challenge is that technology can raise inequality across the world. One of the biggest tasks to be tackled in the 21st century will be to ensure that whatever be the impact of e-commerce, it is meted out in a fair and equitable manner. It should bridge the global North-South gap, instead of widening it.

2 Mujahid, Y. H. , E-commerce & WTO: Digitalizing Trade Liberalization, 2003, National Post-Graduate Institute of Telecommunications and Informatics, Islamabad, Available at: http://kavehh.com/my%20Document/Essex/wto/E-commerce%20and%20WTO.pdf (Accessed on 3 October, 2017).

In order to address the challenges associated with advancement of technology, one must understand the technology behind e-commerce and direction of the governing rules that are sought to be tabled in global e-commerce discussions, mainly by the developed countries. The legal system faces dual challenge; first, to create a system which accounts for continually mutating technology and second, to establish an equitable ecosystem.

This paper seeks to understand the present state of technology, its linkage with law and challenges posed by law-technology interface. This examination is conducted in two stages- basic infrastructure, and framework of the Internet and Internet as platform for various applications. First section discusses Internet's infrastructure, its operational basics, and legal issues associated with it (**II)**. Second section studies applications of the Internet i.e. services and products based on the Internet and legal concerns arising from it (**III**). Third section briefly discusses specific cases of new information technology based services and products (**IV**). Finally, on the basis of issues examined in this paper some conclusions are drawn as to the direction taken by the Internet related legal rules in the context of e-commerce.

II. INTERNET: STRUCTURE AND OPERATION

The Internet is the framework which allows e-commerce to exist and flourish. Understanding its structure and functioning is necessary to comprehend the basic technology at the back-end e-commerce. This section, therefore, seeks to understand the basic concept and core principles based on which the Internet, as the infrastructure enabling physical transmission of the data, functions. This section also examines legal concerns relating to Internet's infrastructure.

A. Concept and Core Principles

The internet is a worldwide collection of networks that links millions of businesses, government offices, educational institutions, and individuals.[3] It is a structure which provides services like e-mail, search engines videos, file transfer, World Wide Web (WWW or Web) etc.[4] It is able to transfer information from one corner of the world to another at the speed of light due to technology of IP packets. Any content (e-mail, webpage, video, image, audio etc.) when sent through the Internet, is

3 University of West Florida, Chapter 02: The Internet and World Wide Web, In CGS 1570W: Computer Concepts and Applications, Summer 2006, Available at: http://uwf.edu/clemley/cgs1570w/index.htm (Accessed on 3 October 2017).
4 Diffen LLC, Internet vs. World Wide Web, 2017, Available at: http://www.diffen.com/difference/Internet_vs_World_Wide_Web, (Accessed on 4 October 2017).

converted into electric signals and divided into small pieces or bundles called Internet Protocol packets (IP packets or packets). Each packet is tagged with its ultimate destination and travels separately. When all the packets reach their ultimate destination, they are reassembled and converted back into the form of original content.[5] For example, a video sent through internet will be divided into numerous IP packets and each of these packets can take separate routes across internet to reach its intended receiver. Upon reaching the destination, packets will reassemble and form the video.

Audio, video, image, file etc. or data which is transferred in form of the packets is stored in a data storage system and a server processes requests and delivers the data to other computers (clients) over the Internet. Server comprises hardware and software components. They are classified into various categories depending upon the type of data handled- File Transfer Protocol (FTP) server for file storage and transfer, Web server for hosting websites, Gaming server for connecting games and gamers and so on.[6] Couple of chief server types are explained as follows:

i. *Domain Name Service (DNS)* server plays a crucial role in connecting various computers over the Internet. It contains a database of public IP addresses and their corresponding hostnames. It functions like a telephone exchange which maintains telephone number registry and connects callers to intended receivers. Each computer and device connected to the Internet is assigned a unique number called IP address. This number works as an address to the device and must be known to send or receive data over the Internet. There are two types of IP addresses- IPv4 and IPv6. They are unique identifiers and are aligned with a standard set of protocol parameters that ensure computers can talk to and understand each other. Since names are much easier to remember than numbers, number address (IP address) is converted into name (called hostname) for user convenience. For example, if user wants to access Flipkart, he/she does not have to remember its IP address (163.53.78.87). When user types Flipkart.com in the Internet browser, a request is automatically sent to the designated DNS server for IP address. If the DNS server has the IP address it will send the IP address back to the user's computer or in case designated server does not have the IP address it will send the request to other DNS servers, procure IP address from them and send it to the user computer. When user computer receives the IP address of Flipkart, it connects the user to Flipkart's website. An operator of DNS system

5 Woodford, Chris, The Internet, 2011, Available at: http://www.explainthatstuff.com/internet.html (Accessed on 4 October 2017).

6 Kanika Khara, A List of the Different Types of Servers You Must Know About, 2016, Available at: https://www.buzzle.com/articles/different-types-of-servers.html (Accessed on 5 October, 2017).

ensures that each device connected to the Internet has a unique IP address to facilitate seamless connectivity. There are five Regional Internet Registries (RIRs) that own, maintain and coordinate DNS servers across the world. [7] IP addresses are assigned and managed according to the rules formulated by Internet Corporation for Assigned Names and Number (ICANN) and Internet Assigned Number Authority (IANA).[8] ICANN is a private organisation and is responsible for maintaining the record of allocated and unallocated blocks of IPv4 addresses and IPv6 addresses; and is responsible for allocating large blocks of IP addresses to the five Regional Internet Registries (RIRs) according to its global policies.[9]

ii. *Web server* is another type of server which hosts websites on the Internet.[10] Web browser (a type of software) enables browsing through World Wide Web (WWW or Web). Google Chrome, Internet Explorer, Mozilla Firefox are types of Web browsers. Web browser is distinct from search engine. While Web browser facilitates access to websites based on domain name addresses, search engine is a application which helps finding information on the Web based on occurrence of certain words and phrases.. For instance, Google Chrome is Web browser and Google is search engine.

It is worth noting that the Internet is the host to various online services and it primarily refers to the network interconnecting these services. For example, the Web consists of a worldwide collection of electronic documents called Web pages, which can be accessed on the Internet with the help of Web browser[11] The Web is linked through hyperlinks and URLs.[12] Thus, Internet is the building which houses various facilities including the Web. Dark Web and Deep Web are two lesser discussed components of the Web. Dark Web is called the virtual black market.[13] It consists of sites which use anonymity tools (*e.g.* Tor and I2P Software) to mask their IP addresses and thus remain untraceable. These are publicly accessible websites that stay

7 The Number Resource Organisation, Regional Internet Registries, Available at: https://www.nro.net/about-the-nro/regional-internet-registries/ (Accessed on5 October, 2017).
8 PC Names, The Difference Between DNS and Name Servers, 2012, Available at: http://www.pcnames.com/articles/the-difference-between-dns-and-name-servers (Accessed on5 October, 2017).
9 United States Department of Commerce's National Telecommunications and Information Administration (NTIA), IANA functions, Available at: https://www.ntia.doc.gov/category/iana-functions (Accessed on5 October, 2017).
10 Mozilla Foundation, What is a Web Server?, 2017, Available at: https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_web_server (Accessed on5 October, 2017).
11 Supra note 2, Diffen.
12 URL stands for 'Uniform Resource Locator. It is a common term for 'web address'.
13 The Hindu, What is Dark Web?, 18 May, 2017, Available at: http://www.thehindu.com/sci-tech/technology/internet/what-is-dark-web/article18485139.ece (Accessed on 5 October, 2017).

anonymous by using encryption tools.[14] Anonymity software make encrypted data pass through randomly selected computers across the world before arriving at the intended destination.[15]

Thus, packets before reaching the ultimate IP address pass through multiple IP addresses making IP address of actual sender difficult to identify. It is infamous for facilitating illegal trade of drugs and pornography, although it is also used by whistleblowers such as WikiLeaks. On the other hand Deep Web is the area of the Internet which is not accessible through search engines.[16] It consists of background sites created for email accounts, password registration etc. These are not encrypted or hidden, but un-indexed Web sites or pages which can be accessed only if exact IP address is known. Dark Web is a part of Deep Web. Surface Web refers to the part of Web comprising unencrypted and indexed Websites. Thus, Web can be classified into three categories- Surface, Dark and Deep Web.

Popular websites or e-commerce platforms often rent or own physical or virtual server spaces all over the world. Since single servers do not function effectively under the pressure of high speed and large distances, network of servers across the world is used to provide seamless connection and backup at the time of failure of one or more servers. Big companies like Facebook, Google and Amazon, maintain their own data centres. Data Centres house and manage servers.[17] They are built to support various types of server farms (cluster of servers). [18]

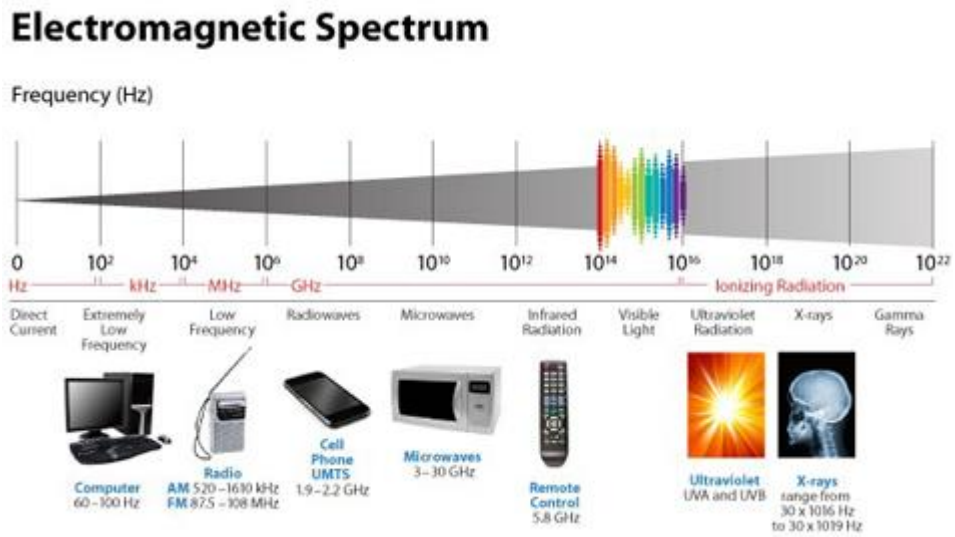
B. Physical Transmission Infrastructure

As mentioned earlier, data travels throughout the world in the form of electronic signals. These signals are a form of energy wave, specifically electromagnetic wave. Energy waves or electromagnetic radiations are classified into various bands according to their frequency and

14 Vijay Prabhu, The Dark Web explained: What lies on the Tor Accessible Dark Websites , 11 February, 2017, Available at: https://www.techworm.net/2017/02/dark-web-explained-lies-tor-accessible-dark-websites.html (Accessed on 5 October, 2017).
15 Andy Greenberg, Hacker Lexicon: What is Dark Web?, 19 September, 2014, Available at: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (Accessed on 5 October, 2017).
16 Supra note 12, The Hindu.
17 Paloalto Networks, What is a Data Center?, 2017, Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-data-center (Accessed on 5 October, 2017).
18 Maurizio Portolani and Mauricio Arregoces, Data Centre Design Overview, In Data Center Fundamentals, 2003, Cisco Press, Indianapolis, Indiana, Available at: http://www.ciscopress.com/articles/article.asp?p=102268 (Accessed on 5 October, 2017).

wavelength.[19] Whole range of electromagnetic radiations is called electromagnetic spectrum (Spectrum). Radio waves frequency band ranges from about 3,000 cycles per second or 3 kilohertz (kHz) up to about 300 billion hertz, or 300 gigahertz (GHz).[20] Band of radio waves enable electric wireless communication. It can transmit video, voice, data through TV, radio or wi-fi. Further, frequency of radio wave determines its bandwidth i.e. capacity to carry Internet data. Bandwidth is an important element. When bandwidth is not enough, IP packets do not arrive together and quality of content delivered suffers.

It must be mentioned that all data transmitted through the Internet travels through the spectrum i.e. band of electromagnetic waves whether the internet connection is wireless or wireline. However, in common parlance, spectrum is associated with wireless transmission of the data. This section discusses the types of physical channels or networks used to transmit data over Internet. In other words, it presents kinds of Inter-net (works) available. Further, hierarchy of networks is also discussed.



Source: https://www.publicknowledge.org/international-spectrum-management

Figure 1: Electromagnetic Spectrum

i. *Wireline Internet*

Majority of the Internet network is composed of undersea and land cables. Undersea cables, also known as submarine cables, form the connection between landing sites situated on various

19 Vibha Varshney et. al., All About Mobile Spectrum, Down to Earth, 15 March, 2011, Available at: http://www.downtoearth.org.in/coverage/all-about-mobile-spectrum-33106 (Accessed on 5 October, 2017).
20 Jim Lucas, What Are Radio Waves, Live Science, 6 April, 2017, Available at: https://www.livescience.com/50399-radio-waves.html (Accessed on 5 October, 2017).

continents. A landing site is a place where undersea cable reaches landmass and provides access to intra-land networks. Undersea cables transport nearly all of the transoceanic data traffic.[21] They are laid on the bottom of ocean floor and carry the world's Internet, phone calls and even TV transmissions between continents at the speed of light. A single cable can carry tens of terabits of information per second.[22] Together, they form the backbone for the data centres powering the Web.[23] Undersea cables are the data super highways and are crucial to the growth of content-rich services.[24]On land, cables further extend the Internet network. Land cables are used for backbone internet as well as for last mile connectivity to computer devices.

ii. *Wireless Internet*

If cables are highway on land and sea, then spectrum is expressway in air. Though, technically electromagnetic waves are used in wire and wireless form, here spectrum denotes its popular use in reference to wireless radio waves transmission. It is mostly used by telecommunication companies to provide cellular or mobile internet. It is a resource of limited quality and cannot be used by multiple parties at the same time. Its capacity to carry data is affected by distance travelled and frequency used. Also, if two stations transmit over the same frequency at the same time in the same area, they would cause interference with one another.[25]

In recent times, progress in digital technology and cellular applications has increased the extent of usable spectrum. Nevertheless, spectrum remains limited in quantity and requires efficient allocation and management. Spectrum management entails deciding which radio frequencies are used for which types of wireless communications and allocation of frequencies among various operators.[26] International Telecommunication Union (ITU) undertakes spectrum management at international

21 Nicole Starosielski, Why Undersea Internet Cables Still Power Our 'Wireless' World, 5 November, 2015, Available at: http://www.csmonitor.com/Technology/Breakthroughs-Voices/2015/1105/Why-undersea-Internet-cables-still-power-our-wireless-world (Accessed on 5 October, 2017).
22 Ibid.
23 Nokia, Crossing Oceans to Connect the Planet, 2017, Available at: https://networks.nokia.com/solutions/submarine-networks (Accessed on 5 October, 2017).
24 Ibid.
25 Marguerite Reardon, Wireless spectrum: What it is, and Why You Should Care, 13 August, 2012, Available at: https://www.cnet.com/news/wireless-spectrum-what-it-is-and-why-you-should-care/ (Accessed on 5 October, 2017).
26 Ibid.

level through multi-stakeholder model and national telecommunications ministry/agency perform this function in their respective countries.[27]

Spectrum (wireless) is used for providing wi-fi, satellite internet and mobile internet. Wi-fi networks use unlicensed spectrum- electromagnetic frequencies that are available for anyone to use without charge.[28] It has limited range and therefore is used in a small area such as a house. Satellite internet uses satellite to transmit radio signals. It is useful in remote areas, but has limited utility due to slow speed and high cost.

Cellular networks use licensed spectrum and cover long range communications. They further cover large area by transmitting from one radio tower to another. They provide internet on handheld mobile devices and hence known as mobile internet. Over the years, various technologies have developed for transmission of mobile internet. These technologies are indicated in form of successive generations- 2G (2nd generation), 3G (3rd generation), 4G (4th generation) and 5G (5th generation). Each generation is based on standards developed by Standard Setting Organisations (SSOs) such as European Telecommunications Standard Institute (ETSI) and Institute of Electrical and Electronics Engineers (IEEE).[29] SSOs are voluntary associations of market participants where standard is decided on the basis of consensus.[30] Major features of successive generations of cellular technologies are listed in the **Table 1.** Mobile Internet is a key factor in the success of e-commerce. It is evident from the fact that over 41 percent of the e-commerce market is driven by mobile traffic.[31] Mobile Internet penetration worldwide has doubled from 18 percent in 2011 to 36 percent

27 International Telecommunication Union, What Does ITU do?, Available at: http://www.itu.int/en/about/Pages/whatwedo.aspx (Accessed on 5 October, 2017).
28 Timothy B. Lee ed. The Internet, Explained, 14 May, 2015, Available at: https://www.vox.com/cards/the-internet/how-does-wireless-internet-work (Accessed on 5 October, 2017).
29 Jorge L. Contreras, Patents and Internet Standards, GCIG Paper No. 29, 15 April, 2016, Centre for International Governance Innovation, Ontario, Canada.
30 Kirti Gupta, Technology Standards and Competition in the Mobile Wireless Industry, George Mason Law Review, 22, 865-896, 2015.
31 The Indian Express, Mobile Internet Driving India's E-commerce: Mary Meeker Report's Big Highlights, 29 May, 2015, Available at: http://indianexpress.com/article/technology/tech-news-technology/mary-meeker-report-these-slides-confirm-that-in-india-mobile-internet-is-the-driving-force/ (Accessed on 5 October, 2017).

in 2017.[32] Further, it is predicted that by 2017, mobiles will account for almost 60 percent of all spending on Internet access.[33]

iii. *Broadband Internet*

Broadband is a very commonly used term in reference to the Internet with a certain level of bandwidth capacity. Recommendation I.113 of the ITU Standardization Sector defines broadband as a "transmission capacity that is faster than primary rate Integrated Services Digital Network (ISDN) at 1.5 or 2.0 Megabits per second (Mbits)".[34] It combines connection capacity (bandwidth) and speed; in other words, ability to carry large volumes of data at a high speed.[35] It allows websites, text, graphics, music and videos to be experienced in real time. It can be provided through Wireline Internet (optic fibre cable or copper cable) or through wireless Internet (mobile, satellite etc.). [36] Wireline broadband is available at a fixed location whereas wireless broadband is not restricted to one location. Though wireless broadband provides mobility, fixed broadband is more reliable in terms of consistency of quality signals. Wireless broadband may partly use cables. It first connects through a cabled connection and then broadcasts that connection using wireless radio waves (part of spectrum).[37] Broadband's ability to transfer large amount of data at faster speed makes it an essential component for e-commerce infrastructure.[38]

As mentioned above, there are various channels of data transmission over the Internet. Mobile internet and broadband internet can be categorised significant factors in the growth of e-commerce. Mobility, accessibility and increased capacity to provide content-rich services contribute to the

32 Wolfgang Bock et. al., The Growth of the Global Mobile Internet Economy: The Connected World, 10 February, 2015, BCG Perspectives, Available at: https://www.bcgperspectives.com/content/articles/telecommunications_connected_world_growth_global_mobile_internet_economy (Accessed on 5 October, 2017).
33 Ibid.
34International Telecommunication Union, The Birth of Broadband, Frequently Asked Questions, September 2003, Available at: https://www.itu.int/osg/spu/publications/birthofbroadband/faq.html (Accessed on 5 October, 2017).
35 Ibid.
36 Alok Vats, 4 Different Types of Broadband Technology, 3 February, 2011, Available at: http://www.techacid.com/2011/02/03/4-different-types-of-broadband-technology/ (Accessed on 5 October, 2017).
37 Guy McDowell, Types of Internet Access Technologies Explained, And What You Should Expect, 22 September, 2014, Available at: http://www.makeuseof.com/tag/types-of-internet-access-technologies-explained-and-what-you-should-expect/(Accessed on 5 October, 2017).
38 Organisation for Economic Co-operation and Development, Broadband and the Economy, Ministerial Background Report, DSTI/ICCP/IE(2007)3/FINAL, Available at: https://www.oecd.org/sti/ieconomy/40781696.pdf (Accessed on 5 October, 2017).

significance of mobile and broadband Internet. Thus, in order to develop a booming e-commerce ecosystem, substantial investment in these two areas is necessary.

Table 1: Mobile Internet Technologies

Generation	Signal and Technology	Data Transfer Capability	Standard Used
1G	Analog Signal or Analog Electric Signal	No data transfer of text messages	
2G	Digital Signal *Time Division* - allowed multiple users to access the same frequency channel; *Code Division Multiple Access*- allowed users to share a single communication channel of different frequencies	Internet data transfer through modems if in proximity of cell tower. **Maximum Download Speed**- From 80 Kbps to 0.3 Mbps	GPRS/ EDGE/1xRTT
3G	Circuit and Packet Switching	Enabled GPS, Video conferencing, video streaming etc. **Maximum Download Speed-** From 384 Kbps to 4.9 Mbps	UMTS (WCDMA/ HSPA/ HSPA+/ EvDO Rev. A/ EvDO Rev. B
4G	Packet Switching *Multiple Input and Multiple Output*[3] procedure: expands the capacity of a signal using multiple antennas at the transmitter and receiver Improved *Frequency Division Multiplexing (FDM)* technique which divides the available bandwidth into non-overlapping frequency sub-bands, each of which carries a separate signal.	3D TVs, HD mobile streaming and high definition gaming and synchronizing **Maximum Download Speed-** From 100 Mbps to 1 Gbps	LTE/ LTE-A/ WiMAX Rel. 1/ WiMAX Rel. 2
5G	Qualifying criteria set by Groupe Speciale Mobile Association: 1. One to 10Gbps connections to end points in the field 2. One millisecond end-to-end round trip delay 3. 1000x bandwidth per unit area 4. 10 to 100x number of connected devices 5. (Perception of) 99.999 percent availability 6. (Perception of) 100 percent coverage 7. 90 percent reduction in network energy usage 8. Up to ten-year battery life for low power, machine-type devices	Theoretical download speed of 10,000 Mbps	Formal standard not yet decided

Source: Author's compilation from sources in the footnote.[39]

39 Christina Mercer, What is 5G? Everything You Need to Know About 5G, 13 May, 2017, Available at: http://www.techworld.com/apps-wearables/what-is-5g-everything-you-need-know-about-5g-3634921/ (Accessed on 5 October, 2017).

C. Hierarchy of the Networks

Internet being a network of networks is divided into numerous separately managed networks. These networks are interconnected and controlled by private entities called Internet Service Providers (ISPs). These networks are classified into a hierarchical order depending on the amount of Internet traffic carried, reach of the network and market serviced. At the top are Tier 1 ISPs who have international reach and form the internet backbone. Their end users can be Tier 2 ISPs, individual users, companies using this backbone to interconnect their networks spread across the country or companies hosting web content on their servers.[40]

Next are Tier 2 ISPs who have regional presence and purchase transit from Tier 1 ISPs for the Internet connectivity. [41] Further down the hierarchy, Tier 3 ISPs are restricted to smaller regional areas and purchase transit from Tier 1 ISPs, but tend to focus on retail market.[42] In general, there are 3 to 4 tiers of ISPs. This network system can be compared to a grid of roads, where various interconnected national highways form backbone for traffic and connect to state highways which further connect to local roads.[43]

IP packet traffic is exchanged at points where ISPs connect to the backbone network and where two backbone networks connect with each other. Such exchange is called 'Interconnection'. Interconnection can be with or without charge. When it is without charge it is called 'Peering'. It is done in the cases where the amount data traffic coming from each of two ISPs is similar or almost similar in amount. It is generally between ISPs of same tier. On the other hand, non-peering Interconnections (i.e. for charge) is made where one ISP is delivering more data traffic than it is receiving. It is common between ISPS belonging to separate tiers. Usually, Tier 1 ISPs exchange data

40 Anuj Karnik, et. al., A Fragile Internet: Non-Technical Issues Leading to Internet Blackouts, 4 May, 2011, Interdisciplinary Telecommunications at the University of Colorado, Boulder, Available at: http://morse.colorado.edu/~tlen5710/12s/FragileInternet.pdf (Accessed on 5 October, 2017).
41 Yudhanjaya Wijeratne, The Seven Companies That Really Own The Internet, 28 July, 2016, Available at: http://icaruswept.com/2016/06/28/who-owns-the-internet/(Accessed on 5 October, 2017).
42 Logan Rivenes, What is an Internet Service Provider (ISP)?, 12 July, 2016, Available at: https://datapath.io/resources/blog/what-is-an-internet-service-provider/ (Accessed on 5 October, 2017).
43 Marguerite Reardon, Comcast vs. Netflix: Is this really about Net neutrality?, 15 May, 2014 Available at: https://www.cnet.com/news/comcast-vs-netflix-is-this-really-about-net-neutrality/(Accessed on 5 October, 2017).

exclusively through peer arrangement, Tier 2 ISPs use both peer and purchase arrangements and Tier 3 ISPs mostly through purchase agreements.[44]

D. Internet Infrastructure- Legal Concerns

At this stage, it is evident that the Internet is a fragmented space. It has multiple modes of transmission; these modes are owned and operated by multiple entities; its operational principles & standards are developed by numerous parties; and it is administered through decentralised multi-stakeholder system. Consequently, there are myriad legal issues concerning the Internet infrastructure. These issues are briefly discussed as follows:

i. *ICANN Jurisdiction*

ICANN, a private not-for profit organisation based out of California, United States of America (US), oversees the IANA functions.[45] These functions include, coordination of assignment of Internet protocol parameters, administration of DNS root zone management, allocation of Internet numbering resources and top-level domain management.[46] ICANN derived its authority from a contract with National Telecommunications and Information Authority (IANA) under US Department of Commerce. US government supervision of IANA functions was a source of apprehension for several countries. In response to international push at International Governance Forum (IGF) and to placate international concerns, US government in October 2016 transferred its supervisory power to a global multi-stakeholder community consisting of technical experts, governments and business representatives. However, international concerns have not subsided. Firstly, US agencies and private bodies still hold great sway at the newly found multi-stakeholder forum. Secondly, all ICANN functions fall under territorial jurisdiction of California State and US. If any legal dispute were to arise regarding management of DNS system, allocation of IP addresses, determination of IP parameters and standards, it will be adjudicated as per the laws of California. Thus, ICANN jurisdiction remains contentious topic at international level.

ii. *Competition Law and Policy*

Competition policy issues with respect to the Internet can be bifurcated into two kinds- one, Internet infrastructure related issues and two, Internet online usage issues.

44 Supra note 40, Wijeratne.
45 Supra note 8, US DoC NTIA.
46 Supra note 8, US DoC NTIA.

As discussed under Section II (C) Hierarchy of Networks, Internet transmission lines infrastructure is deeply stratified in nature. Further, many players (ISPs) exhibit vertical integration such that they service the wholesale and retail markets at the same time. Such market structure has tendency towards 'price or margin squeeze' practices.[47] Price or margin squeeze is defined as a practice whereby incumbent network provider charges such high wholesale price or low retail price that profit margin of competing network providers in the retail market is squeezed out.[48] This practice is either considered stand alone category of abuse of dominant position or as a type of predatory pricing. European Union (EU) courts treat price-squeeze as separate category and only require establishing that difference between the retail prices charged by a dominant undertaking and the wholesale price charged to its competitors for comparable services is negative or insufficient to cover costs of dominant operator for providing its own retail services in the downstream market. On the other hand, US courts do not consider price-squeeze a separate offence. US courts conduct examination under Section 2 of the Sherman Act to determine if low retail price is predatory or not. According to this approach high wholesale price due to lawfully acquired monopoly is not a violation of anti-trust laws. This debate remains alive in other countries as well. In the light of availability of growing African and Asian markets, Countries require a cogent policy on the issue to avoid legal and regulatory costs.

iii. *Network Neutrality*

'Network Neutrality' (Net Neutrality), a term first popularised in 2003, means that ISPs do not discriminate between different types of content.[49] It connotes that ISPs should not block or slow down the Internet traffic on their local broadband networks based on specific users or content of the Internet traffic or origin of the content.[50] It is considered an essential element of 'Open Internet' which entails that the Internet as a resource should be open and equally accessible to all individuals, companies and organizations.

47 Choi, S.M., et al., Margin Squeeze in the Internet Backbone Interconnection Market: A Case Study of Korea, Telecommunication Systems, 61, 531, 2015, Available at: https://.doi:10.1007/s11235-015-0010-0 (Accessed on 5 October, 2017).

48 Justus haucap and Torben Stühmeier, Competition and Antitrust in Internet Markets, In Handbook on the Economics of the Internet, Edward Elgar Publishing, Cheltenham, United Kingdom, p.199.

49 Tim Wu, Network Neutrality, Broadband Discrimination, Journal of Telecommunications and High Technology Law, 2, 141, 2003.

50 Supra note 42, Reardon.

In the absence of universally established definition of Net Neutrality, its breadth of application remains debatable. Blocking of content is acceptable to prevent harm to the system or user devices (e.g. virus, malware etc.) and to comply with the law (e.g. Chinese law prohibits Facebook access). In other cases, Net Neutrality has developed on a case by case basis. For instance, in 2008 Federal Communications Commission (FCC) of US found that slowing down of BitTorrent Traffic by Comcast ISP was illegal.[51] Telecom Regulatory Authority of India (TRAI) has passed a regulation prohibiting zero-rated plans which exempt particular data from user's data cap, or provide it without excess usage charges.[52] However, the most controversial area is preferential Internet traffic management. Sometimes, Content Delivery Network (CDN) providers enter into an Interconnection agreement with ISPs to deliver content from their servers (called cache server) to end user through shortest route and ensure fast delivery of their content. Further, when ISPs are content generator too, there is strong likelihood of prioritization of content from ISP over the content from other sources. Such conflict was seen in Netflix-Comcast negotiations. Netflix had its own cache server and wanted Comcast (ISP) to route its content directly to its end users. Comcast sought to charge Netflix as it would have charged any CDN whereas Netflix contended that it is a content provider and any charge by Comcast would be discriminatory. Matter was further complicated due to Comcast's merger deal with another content provider, NBC Universal. This dispute was resolved privately between the parties where Netflix agreed to pay undisclosed sum to Comcast. Netflix entered into a similar deal with Verizon ISP. Though these disagreements were resolved amicably, they ignited debate over acceptable Internet traffic management practices.

There are two schools of thought on this issue. Proponents of strict net neutrality argue that any leeway would lead to discriminatory practices by the ISPs and therefore all preferential interconnection agreements should be prohibited. However, advocates of limited net neutrality demand that complete prohibition would affect investment and innovation and interconnection cases should be dealt on case by case basis as per the competition law.

So far 'network management practices' has remained unresolved area, but the now defunct Trans Pacific Partnership (TPP) allowed 'reasonable network management' by ISPs.[53] Similar provision is

51 Although FCC order was struck down on the basis of lack of jurisdiction.
52 Telecom Regulatory Authority of India, Prohibition Of Discriminatory Tariffs For Data Services Regulations, 2016, Notification, 8 February, 2016, Rule 3 (1) And (2).
53 Article 14.10, Trans Pacific Partnership

made in Trade in Services Agreement (TISA).[54] It must be noted that currently ISPs in all the jurisdictions do undertake 'network management practices' for legitimate technical purposes. However, language of TPP and TISA does not make clear if network management practices are restricted to technical reasons or whether it extends to business or commercial reasons. There is a possibility that TPP and TISA may be interpreted to legitimise network management for commercial purpose and to this extent at international level new trade rules are opting for limited net neutrality.

iv. *Infrastructure-Sharing*

Infrastructure-sharing can be defined as joint utilization of assets and/or services necessary to provide a service.[55]In the telecommunication sector, infrastructure is categorised into passive and active infrastructure. Passive Infrastructure refers to the non-electronic infrastructure such as tower, sites, air-conditioning equipments, diesel electric generator, battery, electrical supply, technical shelters, equipment rooms, premises, security systems, billing systems, poles, ducts, trays, power system, etc.[56] Active Infrastructure refers to the active electronic infrastructure/ elements such as base tower station, microwave radio equipment, switches, antennas, spectrum, signal transceivers, antennae.[57] It is the infrastructure necessary for the reception, processing and/or transmission of telecommunication signals.[58]

Since there is a growing demand for the Internet infrastructure in the light of a booming e-commerce market, particularly in the developing countries, attention has shifted towards infra-structure sharing as a tool of fast deployment of the Internet services. Infrastructure-sharing cuts investment cost and time for the new entrants and facilitates market access in otherwise investment intensive sector. It is worth noting that in cases where developing countries have not undertaken market access commitments in the telecommunication services sector under the GATS Schedule of Commitments, infrastructure-sharing allows alternative route for market access in the sector.

So far countries have been using an array of approaches towards infrastructure-sharing, depending on the maturity of domestic market, extent of competition and consumer interest. In some

54 Article 8, Trade in Services Agreement (TISA) Provisions (Leaked Text)
55 Jose Marino Garcia and Tim Kelly, The Economics and Policy Implications of Infrastructure Sharing and Mutualisation in Africa, Background Paper (World Development Report: Digital Dividends), 2016, World Bank Group.
56 Ibid
57 Ibid.
58 Ibid.

countries, infrastructure sharing is not restricted, i.e., is permitted, whereas in other countries, it is absolutely prohibited. While in certain countries, the telecom regulator may permit sharing of certain type of infrastructure (such as, in passive) while prohibiting sharing of the other type of infrastructure (that is, active). Apart from these, certain countries have gone a step further and required mandatory sharing of infrastructure (either passive or active or both) by incumbent operators with new operators, whereas certain other countries have deferred to market choice in sharing of infrastructure.[59]

TPP provides push for mandatory infra-structure sharing. Such approach may be premature as further research is necessary to convincingly establish the implications of mandatory infrastructure sharing on competition, investment and innovation.[60]

v. *Interoperability*

The Oxford dictionary defines interoperability as the ability of computer systems or software to exchange and make use of information.[61] It means the ability of information systems to work with each other because their interfaces are completely understood even when individual components are technically different and managed by different organizations.[62]It is a wide meaning and the actual implication depends on the context of the application. For instance, two Web browsers are interoperable when a Webpage or Website can be accessed through both of them[63] or two Internet networks are interoperable if the Internet data is exchanged between them without additional outside support. Similarly, two or more interoperable eHealth systems use and exchange computer interpretable data and human understandable data and knowledge.[64]

59 Jayant Raghu Ram, When Sharing Ins't Always Caring: Understanding telecom Infrastructure Sharing in the Multilateral Context, Working Paper WP/CWS/200/38, 2017, Centre for WTO Studies, Indian Institute for Foreign Trade, New Delhi.

60 Supra note 54, Garcia and Kelly.

61 English Oxford Living Dictionaries, Interoperability, 2017, Available at: https://en.oxforddictionaries.com/definition/interoperability (Accessed on 5 October, 2017).

62 Agosti, D. et al., 2016. Legal Interoperability of Research Data: Principles and Implementation Guidelines. s.l.:RDA-CODATA Legal Interoperability Interest Group.

63 World Wide Web Consortium (W3C), WIP -- The Web Interoperability Pledge, 1999, Available at: https://www.w3.org/Promotion/WIP/ (Accessed on 5 October, 2017).

64 eHealth Governance Initiative, Discussion Paper on Semantic and Technical Interoperability, 2012, Available at: https://ec.europa.eu/health//sites/health/files/ehealth/docs/ev_20121107_wd02_en.pdf (Accessed on 5 October, 2017).

In the context of the Internet infrastructure, interoperability can be examined under two heads: a) technological interoperability and b) legal interoperability.

a. *Technological Interoperability* as typically used by the computer and information science communities, includes technical, syntactic and semantic interoperability.[65] *Technical* interoperability is usually associated with hardware and software components, systems and platforms that enable machine-to-machine communication.[66] *Syntactic* interoperability is usually associated with data formats and provides for the exchange of clearly defined classes of data.[67] *Semantic* interoperability is concerned with ensuring that the precise meaning of exchanged information is understandable by any other application and is the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results.[68]

Standards development is an inextricable part of technological interoperability. The general opinion is that open standards promote interoperability as they are publicly available and developed via processes that are transparent and open to broad participation.[69] In contrast, proprietary standards which are privately owned by one or more entities that control their distribution and access; make interoperability difficult to achieve and costly process.[70] Open standards help guard against large technology companies' pushing the adoption of their own "standards" in a way that reinforces their market dominance and limits choice for others.[71] In fact, the European Commission Decision of March 24, 2004 found Microsoft's refusal to supply interoperability information to other market participants to be a violation of Article 82 of the European Treaty prohibiting the abuse of a dominant position.[72]Moreover, the Internet is founded upon an open and interoperable structure and this characteristic is instrumental for the global nature of the Internet and Internet-enabled technologies. Therefore, interoperability of

65 Agosti, D. et al., Legal Interoperability of Research Data: Principles and Implementation Guidelines, 2016., RDA-CODATA Legal Interoperability Interest Group.
66 Ibid.
67 Ibid.
68 Ibid.
69 Internet Society, Open Internet Standards, Policy Brief, 30 October, 2015, Available at: https://www.internetsociety.org/policybriefs/openstandards (Accessed on 5 October, 2017).
70 Ibid.
71 Open ePolicy Group, Roadmap for Open ICT Ecosystems, 2005, Available at: http://cyber.law.harvard.edu/epolicy/roadmap.pdf (Accessed on 5 October, 2017).
72 European Committee for Interoperable Systems, Interoperability & Competition law, Available at: http://www.ecis.eu/interoperability-competition-law/ (Accessed on 5 October, 2017).

the Internet systems is instrumental in achieving development goals. It is also acknowledged by IGF, UNCTAD, OECD etc., that thrust should be towards adopting open standards.

b. *Legal interoperability* addresses the process of making legal rules cooperate across jurisdictions, on different subsidiary levels within a single state or between two or more states.[73] According to Rolf H. Weber there are various regulatory modes of achieving interoperability between different legal systems, namely, harmonization, standardisation, mutual recognition, reciprocity and cooperation.[74]

Harmonization depicts the process of the unification of law achieved through treaties, self-regulations etc.[75] Standardization is usually defined as a regulatory approach that is based on widely accepted good principles, practices or guidelines in a given area.[76]In the area of Internet infrastructure, international level of standardisation is done through the SSOs. Most SSOs are established as private entities (for example, as associations) and composed of national standards bodies; in the cyberspace field, the ITU is an exception as a treaty based organization established as a permanent agency of the United Nations and driven by national governments as the primary members.[77] Mutual recognition accepts another state's regulation as satisfactory and acknowledges that different national requirements can be interchangeable in order to be domestically applied.[78]Reciprocity is attained through commitments undertaken bilaterally.[79] Cooperation is manifested through collective regulatory rules or coordination between agencies with respect to designing, applying and enforcing different regulatory issues.[80]

The current legal system governing e-commerce and internet based technologies is fragmented into various domestic jurisdictions, however there is a push towards establishing legal interoperability.[81] It

73 Rolf H. Weber., Legal Interoperability as a Tool for Combatting Fragmentation,, GCIG Paper No. 4, December 2014, Centre for International Governance Innovation, Ontario, Canada.
74 Ibid.
75 Ibid.
76 Ibid.
77 Ibid.
78 Rolf H. Weber, Mapping and Structuring International Financial Regulation — A Theoretical Approach, European Banking Law Review 20 (5), 651–88, 2009.
79 Supra Note 72, Weber.
80 Supra note 77, Weber.
81 Luca Belli and Nathalia Foditsch , Network Neutrality: An Empirical Approach to Legal Interoperability, Thermoplastic composites Research Center, 43: The 43rd Research Conference on Communication, Information and

is argued that legal interoperability drives innovation, competition, trade and economic growth.[82] However, legal interoperability should not be confused with legal uniformity. It refers to the cooperation between different legal systems and does not stand for single legal system. Thus, while pursuing for legal interoperability a few points should be considered. First, interoperability should not overlook country specific needs and challenges. Second, interoperability should aim towards creating a level-playing field for all. Third, the degree of legal interoperability depends on the material issue at stake. For example, harmonized legal rules are important for the implementation of the Domain Name System (DNS); however, less unification appears to be needed in the field of cultural expression.[83]

Ultimate objective of technological and legal interoperability should be defragmentation of the Internet infrastructure and rules governing it, while ensuring equitable development.

Internet Policy Paper, 31 March, 2015, Available at: http://dx.doi.org/10.2139/ssrn.2588572 (Accessed on 5 October, 2017).

82 John Palfrey and Urs Gasser. Introduction in Interop: The Promise and Perils of Highly Interconnected Systems, Persens Books Group, New York, 2012, Available at: http://cyber.harvard.edu/sites/cyber.harvard.edu/files/Interop-PalfreyGasser-Introduction.pdf (Accessed on 5 October, 2017), p.8.

83 Supra note 72, Weber.

III. DATA FLOW- CONCEPT AND APPLICATIONS

Preceding section discussed what the Internet-highways are, and how they are made and operated. This section now studies the traffic moving on those highways. As mentioned in the previous section, Internet carries data (in the form of text, audio, video etc.) from one point to the other. This movement is labelled "data flow". Data flow is the cornerstone of e-commerce growth. Selling and delivering services, collecting payment, and receiving consumer feedback (with or without consumer's active participation) all involve data flow. This section examines what are the constituents of data-flow and how it is used by consumers, businesses and governments. It identifies the meaning and type of data, understands data analytics and lists services based on data-flow.

A. Data- Meaning and Types

Data has earned monikers like the new oil, new currency and lifeblood of the digital economy. There is no exhaustive definition of data. In a general sense, it is described in terms of numbers, characters, symbols, images, sounds, and electromagnetic waves, bits – that constitute the building blocks from which information and knowledge are created.[84] In the context of digital world, data can be understood as all the information generated and collected during an online activity. It includes information directly provided by the user; information indirectly and automatically produced regarding sites visited, time spent online, products bought and sold etc.; and information produced upon analysis of direct and indirect information.

Data can be classified into various categories on the basis of source, nature and method of collection:

i. Data can be distinguished into *captured data* and *exhaust data* on the basis of the source. *Captured data* is the deliberate product of measurement i.e. information intentionally and directly captured such as name, address, credit card details etc.[85] On the other hand, *exhaust data* is a by-product of the main function rather than the primary product i.e. online imprint left by the user in the form of websites visited, videos watched, posts liked etc.[86]

84 Rob Kitchin, Conceptualizing Data, In The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences, SAGE Publications, 2014.
85 Ibid.
86 Ibid.

ii. Based on the method of collection data is categorised into *active* and *passive data. Active* user data collection, involves explicitly asking users for information, preferences, and opinions. While users are often reluctant to enter information due to time and privacy issues, if the Websites can offer some service or product in return for the information, users may be compelled to provide some level of information to the site.[87] It is also called *volunteered data.*[88] In contrast, *passive data* is the trail of data produced automatically during an online activity. It is a by-product of everyday technological existence. *Passive data* collection requires no explicit action on the user's part and in fact, user often has little awareness of the data collection effort. It uses the interactions between Web clients and servers to collect and store information about the user actions or reactions to information provided on a Web site. As a result, this information – and its intrinsic monetary value – often goes unnoticed by Internet users.[89] It is also known as *automated data.*[90] In short, *automated data* is generated as an inherent, automatic function of the device or system, whereas volunteered data is traded or gifted by people to a system.[91]

iii. Based on the nature of the data, it is categorized into *personal* and *non-personal* data. European directive defines *personal data* as "any information relating to an identified or identifiable natural person ("data subject")".[92] It further defines identifiable person as one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[93] *Non-personal data* is data which does not lead to identification of a particular person. *Personal data* is considered sensitive data due to deep ramification of its misuse.

iv. Another category of data is *Big Data.* As per Rob Kitchin, any data is classified as *Big Data* if it possesses these characteristics- huge volume, consisting of terabytes or petabytes of data;

87 Massachusetts Institute of Technology, Data Collection: Defining the Customer, Available at: http://web.mit.edu/ecom/www/Project98/G2/data.htm (Accessed on 5 October, 2017).
88 Supra note 83, Kitchin; David Lyon, Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique, Sage Journals, 1(2), 9 July, 2014, Available at: http://journals.sagepub.com/doi/full/10.1177/2053951714541861 (Accessed on 5 October, 2017).
89 Nathan Eagle, Who Owns the Data You Generate Online?, 11 October, 2014, Available at: https://www.weforum.org/agenda/2014/10/digital-footprint-data-mining-internet/ (Accessed on 5 October, 2017).
90 Supra note 83, Kitchin.
91 Supra note 83, Kitchin.
92 Council Directive1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.
93 Ibid.

high velocity, being created in or near real time; extensive variety, both structured and unstructured; exhaustive in scope, striving to capture entire populations of systems; fine-grained resolution, aiming at maximum detail, while being indexical in identification; relational, with common fields that enable the conjoining of different data-sets; flexible, with traits of extensionality (easily adding new fields) and scalability (the potential to expand rapidly).[94] The key features of *Big Data* are three Vs – volume, velocity and variety.[95] That is, data must be huge in volume, collected at rapid velocity in real time and contains information from wide variety of sources. Radical expansion and integration of computation, networking, digital devices and data storage has provided a robust platform for the explosion in big data, as well as being the means by which big data are generated, processed, shared and analysed. [96]

It is important to note that *Big Data* and *personal data* do not always overlap. If *Big Data* sources personal information such as credit card details, user name, location, and health record it is called *personal Big Data.* On the other hand, *Big Data* may purely comprise of non-personal data like traffic data, astronomical data, weather and climate data, and crop pattern data and is not attributed to single entity or person.

Big data related activities can lead to privacy breach i.e. identification of an individual in three scenarios:

i. If it contains *personal data.*
ii. If *personal data* contained in *Big Data* is not sufficiently anonymised. Here 'anonymised' means making it impossible to identify an individual from the data itself or from that data in combination with other data, taking account of all the means that are reasonably likely to be used to identify them.[97]If anonymisation is not sophisticated enough, re-identification tools can be used to reverse it.

94 Supra note 83, Kitchin.
95 Supra note 83, Kitchin.
96 Supra note 83, Conceptualizing Data, In The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences.
97 United Kingdom Information Commissioner's Office, Big Data, Artificial Intelligence , Machine Learning and Data Protection, 2017, Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (Accessed on 5 October, 2017) p.58.

iii. *Personal data* may be obtained by combining separate anonymous *Big Data* sets.[98]

In recent years, use of *Big Data* has increased considerably in private and public sector. Major beneficiaries of *Big Data* are public sector services, healthcare sector, insurance services, transportation services and banking sector.[99] It is used to analyze claims and transactions in real time, identifying large-scale patterns across many transactions or detecting anomalous behaviour from an individual user, to detect fraud.[100]It also uses data collected from social media to provide real-time insights into how the market is responding to products and campaigns. With those insights, companies adjust their pricing, promotion, and campaign placement on the fly for optimal results.[101] Companies such as DataSift provide marketing insights by collecting data from Twitter (via Twitter's GNIP service), Facebook and other social media.[102] *Big Data* is also used for keeping patient history, disaster response and preparedness, traffic management, preparing population estimates etc.[103]

v. All the above types of data are used to produce *derived* and *inferred data.*[104] It is interpretive data produced by analyzing *automated*, *volunteered* and/or *Big Data.* While *derived data* is produced from other data through simple methods of calculation and interpretation, *inferred data* is produced by using more complex methods to find correlations between datasets.[105] *Inferred data* is used for profiling users and predicting future trends.[106]

B. Data Analytics

98 Supra note 96, UK Information Commissioner's Office, p.14.
99 Intellipat, 7 Big Data Examples- Application of Big Data in Real Life, Available at: https://intellipaat.com/blog/7-big-data-examples-application-of-big-data-in-real-life/ (Accessed on 5 October, 2017).
100 Ingram Micro, Four Powerful Big data Application Examples, February 2017, Available at: http://www.ingrammicroadvisor.com/data-center/four-powerful-big-data-application-examples (Accessed on 5 October, 2017).
101 Ibid.
102 Mayer-Schönberger, Viktor and Cukier, Kenneth,, Chapter 2 More, In Big data: A Revolution That Will Transform How We Live, Work and Think. John Murray, London, 2013, p.92.
103 Supra note 99, Micro; Nigel Swier, Bence Kormaniczky, and Ben Clapperton, Using geolocated Twitter traces to infer residence and mobility, Office of national Statistics, United Kingdom, Available at: www.ons.gov.uk/ons/guide-method/method-quality/specific/gss-methodology-series/-41-powerpoint-twitter-traces.ppt%3Fformat%3Dhi-vis+&cd=2&hl=en&ct=clnk&gl= (accessed on 5 October, 2017).
104 World Economic Forum, Personal Data: The Emergence of a New Asset Class, 2011, Available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed on 5 October, 2017); Martin Abrams, The Origin of Personal Data and its Implications for Governance, 21 March, 2014, Available at: http://dx.doi.org/10.2139/ssrn.2510927 (accessed on 5 October, 2017).
105 Supra note 96, UK Information Commissioner's Office, p.13.
106 Ibid

Data in itself is not valuable unless it is processed and converted into actionable results. The value derived from *Big Data* is partially a function of amount of data created, but more due to ability to use that data in real time to make smarter, more efficient decisions.[107] This ability comes from data analytics. *Data analytics* is a sub-area of *Big Data* which comprises of process of converting raw data into valuable resource.[108] It can be described as taking *Big Data* and creating predictive model to obtain actionable insights. Companies and governments then base their decision on such insights.
Rob Kitchin lists four types of data analysis, namely data mining and pattern recognition; data visualisation and visual analytics; statistical analysis; and prediction, simulation and optimisation.[109]

i. *Data Mining and Pattern Recognition*

Data mining is the process of extracting data and patterns from large datasets.[110] After extraction, processes like machine learning are used to detect, classify and segment relationships, associations and trends between data variables. It refers to algorithms which enable computers to automatically analyse complex datasets and continuously learn and adapt its analysis.[111] It is a branch of artificial intelligence.[112]

Advertising agencies, marketers and financial services use the results of data mining and pattern recognition to identify emerging trends and leverage them for economic gains. According to the Data-Driven Marketing Institute, the data-mining industry generated $156 billion in revenue in 2012 – roughly $60 for each of the world's 2.5 billion internet users[113]

ii. *Data Visualisation and Visual Analytics*

It refers to visual representation of patterns, relationships etc. Traffic management, weather forecast, stock market trends, electricity demand are few of the examples of visual analytics. It helps in converting the results of analysis into simple terms which can be understood by the ultimate users.

107 Alec Ross, Data: The Raw Material of the Information Age in The Industries of the Future (Simon & Schuster, London, 2017) p. 155.
108 Domingue J., Lasierra N., Fensel A., van Kasteren T., Strohbach M., Thalhammer A., Big Data Analysis in New Horizons for a Data-Driven Economy, Cavanillas J., Curry E., Wahlster W. (eds) (Springer, Cham, 2016).
109 Supra note 83, Kitchin.
110 James Manyika et al., Big data: The next frontier for innovation, competition, and productivity, McKinsey Global Institute, May 2011, p.28; Supra note 83, Chapter 6: Data Analytics.
111 SAS Institute Inc., Machine Learning: What it is and why it matters, Available at: https://www.sas.com/en_us/insights/analytics/machine-learning.html (accessed on 5 October, 2017).
112 Supra note 83, Kitchin..
113 Nathan Eagle, Who owns the data you generate online?, World Economic Forum, 1111 October 2014, Available at: https://www.weforum.org/agenda/2014/10/digital-footprint-data-mining-internet/(accessed on 5 October, 2017).

iii. *Statistical Analysis*

It seeks to explain the patterns and relationships between various datasets.

iv. *Prediction, Simulation and Optimisation*

These are used to predict the trends in the market and society. For example, Target store is able to know if someone is pregnant on the basis of consumers shopping habits.[114]

A discussion on data analytics is incomplete without examining *artificial intelligence (AI).* AI is also a method of data analytics. However, it stands apart from other methods due to its ability to learn from the data in order to respond intelligently to new data and adapt its outputs accordingly.[115] This unique ability enables AI to cope with the analysis of big data in its varying shapes, sizes and forms.[116]

Its objective is to make informed choices and conduct tasks after analyzing the repercussions of choices like a human being. Like all software, AI works with the data provided through an interface of a data source and a pre-determined algorithm. These algorithms are created with the help of machine learning. Machine learning is defined as "…the set of techniques and tools that allow computers to 'think' by creating mathematical algorithms based on accumulated data."[117] Thus, machine learning is a tool to create AI. Further, the amount of data created plays a great role in the efficiency of AI. As the amount of data that informs AI grows exponentially, AI will grow exponentially more accurate and be able to parse the smallest detail.[118] Thus, the complexity of the input source and the sophistication of the algorithm are the deciding factors in the development of an AI system.

114 Charles Duhigg, How Companies Learn Your Secrets, The Nye York Times Magazine, February 16, 2012, Available at: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp (accessed on 5 October, 2017).
115 International Data Group, The Outlook for Big Data and Artificial Intelligence (AI), 11 November, 2016, Available at: https://idgresearch.com/the-outlook-for-big-data-and-artificial-intelligence-ai/(accessed on 5 October, 2017).
116 Supra note 96, UK Information Commissioner's Office, p.7.
117 Deb Miller Landau, Artificial Intelligence and Machine Learning: How Computers Learn, IQ, 2 September, 2016, Available at: https://iq.intel.com/artificial-intelligence-and-machine-learning/ (accessed on 5 October, 2017).
118 Supra note 106, Ross, p. 158.

There are two types of AI- narrow and general. Narrow or weak AI is designed to perform narrow tasks such as facial recognition or internet searches. However, the long-term goal of the field of AI is to create general AI (AGI or strong AI). While narrow AI may outperform humans at specific tasks like chess or mathematical equations, AGI, if materialized, is expected to outperform humans at nearly every cognitive task.[119]

The design of an AI system has been outlined to imitate the workings of a human brain. This involves a complicated mix of various disciplines such as Computer Science, Biology, Psychology, Linguistics, Mathematics, and Engineering.[120] In order to make a machine replicate the reasoning, learning and problem solving abilities of a human brain, scientists have been trying to replicate in machine code the way a human brain produces new neural networks as a person learns a new skill, performs multiple tasks simultaneously and prioritizes them.[121]

The business of information management—helping organisations to make sense of their proliferating data—is growing by leaps and bounds. In recent years Oracle, IBM, Microsoft and SAP between them have spent more than $15 billion on buying software firms specialising in data management and analytics. This industry is estimated to be worth more than $100 billion and growing at almost 10% a year, roughly twice as fast as the software business as a whole.[122]Data companies are involved both in managing a physical layer (storage and processing) and a digital layer (non-trivial data collection, interpretation and actionable data production).[123] This sector has immense scope of growth as currently 56% of the companies do not have the right systems to capture the data they need or are not collecting useful data, and 66% lack the right technology to

119 Future of Life Institute, Benefits & Risks of Artificial Intelligence, Available at: https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/ (accessed on 5 October, 2017).
120 Tutorials Point, Artificial Intelligence: Overview, Available at: https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_overview.htm (accessed on 5 October, 2017).
121 Torah Kachur, Human Brain Structure Inspires Artificial Intelligence, CBC News, 29 June, 2017, Available at: http://www.cbc.ca/news/technology/human-brain-inspires-artificial-intelligence-1.4183556 (accessed on 5 October, 2017).
122 The Economist, Data, data everywhere, 25 February, 2010, Available at: http://www.economist.com/node/15557443 (accessed on 5 October, 2017).
123 Jean-Baptiste Dumont, The Data Revolution, Tech Crunch, 6 October, 2016, Available at: https://techcrunch.com/2016/10/06/the-data-revolution/ (accessed on 5 October, 2017).

store and access data.[124] Data analytics sector needs to overcome these hurdles to make full use of *Big Data opportunities.*[125]

124 Rasmus Wegner and Velu Sinha, The Value of Big Data: How Analytics Differentiates Winners, Bain & Company, 2013, Available at: http://aabdp.org/BAIN%20_BRIEF_The_value_of_Big_Data.pdf (accessed on 5 October, 2017).
125 Supra note 83, Kitchin.

C. Data - Uses

After discussing various types of data and how they are analyzed to generate actionable products, this section lists a range of new and emerging data-based online services. Data collection and analysis is intrinsic to these applications. These applications have developed due to the Internet's ability to transfer data from one point to another. This section also briefly mentions legal concerns attached to each of these applications. Data-flow based applications are as follows:

i. *Internet of Things*

Internet of Things (IoT) is about connecting devices over the internet, letting them talk to users, and each other.[126] It entails conversion of 'dumb' devices into 'smart' ones with the help of computer software. IoT is a term used to define the network of connected "smart" devices, i.e., devices embedded with sensors, software, electronics and network connectivity which have the capacity to collect and exchange data. The 'smart' device has a programmed awareness and an ability to make autonomous and automatic decisions from a suite of defined choices through the deployment of algorithms on produced data.[127] It does so with the help information technology. Recently trend of smart devices using AI has risen and in future all devices may incorporate AI element.

IoT is the convergence of Operational Technology (OT) and Information Technology (IT). OT refers to the hardware and software that controls the performance of physical devices.[128] Traditional OT is restricted to the pre-programmed functions embedded in the device. Such as, air conditioner (AC) functions according to the cooling settings already fed in the device. In contrast, OT when coupled with IT acquires ability to interact with other devices. A 'smart' AC is connected to the user's mobile device and can switch on or off according to location of the paired mobile device.

The 'smart' device which has been fitted with a sensor constantly records and monitors its surroundings. The device's processors do not usually have the capacity to analyze and process the data. The accumulated data is, therefore, sent to the manufacturer's central database where the

126 Nicole Kobie, What is the Internet of Things?, The Guardian, 6 May, 2016, Available at: https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google

127 Martin Dodge and Rob Kitchin, The Automatic Management of Drivers and Driving Spaces, Geoforum, Vol. 38, Issue 2, March 2007, 264-275.

128 Gartner IT Glossary, Operational Technology (OT), Available at: http://www.gartner.com/it-glossary/operational-technology-ot (accessed on 5 October, 2017).

necessary analyses are performed. AI or other kinds of technologies are used for data analysis and developing insights. IoT devices are the source of observed data, while derived and inferred data are produced by the process of analysing the data.[129]A decision prompt is then sent back to the smart device. As the new data collected by the smart device is constantly available to be taken into account, the prompt is accordingly altered.

The future of IoT looks very promising and it has wide range of applications for both the consumers and businesses. But there remain several technical, legal and ethical challenges. As early as in 2008 a European Commission's Staff Working Document identified policy challenges for IoT, namely, security, privacy, data protection, control of critical global resources, subsidiarity, identity management, naming, interoperability, fostering innovation, spectrum and standardization.[130] These matters still hold challenge for all the stakeholders- governments, businesses and consumers.
Some key legal issues that are involved are briefly discussed here. *First* major issue is *data security*. As the smart devices are always connected to the Internet for information and system updates, there is a possibility of the devices being 'hacked'. Hacking is defined as the unauthorized interception of computer-based information.[131] Hacker can steal data or deny access to the smart device or spam the user. Such threats can go beyond being a simple menace to economic safety and can endanger national and international security.[132] *Second,* continuous connection to the internet increases the risk of a spontaneous machine malfunction, which, in case of machines such as household heating, can cause *physical danger* to the user.[133] *Third*, without sufficient data protection measures *consumer privacy* is vulnerable to violation. The devices have access to sensitive information such as present location, preferences and personal information of the user through the connected mobile devices. Moreover, in the case of some manufacturers, the data processing for the equipment is not conducted directly by the manufacturer or a subsidiary. It is instead outsourced to a third party who may not adhere to the privacy policy sworn by the manufacturer. This leads to the risks of third party infiltration, data

129 Supra note 96, UK Information Commissioner's Office, p.9.
130 European Commission, Future networks and the Internet: Early Challenges regarding the "Internet of Things", Commission Staff Working Document Accompanying Document To The Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, SEC(2008) 2516 , Brussels, 2008, Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008SC2516&from=en (accessed on 5 October, 2017).
131 Cybercrime Organisation, Data Theft Definition, Available at: http://cybercrime.org.za/data-theft/(accessed on 5 October, 2017).
132 Rolf .H. Weber and Romana Weber, Internet of Things: Legal Perspectives, (Springer- Verlag GmbH Berlin Heidelberg, 2010)
133 Nisrag Desai, IT vs. OT for the Industrial Internet- Two Sides of the Same Coin, 27 April, 2016, Available at: https://www.globalsign.com/en/blog/it-vs-ot-industrial-internet/(accessed on 5 October, 2017).

theft and unauthorized resale. In this aspect, European Commission has explored the right to "silence of the chips" i.e. individuals should be able to disconnect from their networked environment at any time, to limit the threat to privacy.[134] *Fourth*, IoT suffers from *standardisation* issues. At present IoT developers are using varied standards. In the IoT sphere, the eXtensible Messaging and Presence Protocol (XMPP), the Constrained Application Protocol (CoAP) and Message Queue Telemetry Transport (MQTT) are major protocols to communicate between the objects.[135] A new organisation called oneM2M is developing specifications to ensure the global functionality of M2M-allowing a range of industries to effectively take advantage of the benefits of this emerging technology[136] This exercise is critical because lack of standards for sound data protection directly contributes to data security and privacy susceptibility. It further aggravates the technological interoperability problem. *Fifth*, *spectrum policy* of various countries and ITU will have to accommodate IoT. Globally, the trend is to use telecom network of Telecom Service Providers (TSPs) and/ or free wireless bands in non-TSP frequency domains for M2M communications.[137] But with the enhanced use of IoT, the need for additional spectrum will multiply too. Countries have to review their infrastructure-sharing policy and net-neutrality principles with regard to spectrum and Internet infrastructure. The availability of White Space (unused frequency of the wireless spectrum) will have an influence of how M2M/IoT evolves, while there are licensing issues related to the use of alternative technologies such as Low Power Wide Area (LPWA) networks.[138]

ii. *3-D Printing*

Three dimensional (3D) printing is the process of creating three dimensional objects in which the material is layered in thin coats to form the desired object. This procedure is technically termed Additive Manufacturing because material is added to the object as opposed to conventional production processes which employ subtractive processes such as milling, cutting, drilling and

134 European Commission, Internet of Things: An Action Plan for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2009/0278 final, 18 June, 2009, Available at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52009DC0278 (accessed on 5 October, 2017).
135 Immanuel Kim, The Internet of Things: A Reality Check for Legal Professionals, Law Practice Today, 14 January, 2016, Available at: http://www.lawpracticetoday.org/article/the-internet-of-things-a-reality-check-for-legal-professionals/ (accessed on 5 October, 2017).
136 Ibid.; India Ministry of Communications & Information Technology, Department of Telecommunications, National Telecom M2M Roadmap, May 2015, Available at: http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf (accessed on 5 October, 2017) p. 13.
137 Ibid., p. 9.
138 Ibid., p. 17.

machine to manufacture the final design. The procedure by which the material is layered classifies the technology. Fused Deposition Modelling, where the material is passed through a melted nozzle that heats it and is then extruded according to a pre-specified software code. Digital Light Processing (DLP), where a platform is submerged into built resin and the light source controlled by the machine maps every layer of the object into the platform and solidifies it. The software CAD (Computer Aided Design) is used with varying degrees of complexity according to the material used in the prototype and the complexity of its design. The most common being a STL (STereoLithography) file format which allows the user to incorporate a "repair" code into the program to allow for revision in case of failure. Some examples of changes in the printers include using lasers and electron beams in place of ultra-violet (UV) or white lighting in the case of DLP.
3D printing has had a substantial rise in commercial use with companies using the printers to produce varied prototypes to finalize the final model that would be approved for mass production. It has also found increased use in medicine, with doctors experimenting with prostheses, living tissue and bone material. At present the units are too sophisticated and expensive for home-users, however, home printers are near future possibility.

3D printing presents exciting prospects for the future; however it also poses many legal puzzles. *Firstly*, it has serious *security* repercussions. It enables individuals, including terrorists, to manufacture any weapon comfortably. In fact, 3D printed guns have been already manufactured in United States, Japan and Australia.[139] *Secondly*, it has significant *tax* implications. Since product sold (CAD) is in a form of digital file, it will not be subject to custom duties imposed on physical products. In this context, effort towards making WTO moratorium on custom duties on digital products permanent, acquires considerable weight. *Thirdly*, some scholars argue that 3D printing will increase the incidence of *patent infringement*. Consumer will merely need to procure digital file containing instructions for the 3D printer (CAD) and can make infringing copies at home.[140] *Fourthly*, issue of standards and interoperability will come into play here as well.

139 Andy Greenberg, How 3-D Printed Guns Evolved Into Serious Weapons in Just One Year, Wired, 15 May, 2014, Available at: https://www.wired.com/2014/05/3d-printed-guns/ (accessed on 5 October, 2017); Nick Whigham, Police Seize Another Batch Of 3D Printed Guns As Authorities Deal With Danger Of Downloadable Firearms, News Limited, 12 December, 2016, Available at: http://www.news.com.au/technology/innovation/design/police-seize-another-batch-of-3d-printed-guns-as-authorities-deal-with-danger-of-downloadable-firearms/news-story/c2fa2711ebf7b761e3e2f0802a80d1b2 (accessed on 5 October, 2017).
140 Davis Doherty, Downloading Infringement: Patent Law As A Roadblock To The 3d Printing Revolution, Harvard Journal of Law & Technology, Vol. 26, Issue 1, Fall 2012.

iii. *Sharing Economy*

Rise of the Internet has led to the phenomenon of shared economies. Sharing economy is defined as "the peer-to-peer based activity of obtaining, giving, or sharing access to good and services".[141] It is also known as gig economy, platform economy, access economy, and collaborative consumption.[142] It has created a market for wide variety of goods and services which were once marked non-monetisable. Airbnb, Home Exchange, Couch Surfing allow travellers to rent lodgings from hotels or from private homeowners across the globe. Airbnb was used by over 4 million people between 2008-12 period;[143] Eatwith allows locals to share home-cooked food with travellers; DogVacay helps dog owners find a host who will take care of their dogs; Uber and Ola help commuters hail cabs from their phones.

In a sharing economy, the service providers, termed as "owners" advertise the service or good they intend to share with an online platform. The platform then filters and customizes the options according to the renter's preferences, history and the buyer's proximity to and haste for the good or service. The options are then listed to the renter and the parties are then introduced on the platform. A price is negotiated, if such a negotiation clause exists and the finer details are agreed upon, through the platform or approved channels. Payment can be made through online payment systems. The key concept behind the sharing economy include unlocking the value of unused or underused assets ("idling capacity"), and a shift from "asset-heavy" to "asset-light" business models.[144] Sharing economy pioneers like Airbnb, Uber, and E-bay do not own hotels, cars and brick & mortar shop, respectively. Growth of sharing economy can be contributed to number of factors. Smart phones and apps provide the gateway, mobile internet fuels ever-faster growth, location-based services mean whenever/wherever service provision, digital payments kill cash, while recommendations and reviews are digitizing trust.[145] All these technological changes coupled with the availability of more data about people and things, has given fillip to the sharing economy.

141 Niam Yaraghi and Shamika Ravi, The Current and Future State of the Sharing Economy, Brookings, 29 December, 2016, Available at: https://www.brookings.edu/research/the-current-and-future-state-of-the-sharing-economy/(accessed on 5 October, 2017).
142 Ibid.
143 The Economist, The Rise of the Sharing Economy, 9 May, 2013, Available at: https://www.economist.com/news/leaders/21573104-internet-everything-hire-rise-sharing-economy (accessed on 5 October, 2017).
144 Tyler Durden, A Primer On The "Global Sharing Economy" In 20 Charts, ZeroHedge, 24 July, 2017, Available at: http://www.zerohedge.com/news/2017-07-24/primer-global-sharing-economy-20-charts (accessed on 5 October, 2017).
145 Ibid.

Sharing economies have disrupted the traditional forms of business. Consequently, they put a great strain on the traditional regulatory and legal systems. They have numerous legal complexities associated with them. *First,* data security and privacy issues are inherent to the sharing economies. These services collect vast amount of data about their users which include user name, location, credit/debit card information, preferences, Internet search history etc. This data is susceptible to theft or misuse and poses threat to user privacy. *Second*, fixing of liability is complicated by multi-party model of sharing economies. It is debatable if an e-platform, matching owners and renters with each other, is considered an intermediary or a service provider. For example, ride-hailing service Uber had claimed no accountability for behaviour of the drivers as it is mere aggregator of taxis.[146] This applies to tort and criminal liability cases.[147] *Third,* sharing economies are forcing regulators to relook at licensing and business regulations. Traditionally sectors like hospitality, taxi, restaurants are heavily regulated. However, services like Airbnb and Uber due to their asset-light business model are able to bypass the regulators. These regulations include safety restrictions, zoning requirements and tax laws.[148]

iv. *E-Platforms*

Electronic platforms (e-platforms) are where most e-commerce occurs. There are two types of e-commerce platforms, Self-hosted and (third party) hosted. In the case of self-hosted platforms, operator of the platform and seller of the goods is the same party. On the other hand, hosted platforms are run by operators who allow other sellers to use it as marketing and selling place. Hosted platforms are the most common form of e-platform. Their functioning from business and technological perspective is explained as follows:

Business Model: Hosted e-platforms like Flipkart enable "search and match" between the buyer and seller. Sellers advertise their goods on the e-platform for a standing fee or commission. The e-platforms have elaborate websites with exhaustive search parameters that pinpoint the buyer's

146 Sanjay Vijaykumar, Uber: radio taxi or just an aggregator?, The Hindu, 9 December, 2014, Available at: http://www.thehindu.com/business/uber-radio-taxi-or-just-an-aggregator/article6674136.ece (accessed on 5 October, 2017).
147 Rick Schmitt, The Sharing Economy: cccan the Law Keep Pace with Innovation?, Stanford Lawyer, Stanford Law School, Issue 96, Spring 2017, 31 May, 2017, Available at: https://law.stanford.edu/stanford-lawyer/articles/the-sharing-economy-can-the-law-keep-pace-with-innovation/(accessed on 5 October, 2017).
148 Matt Faustman, 3 Ways the Sharing Economy is Pushing Legal Boundaries, Upcounsel Blog, 2014, Available at: https://www.upcounsel.com/blog/3-ways-the-sharing-economy-is-pushing-legal-boundaries (accessed on 5 October, 2017).

requirement and the buyer is able to compare makes and models, prices or delivery periods. E-platforms as facilitator between buyers and sellers ensure that the seller receives the payment and the buyer receives the commodity at the stated price and time. The e-platforms also assure buyers of product quality and product delivery. In a trust-driven transaction, it is essential that the buyer has enough faith to provide personal details and banking credentials. The e-platforms conduct verifications on the sellers and assure the buyers of seller and product authenticity for which they charge a fee.

E-platforms have simplified the "search and match" between the buyer and seller. They provide the buyers with a wider range of choices and the sellers with a larger market. Selling on e-commerce platforms is attractive as they do away with store maintenance, sales associates and inventory costs. This allows sellers to offer goods at much lower mark-ups than they can in the stores, a feature appealing to buyers.

Technological Model: E-platforms have three different systems working in tandem. A *web server* that manages an online storefront and processes transactions such as verifying bank or card details entered by the user; a *database system* which virtually catalogues all the advertised items, matches them with the physical inventory in stock, and updates the information in line with the orders being placed and the transactions being made simultaneously; and a *dispatch system* matches the transactions and the stock with the warehouse closest to the user and manages logistics of the delivery of products.

E-platforms make extensive use of Big Data (explained in Section III). E-platforms collect Big Data in the form of active and passive data. While active data is voluntarily given by the buyers, passive data is collected with the help of a tracker code called cookie. Tracking cookies are owned by the third-party advertisers and implanted into the user's computer when the user visits the advertiser's website or clicks on their advert. These cookies attaches itself to the Hard Disk Drive (HDD)[149] of the computer and keep data trail of all the user activities such as browser searches, frequently visited websites or pages, pages and content frequently mentioned or visited on social media, the cited areas of interest. This method allows the e-platforms to collect extensive amount of data about the users and generate a unique profile. It helps e-platforms in micro-targeting their users and providing them

149 Data storage device in the computer.

with a personalized experience. The volume of trade conducted through e-commerce platforms has soared in proportion to the development of data bases and refinement of data analysis technologies.

E-platforms suffer from same legal complexities as sharing economies. *First,* data security and privacy are one of the major concerns. As mentioned above, e-platforms collect extensive amount of data related to their buyers. This data is prone to misuse in form of theft, resale and privacy breach. *Second*, consumer protection is another pertinent issue. Standard online contracts where buyers do not have bargaining power often take way the right to enforce consumer claims; and *Third*, intermediary liability laws[150] are not fully developed with respect to the e-platforms. This adds to the ambiguity of the extent of the liability of the e-platform for the faulty goods sold through its website.

v. *Entertainment Services*

Recently there has been proliferation of online entertainment services which provide online access to movies, documentaries, TV shows for subscription fee or free of charge. Such services can be called Over the Top (OTT) Video Streaming Services. Netflix, Amazon Prime and Hulu Plus are some of the leading players in this market.

OTT video streaming services provide unlimited video streaming service i.e. supply of content (movies, TV shows, documentaries etc.) to the subscribers via internet which can viewed on the Internet connected devices such as smart-phones, laptops, tablets and smart televisions. They offer following benefits as compared to traditional cable TV or Direct to Home (DTH) broadcast:

a) Subscribers have option of choosing from wide variety and extensive amount of content.
b) Content can be instantly accessed at any time (24 hours) unlike traditional TV where movies or shows can be watched at pre-specified time slots.
c) Customers pay subscription fee like DTH service, but do not get any advertisement during streaming.
d) Subscribers can access unlimited amount of content i.e. there is no limit on number videos that can be watched during subscription period.

150 For example, Section 79 of the Information Technology Act of 2000 (India) provides for exemptions to the liability of intermediaries if certain requirements have been fulfilled.

e) Subscribers can watch content at their pace i.e half an episode, full episode or entire TV show in one go.
f) Content can be viewed on multiple screens at the same time.

These services primarily licenses content created (produced) by others, but they also creates their own content which can be exclusively viewed through their website. They generates revenue through subscription fee charged to users and in return subscribes can access unlimited amount of content during the subscription period. They also collect great quantity of user data through active and passive means. This data is used to create unique user profiles and provide them with personalised experience through content recommendations. User preferences are also used to as a guide for creating, cancelling or continuing the content.

Major legal issues associated with these services are: *First*, net neutrality is uniquely associated with OTT video streaming. As discussed in the Section II, physical distance between content provider and user affects the quality and speed of the delivery of the Internet data. OTT video streaming is particularly sensitive to the distance from the subscriber as seamless delivery of videos requires higher bandwidth. Therefore, such service providers enter into agreements with the ISPs for dedicated channel for their content. This induces ISPs to discriminate between the various types of contents delivered by them and many consider it a violation of net neutrality principle. At the same time, many others argue that such practice is reasonable network management and integral to efficient Internet service. Netflix and Comcast were involved in a dispute over this issue. Though, they resolved the dispute, legally it remains unsettled. *Second,* data security and privacy are inextricably involved with these services as well due to large amount of data collected by the service providers. *Third,* mobile and cable network operators argue that OTT service providers use the telecom infrastructure without paying for it, and they're not subject to the regulatory regimes that apply to operators such as Idea, Airtel & Vodafone. The telecom service providers also bear the additional burden of various tax provisions by local, regional and national authorities.[151] *Fourth,* Countries like India amended service tax laws to bring offshore service providers like Netflix providing online services from servers located outside India under the service tax net.[152] Such service

151 Sujata Joshi et al., Impact of Over the Top (OTT) Services on Telecom Service Providers, Indian Journal of Science and Technology, Vol. 8, Issue 4, 145–160, February 2015.
152 Central Board of Excise and Customs, Department of Revenue, Ministry of Finance, Circular No. 202/12/2016-Service Tax, 9 November, 2016.

providers would be required to obtain registration in India or appoint an agent to undertake all such compliances on his behalf in case the service provider does not have physical presence in India.[153]

vi. *Electronic Payment System*

Electronic payment (e-payment) system enables consumers to pay for goods and services electronically. It entails exchange of digital financial information such as encrypted credit/debit card numbers, electronic cheque or digital currency.[154] E-payment system in which large amount of money is transferred is called macropayment system and in which small amount of money is transferred is referred to as micropayment system.[155] A 2006 OECD Report on online payment systems categorised various payment systems into account based and electronic currency systems.[156] As per the report, account-based systems allow payment via an existing personalised account (usually a bank account), whereas electronic currency systems allow payment, if the payer has an appropriate amount of electronic currency. Details are as follows:

a. *Account-based Payment System*

i) *Credit cards and debit cards:* Online use of credit and debit cards is similar to their offline use except physical copy of card and signed confirmation by the buyer. Here payment is made directly from the buyer's account with the bank.

ii) *Mediating systems*: In this system buyer makes an account with the mediating services and is able to make payment to the sellers who have accounts with the same mediating service. When buyer uses a mediating system to make the online payment, he/she does not need to provide bank account details to the seller. Paypal is an example of such service.

iii) *Mobile payment and telephony account systems:* Mobile payments are payments conducted through wireless devices. Telephony payment occurs by phoning a special number the merchant has installed

153 Ibid

154 Indira Gandhi National Open University (IGNOU), Electronic Payment Systems, Virtual Classroom, Available at: https://webservices.ignou.ac.in/virtualcampus/adit/course/cst304/ecom2.htm (accessed on 5 October, 2017).

155 Kannan balasubramanian and M. Rajakani, Electronic payment Systems and Their Security, in Cryptographic Solutions for Secure Online Banking and Commerce (Information Science Reference, Hershey PA, United States of America, 2016), Available at: https://books.google.co.in/books?hl=en&lr=&id=Dto6DAAAQBAJ&oi=fnd&pg=PA20&dq=electronic+payment+ystems&ots=VN7t60fewp&sig=ULwneonG1VIqQPqbzTLbJvKcDZU#v=onepage&q=electronic%20payment%20systems&f=false (accessed on 5 October, 2017).

156 Organisation for Economic Co-operation and Development, Online Payment Systems For E-Commerce, DSTI/ICCP/IE(2004)18/FINAL, Committee For Information, Computer And Communications Policy, 18 April, 2006, Available at: https://www.oecd.org/sti/ieconomy/36736056.pdf (accessed on 5 October, 2017) p. 15.

with an operator, by sending a particular code by SMS, by voice contact, or by dialup to access content on a site and the user is charged by the minute for using the site

iv)*Payments via online banking:* Here the account holder is redirected to the bank's Web site by the merchant site to effect payment.

b. *Electronic Currency Systems*

i) Smart card-based systems which are most commonly used to pay small amounts within organisations (e.g. vending or copying machines or Metro). They usually rely on specialised hardware and dedicated smartcard readers for authentication; and

ii) Online cash systems which are software-only electronic money instruments based on signed (?) money. Electronic cash is broadly defined as electronically stored monetary value. They usually work via prepaid cards (one may not need a physical card, you mention e-tokens below), and arrangements differ although most require merchant subscriptions. Electronic tokens representing a certain value are exchanged in a similar way to cash.

Decreasing technology, operational and processing costs along with increasing online commerce have provided fillip to growth of e-payment systems.[157] However, e-payment systems are not devoid of legal concerns. First, privacy and security of data remain of utmost importance. Since, e-payment system involves exchange of sensitive information like debit/credit card numbers, banking details, passwords etc., data security is very crucial for the protection of consumer privacy and prevention of any theft or fraud. Second, authentication is next major concern. In order to ensure secure transaction in a setting where face to face interaction is absent, robust authentication measures are important. However, laws of different countries provide different authentication standards, sometimes specifying a clear technology bias.[158]Third, determining the relevant law that parties will be governed by in respect of electronic transactions (whether by the contract, or in its absence, by general principles of law). This may create problems, especially when the laws in Country A, where the company is registered permit electronic payment contracts, whereas the laws in Country B, where the consumer is located, do not support electronic payment contracts.[159]Fourth, legal

157 Supra note 133, EC.

158 Aashit Shah and Parveen Nagree, Legal Issues In E-Commerce, Nishith Desai Associates, 2001, Available at: http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Legal_issues_in_eCommerce.pdf (accessed on 5 October, 2017).

159 Ibid.

recognition of digital currencies is a matter of concern too. Currencies like Bitcoin are not recognised in most jurisdictions and any transaction in such currency is risk prone. Transaction in digital currencies is sometimes also used for money laundering. Another recognition related aspect is that e-payment companies do not go through the same rigorous licensing procedure as brick and mortar payment companies. There is an ambiguity as to what should be the extent of regulatory supervision for e-payment companies.

vii. *Financial Technology*

Financial technology (fintech involves intersection of financial services and technology.[160] The application of big data to enhance operations and product development in retail banking is known as fintech.[161]Retail banking refers to the banking where ordinary people are customers, as opposed to the corporations.[162] Fintech sees banks as data companies which record how much money belongs to the people and how much money people owe them.[163] It uses software programs to analyse this data and prepare customised financial instruments for its customers. It enables any bank to have real-time access to its books and thus, know real-time value of the borrower. It does away with the need for checking credit scores and physical inspection of the books. Instead the data for every dollar going in and out of the store is immediately available.[164]

It can increase the visibility of data and prevent disasters like 2008 subprime crisis. Though fintech companies like Square Capital and Standard Treasury are doing well, heavy regulations in the banking sector largely prevent completely big data driven fintech banks from entering the sector. Nevertheless, success of fintech companies is pushing large institutional banks towards investing in their own technology overhauls.

viii. *Cloud Computing*

Cloud computing services allow linking, storing and processing of massive volumes of data generated across an enterprise, drawing on the computational power of hundreds of machines, and

160 Pricewaterhouse Coopers Finacial Services Institute, Q&A What is FinTech?, April 2016, Available at: https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-fsi-what-is-fintech.pdf (accessed on 5 October, 2017).
161 Supra note 106, Ross, p. 166.
162 Ibid.
163 Ibid, p.168.
164 Ibid

analysed via utility services.[165] Individuals and companies can thus utilise storage and computing capacity without the need to make large capital investments, as well as being able to avail themselves of such resources from anywhere where there is network access.[166] Exports of cloud computing services were estimated to be worth approximately $1.5bn in 2010 (and this is likely a conservative figure) and the market for cloud computing services is anticipated to grow by up to 600 percent by 2015.[167]

The legal questions related to the cloud computing are: *First,* Cloud –computing entails storing of massive amount of data and therefore is automatically subject to data privacy and data security concerns; *Second*, data ownership is another significant issue. There is a possibility of ownership conflict between the client using the cloud service and host of the cloud service. Generally, contract would resolve such conflict. But, in the absence of clear contract, host can claim ownership over data even after termination of service; *Third,* extent of the liability of the host for any data misuse or breach is also contentious topic. Currently, it is governed by the contract between client and host. In the cases where client does not have bargaining power or contract is not negotiable, host can escape liability completely. Many publicly available cloud computing contracts limit liability of hosting provider to a level that is not in line with the potential risk; *Fourth*, compliance of regulations and laws related to tax, data protection, damages under contract can be difficult due to absence of onshore facility or legal office.

ix. *Precision Agriculture*

Data analytics has not only transformed how traditional business and sectors work, it has given rise to completely new sectors. An illustration of the new sectors is precision agriculture.

Precision agriculture is a product of big data and agriculture.[168] Precision agriculture system comprises of sensors and GPS for gathering data; software for analysing the collected data; software enabled machinery to execute the results of analysis; and an interface to communicate with all other

165 Michael Farber et al. , Massive Data Analytics and the Cloud: A Revolution in Intelligence Analysis, Booz Allen Hamilton, 2011, Available at: https://www.slideshare.net/BoozAllen/massive-data-13607270 (accessed on 5 October, 2017).

166 Randal E. Bryant et al., Big Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science and Society, Computing Community Consortium, 22 December 2008, Available at: http://cra.org/ccc/wp-content/uploads/sites/2/2015/05/Big_Data.pdf (accessed on 5 October, 2017).

167 Renee Berry and Matthew Reisman, Policy Challenges of Cross Border Computing, Journal of International Commerce and Economics, Vol. 4, Issue 2, November 2012, 9-10.

168 Supra note 106, Ross, p. 161.

components. Monsanto's FieldScripts is an example of precision agriculture in practice. It takes field information about a given farm, including its field boundaries, yield history, and the results of fertility tests, and breaks that farm into a number of small management zones. An algorithm then recommends specific seeds and provides a seeding prescription that is delivered to the farmer over an iPad app called Field View. The framer transfers data from Field View to farm machinery that distributes seed across the field as per the seeding prescription, customized for each management zone.[169] New age farm equipments function on the command of software programs. While farm equipment is working the field, it is gathering the information from sensors deployed in the field; combing it with the information provided by the GPS; and applying it to its performance in the field.

It helps in optimising the use of scarce resources like water, seeds, farm land, and fertilizers. It can also assist in national level budgetary and policy planning. Another benefit of precision agriculture can be in the reduction of pollution caused by fertilizers and decline in green house emissions due to reduced need for fertiliser production. All these features make precision agriculture promising field, especially for the resource-scarce developing countries. Companies like Monsanto, DuPont, and John Deere have been heavily investing in farm-data analytics companies. The most critical component of this application is sophisticated software which is able to analyse big data and produce accurate predictions. It raises concern that companies owning such software algorithm may indulge in rent-seeking behaviour and potentially prevent small farmers and developing countries from making full use of the technology. Another equally important asset is size of data set. Companies which have resources (including capital) to collect large amount of data will be able to produce more accurate predictions and thus will be more profitable.

169 Ibid, p.163.

IV. DATA –GREY AREAS

In the preceding section, this paper studied various types of data and their usage. It also examined various data-based good and services and associated legal issues, in brief. This section focuses on the cross-cutting legal concerns which have resulted from current data economy. These issues are ownership of data, data privacy, data protection, data localisation, taxation of data flows, and jurisdiction applicable to data flows.

A. Data Ownership

In data-economy, the most valuable asset is the data. As seen in the earlier section, all emerging business like IoT, precision agriculture, e-platforms etc., create their business model around big data. According to a 2016 report by International Data Corporation (IDC), worldwide revenues for big data and business analytics (BDA) is likely to grow from $130.1 billion in 2016 to more than $203 billion in 2020.[170] Furthermore, most big businesses today are data based. Companies like Facebook, Uber, Amazon etc., use data to provide services and goods. Thus, entities possessing and controlling the big data are going to be the biggest beneficiaries of data-driven economy. Further, government and public institutions see big data as gateway to precision planning and allocation of the sparse resources.

However, data from its collection to its use and re-use may pass through multiple hands.[171] Furthermore, often entities that build the system for collection of data, store, analyse and, use the data are separate.[172] In addition, data by nature is non-rivalrous i.e. possession of the data by one party does not exclude other parties from gaining possession of the same data. This adds to the complexity of control and use over data. In this context, ownership and control of data becomes pertinent topic for discussion.

170 International Data Corporation, Double-Digit Growth Forecast for the Worldwide Big Data and Business Analytics Market Through 2020 Led by Banking and Manufacturing Investments, According to IDC , Press Release, 3 October, 2016, Available at: https://www.idc.com/getdoc.jsp?containerId=prUS41826116 (accessed on 5 October, 2017).
171Ali M. Al-Khouri, Data Ownership: Who Owns 'My Data'?, International Journal of Management & Information Technology, Vol. 2, Issue 1, 1-8, December 2007, Available at: https://cirworld.com/index.php/ijmit/article/view/1406/pdf (accessed on 5 October, 2017).
172 Ibid

Ownership of data does not fit in the existing legal systems. Firstly, traditional property rights which are based on right to exclude are not suitable for data as unlike tangible property data is non-rivalrous in nature.[173] Secondly, legally created exclusionary right of Intellectual Property too is incompatible with data because creation of data is a by-product of other commercial and non-commercial online activities and does not require additional incentive.[174] Moreover, data is not a product of creative human effort.[175] Thirdly, contribution to data creation is mixed and unquantifiable. This makes allocation of rights over data difficult.[176]

Presently, technical restrictions, legal frameworks and contracts together regulate the data control dynamics:

i. *Technical Restrictions*

Owner of data storage systems get de facto control over the data stored in the system.[177] Organisation controlling the storage may not share the data with other entities, and thus can maintain exclusive ownership. Also, if data is shared in unstructured format, it will not result in effective access.

ii. *Legal Framework*

There are no laws conferring ownership over data. However, there are other legal systems which regulate the control over data. EU database Directive grants copyright protection to original databases (not for the content) and 'sui generis' right for non-original databases, limited to 15 years.[178] Sui generis right extends to the data if qualitatively and /or quantitatively substantive

173 Nestor Duch-Brown et al., The Economics of Ownership, Access and Trade in Digital Data, JRC Digital Economy Working Paper 2017-01, JRC Technical Reports, 2017, Available at: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf (accessed on 5 October, 2017).

174 P. Bernt Hugenholtz, Chapter 9: Something Completely Different: Europe's Sui Generis Database Right, in The Internet and The Emerging Importance of New Forms of Intellectual Property, Susy Frankel and Daniel Gervais (eds.)(Kluwer Law International B.V., Alphen aan den Rijn, The Netherlands, 2016), Available at: https://www.ivir.nl/publicaties/download/Chapter9_ILS37.pdf (accessed on 5 October, 2017).

175 Supra note 166, Berry and Reisman, p. 13.

176 Andreas Wiebe, Who Owns Non-personal Data? Legal Aspects and Challenges Related to the Creation of New 'Industrial Data Rights', Slides presented at the German Association for the Protection of Intellectual Property (GRUR) Conference on Data Ownership, Brussels, 2016, Available at: http://www.grur.org/uploads/tx_meeting/01-Wiebe_Presentation_Brussels.pdf (accessed on 5 October, 2017).

177 Supra note 164, Farber et al.

178 European Council, DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the legal protection of databases, OJ L 77/20, 11 March, 1996, Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31996L0009 (accessed on 5 October, 2017).

investment has been made towards it. It is aimed at protecting the investor against substantial harm to his investment.[179] Another legal instrument is data protection law. EU has General Data Protection Regulation 2016 which protects individuals, called data subjects.[180] It creates inalienable and non-tradable specific rights for natural persons including (a) the prohibition of data processing without a legal basis (e.g. "informed consent"), (b) the prohibition to use personal data for other purposes that those for which they were originally collected, (c) the right for the data subject to access and extract ("port") his personal data, and (d) the right to be forgotten. These rights are assigned to the data subject as a natural person and reduce whatever rights the data collector has as a creator of a database of personal data.[181]

iii. *Contracts*

All online transactions are based on online contracts between the parties. Through these contracts, individuals trade their personal information in return of free online services. Personal data so collected is subject to data protection laws. Nevertheless, it is unclear if individual transfers the ownership or assigns right to use his or her data. One view is that de facto ownership is transferred to the service provider. For instance, Facebook Policy is to keep the user data even after account is deleted.[182] Thus, once user has shared personal data, he or she can no longer take back the possession. Opposing view is that expressed in EU GDPR which treats privacy as an inalienable right. It signifies that user does not transfer ownership over data. However, this protection is restricted to the rights enumerated under right to privacy and does not refer to all types of data.

As can be seen, this area is a Gordian knot, where traditional approach would be counterproductive. To devise most appropriate models, focus should be on the mischief which needs to be addressed. Here objectives are three fold- firstly, protection of privacy rights of individuals; secondly, business should not have undue advantage; and thirdly, governments should have access to useful data. As discussed above, ownership rights do not resolve any of the mentioned issues. In fact, enforcement of ownership is impractical due to non-rivalrous nature of data. Instead defining minimum rights

179 Supra note 166, Berry and Reisman, p. 14.

180 European Commission, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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), OJ L 119/1, 27 April, 2016, Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed on 5 October, 2017).

181 Supra note 166, Berry and Reisman, p. 14.

182 Erick Schonfeld, Zukerberg On Who Owns User Data On Facebook: It's Complicated, Tech Crunch, 16 February, 2009, Available at: https://techcrunch.com/2009/02/16/zuckerberg-on-who-owns-user-data-on-facebook-its-complicated-2/ (accessed on 5 October, 2017).

and obligations of the individuals, business organisations and governments will be the most appropriate method. Fiduciary duty of business corporations who have higher bargaining power should be clearly established. This will require establishing standard of protection measures taken by the party collecting and storing the data. Additionally, when public data is aggregated and used further by business corporations, it should be available for public purpose. Scope for sharing monetised value of customer data requires further consideration. There has to be balance between interests of consumer who is source of data, data collector who has devised the system and infrastructure to collect the data and overall public interest in access to data.

B. Data Protection and Privacy

Privacy is one of the biggest concerns in relation to data flows. Term 'privacy' does not have universally accepted definition and derives its meaning from the context. In reference to data flows, it entails getting consent from individuals before collecting their information, being transparent about why information is collected, what its use will be and deleting the information when it is no longer needed or when consent is withdrawn.[183] Data protection is a connected concept. Data protection involves taking adequate steps to protect data from accidental or malicious disclosure.[184] The factors in considering what efforts must be made to protect data depend on the type of data, its value to criminals and the harm to the victims.[185] Although data privacy and data protection are often used interchangeably, two are separate concepts with different scope and meaning. While data privacy is limited to personal data, data protection has much wider scope and covers all types of data, including personal data. Data protection can be understood as means to securing data privacy.

These two concepts are fundamental to the growth of e-commerce. A safe, secure and, reliable communication and information system is imperative for consumer trust and confidence.[186]Further, ensuring security of personal data has ethical implications. Many argue that people should choose whether to share it, and they should be able to share it on their own terms. Consumers, business and government recognise the benefit of data security, but differ on the methods to achieve it. This has

183 Sushil Kambampati, What India's Data Protection Committee Can Learn from US, EU and China, The Wire, 3 October, 2017, Available at: https://thewire.in/183776/what-indias-data-protection-committee-can-learn-from-us-eu-and-china/ (accessed on 5 October, 2017).
184 Ibid.
185 Ibid.
186 Asia Pacific Economic Corporation Privacy Framework, Preamble.

led to a patchwork of data protection and privacy regimes. Global data protection system comprises comprehensive regulations, self-regulations, sector specific regulations and, no regulations.

i. *European Union (EU)*

EU has comprehensive laws for the protection of personal data. Its data protection laws are rooted in fundamental right to privacy enshrined in the Article 7 of the EU Convention and Article 8 of the Charter on Fundamental Rights.[187]

EU has framed a regulation titled General Data Protection Regulation (GDPR) which will come into force in May 2018 and will replace Data Protection Directive, 1995. [188]GDPR mandates 'privacy by design' i.e. designing and developing new products and services with data protection standards built-in from the start and default to privacy-friendly settings.[189] It has widened the scope of protection and has introduced tougher punishments for violation of rules concerning storage and handling of personal data. Firstly, it has expanded EU data protection commitments to cover all processing activities relating to EU-based data subjects.[190] It covers following activities:[191]

a. processing activities by data controllers and data processors established in the EU, whether or not the processing takes place in the EU;
b. the processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU where the processing activities relate to offering goods or services to data subjects in the EU; and
c. the processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU where the processing activities relate to monitoring their behaviour in the EU.

Secondly, GDPR requires active consent, thus no pre-ticked box and companies must keep a thorough record of how and when an individual gives consent to store and use their personal

187 Juliane Kokott and Christoph Sobotta, The Distinction Between Privacy And Data Protection In The Jurisprudence Of The CJEU And The ECTHR, International Data Privacy Law, Vol. 3, Issue 4, 1 November 2013, 222–228.
188 Supra note 173, Hugenholtz.
189 Trulioo, EU Data Privacy Laws: New Rules for Doing Business in Europe, 26 April, 2017, Available at: https://www.trulioo.com/blog/eu-data-privacy-laws/(accessed on 5 October, 2017).
190 Pulina Whitaker, The New European Data Privacy Regime, Morgan Lewis, 21 July, 2017, Available at: https://www.morganlewis.com/pubs/the-new-european-data-privacy-regime(accessed on 5 October, 2017).
191 Ibid.

data.[192]Further, companies have to show audit trail of consent, including screen grabs or saved consent forms. Thirdly, GDPR further cements the right to be forgotten. It states that individuals have right to withdraw consent and upon withdrawal all the details concerning that individual have to be erased permanently.[193] GDPR framework overall has greater scope and much tougher punishments for those who fail to comply with new rules around the storage and handling of personal data. EU also exports its rules to other jurisdictions through adequacy decisions. European Commission assesses a third country's laws and allows transfer of data to that country if it finds data protection adequate as per the EU law.[194]It has so far recognised 11 countries.[195]

ii. *United States (US)*

US, unlike EU, does not have single comprehensive law for data protection. US has collage of federal and state laws and regulations governing the collection and use of personal data. The overall framework is made of laws directed at specific sectors (finance and health)[196] or specific activities (telemarketing, commercial e-mail etc.)[197]. These laws are further supported by consumer protection laws that are not privacy laws per se, but have been used to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information.[198]In addition, there are self-regulations in form of guidelines developed by industry groups and government agencies.[199] Recently, US has passed *Judicial Redress Act, 2016* which extends the benefits of the US Privacy Act to Europeans and gives them access to US courts.[200]

The major differences between EU and US data protection regime are as follows:

192 Hugh Wilson, European Data Protection Laws Are Changing, The Telegraph, 18 May, 2017, Available at: http://www.telegraph.co.uk/connect/small-business/business-networks/bt/data-protection-laws-changing/ (accessed on 5 October, 2017).
193 Ibid.
194 European Commission, Commission Decisions On The Adequacy Of The Protection Of Personal Data In Third Countries, Available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed on 5 October, 2017).
195 Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay
196 Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB) and Health Insurance Portability and Accountability Act (HIPAA).
197 Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) and the Telephone Consumer Protection Act (47 U.S.C. §227 et seq.) regulate the collection and use of e-mail addresses and telephone numbers, respectively.
198 Leuan Jolly, Data Protection In The United States: Overview, Thomson Reuters Practical Law, 1 July, 2017, Available at: https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (accessed on 5 October, 2017).
199 Ibid.
200 Ibid.

a. EU has clearly defined rights of data subjects and specifically lists requirements to protect these rights, whereas US though recognises right to privacy, does not define components of data privacy.
b. EU has single comprehensive law to ensure data protection, whereas US system is composed of multiple regulations.
c. EU has mandatory laws regulating the actions of business and industry, whereas US relies on self imposed guidelines and best practices.

Data protection is directly related to trade in goods and services in the digital economy. Insufficient protection can create negative market effects by reducing consumer confidence, and overly stringent protection can unduly restrict businesses, with adverse economic effects as a result. Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of utmost importance for global trade flows that increasingly rely on the Internet. Further, the scope of definitions of personal data differs (broad or narrow) depending on the jurisdictions and data protection laws vary from country to country (and region to region), as visible from US and EU model.

C. Data Localisation

Data localisation in general refers to the mandate to retain data within territorial jurisdiction of a country.[201] It can either be direct legal requirement or indirect prescription.[202] These requirements can be in form of direct legal obligations to locate data server within the domestic boundary[203] or to process data locally.[204] Indirect methods of achieving data localisation can be conditional market access and tax incentives. Use of domestic technology, including locally created cryptography or algorithms;[205] technology transfer (including disclosure/sharing of source code);[206] and commercial presence are the examples of prerequisites for conditional market access.

201 United Nations Conference On Trade And Development (UNCTAD), Data Protection Regulations And International Data Flows: Implications For Trade And Development, April 2016, Available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (accessed on 5 October, 2017) p.13.
202 Ibid.
203 Susan Aaronson, Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security, 1 April, 2015, Available at: https://ssrn.com/abstract=2595809 (accessed on 5 October, 2017).
204 Ibid, p.109.
205 Ibid, p.109.
206 Ibid, p.109.

Data localisation is a product of social and economic needs. Its major motivations are national security, data privacy, and developments needs. Firstly, need for data privacy has persuaded countries to impose strict restrictions on the transfer of data of and about their nationals, particularly in case of sensitive sectors like health and finance. Secondly, revelations made by Edward Snowden regarding widespread surveillance by US government institution, National Security Agency (NSA) has alarmed other countries and made data localisation an attractive option. Data localisation provides greater control and asset for surveillance capability.[207] Thirdly, countries recognise that data processing and analytics is a promising industry, and have an important role in businesses in all sectors today, and therefore, want to break foreign hegemony and develop indigenous technology and digital industry.

Many countries have started enacting data localisation requirement; however, most of these are indirect. So far, Russia and Indonesia have passed laws specifically and directly restricting the transfer of data abroad. Other countries considered imposing similar localization requirements (notably Brazil and the Republic of Korea), but after wide stakeholder consultation, they embraced a mixture of alternative approaches.[208]

Growing interest in data localisation has also brought along criticism. It is being touted as one of the biggest hindrance to digital trade.[209] Its opponents cite economic, technical and ethical reasons in their support. Firstly, they claim that requiring data centre to be located domestically undermines the cost-effectiveness of cloud-based computing services where so-called location independence is important.[210] Presently, IT firms make location decisions according to climate condition, electricity costs, sales tax and other subsidies.[211]Secondly, it adversely affects economies of scale, business feasibility and quick market expansion.[212] Thirdly, in some cases this could lead the providers of data services to exit the market, leaving domestic business with access to less efficient and effective

207 Joshua P. Meltzer, A New Digital Trade Agenda, August 2015, E15 Initiative, International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, Available at: http://www20.iadb.org/intal/catalogo/PE/2015/15697.pdf (accessed on 5 October, 2017).
208 Supra note 200, UNCTAD.
209 Bernard Hoekman and Aaditya Mattoo, World Bank Policy Research Working Paper 4461, January 2008, Services Trade and Growth, p 3.
210 Ibid.
211 Shamel Azmeh and Christopher Foster, The TPP And The Digital Trade Agenda: Digital Industrial Policy And Silicon Valley's Influence On New Trade Agreements, Department of International Development, London School of Economics and Political Science, January 2016, p 26.
212 Supra note 208, Hoekman and Mattoo.

services that can reduce their ability to compete domestically and in overseas markets.[213] Fourthly, mandatory data localisation ignores that firms need to easily link into core backbone networks, and suitability of cooler climates, given the high costs of air conditioning for servers;[214]Fifthly, government access to locally stored data can reduce the willingness of consumers and businesses to provide personal data and use cloud computing services.[215] A study has pegged very high GDP losses of introducing economy-wide data localisation requirements that apply across all sectors of the economy -Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%), Korea (-1.1%).[216]

On the other hand, proponents of data localisation argue that it has significant effect on catching-up with developed countries and major players of the industry in terms of technology and market share. Developing a data industry is seen as an important part of the development of a digital industry.[217] Further, investments in the sector have direct benefits to the economy in the form of increased Foreign Direct Investment (FDI), tax revenue, and employment opportunities. They also stress that it can also lead to virtuous circles of new data centres alongside connectivity, skilled staff which support clustering effects that can support the emergence of hi-tech capacity in nations. A 2013 study by the Washington Research Council found that data centres contribute to area in jobs, taxes, construction but also that it gives the area a "key advantage in the quest for technology-based economic development"[218] Similarly, a study by Boston Consulting Group (BCG) on the impact of Facebook data centres in Northern Sweden highlighted the direct and indirect contribution of the project to the local and national economy. It also reiterated the point that such investments provide the backbone of a building wider digital infrastructure and digital industry in Sweden. Ireland, for instance, has attracted investments in the digital industry for years and has become an important location for the software industry, the gaming industry, internet-related industries, and data industries.[219] . Data localization rules could significantly affect the strategies of international IT, web and cloud companies and push them to invest in locations that they would not invest in otherwise.

213 Ibid.
214 Sven Grundberg and Niclas Rolander, For Data Centre, Google Goes for the Cold, The Wall Street Journal, 12 September, 2011, Available at: https://www.wsj.com/articles/SB10001424053111904836104576560551005570810 (accessed on 5 October, 2017).
215 Supra note 208, Hoekman and Mattoo.
216 Matthias Bauer et al., The Costs of Data Localisation: Friendly Fire on Economic Recovery, ECIPE Occasional Paper No, 3/2014, European Centre for International Political Economy, May 2014.
217 Supra note 210, Azmeh and Foster, p. 27.
218 Ibid.
219 Bernadette Andreosso-O'Callaghan et al., The Development and Growth of the Software Industry in Ireland: An Institutionalized Relationship Approach, European Planning Studies, Vol. 13, Issue 5, 2015.

This is particularly relevant for large middle-income and developing countries that are increasingly an important market for digital trade and internet-based services and where negotiation for "data localization" could effectively be used as a bargaining tool in exchange for market access.[220]

Overall, it is very tangled issue with huge economic repercussions. Thus, any law with respect to data localisation should take into account economic loss and gain.

D. Data Jurisdiction

Fragmented legal jurisdictions are not equipped for transnational e-commerce and internet-enabled technologies. Here challenges are of two types- conflict of laws and enforcement difficulties. Also, electronic transactions can spread all over the world and therefore, it is difficult to fix the jurisdiction of cause of action. United States has recently passed the Judicial Redress Act (JRA) in order to reassure customers of cloud services that they could have the same rights to legal redress as U.S. citizens. It is passed to fulfil the conditions of Privacy Shield Agreement with the EU. The Act has a complicated mechanism for assessing who is eligible to exercise these rights, but it is a significant first step in offering dispute resolution options to foreign citizens.[221]In the absence of an international agreement, jurisdiction law is complex. It is too large a subject to be covered in this study.[222]

E. Data Taxation

Another challenge posed by the data economy is in the sphere of tax administration. Current tax structure all over the world has been designed to capture trade in visible products and services where Permanent Establishment (PE) is identifiable. The tax regime recognizes territorial taxation by the source country and personal taxation by the resident country.[223] However, data flows are invisible flows which do not have easily identifiable source and destination. It is completely delinked from traditional concept of territorial borders. Even if source and destination are established, quantifying data and its value is even bigger challenge. Moreover, data crosses several borders during its journey from source to end user.

---

220 Stephen Ezell et al., Localization barriers to global trade: threat to the global economy, 2013, Available at: http://www.itif.org/publications/localization-barriers-trade-threat-global-innovation- economy (accessed on 5 October, 2017).
221 Supra note 200, UNCTAD.
222 Supra note 200, UNCTAD.
223 Rifat Azam, Global Taxation Of Cross-Border Ecommerce Income, Virginia Tax Review, Vol. 31, Issue 4, 639-692, May 2016.

Presently, multinationals (including e-commerce companies) minimise their tax by operating in low-tax jurisdictions and by relying on the separate personality doctrine (also called concept of corporate veil) - a company is a separate person from its shareholders and directors and must be treated as such for tax purposes.[224] Countries have been grappling with this subject for a while. UK and Australia introduced Diverted Profit Tax (DPT) and Tax Integrity Multinational Anti-Tax Avoidance Law (MAAL), respectively.[225] These taxes though applicable to all non-resident corporate entities that avoid tax on sale within the tax jurisdiction due to PE loopholes, have been specifically targeted at US multinational e-commerce giants like Google, Facebook and Apple. These taxes have earned the name of '*Google Tax'*. India went step further and introduced 6 % 'Equalization Levy' (EL) on advertising revenues of multinational web companies and on cloud-based services and online entertainment such as streaming video and audio.[226] It seeks to send a signal that India is not a zero tax economy and at the same time pushes major global players in India's digital economy to set up formal shop in India.[227] The equalisation levy is one of the options suggested by the Organisation for Economic Cooperation and Development's (OECD) report on tackling Base Erosion and Profit Shifting (BEPS) or tax avoidance strategies.[228] Nevertheless, extending its ambit to all cloud computing and online entertainment service provider may have negative impact on domestic players, consumers and may lead to chain reaction of similar laws in other countries. In 2013 France considered imposing tax on collection of personal data. It argued that tax on data collection was justified on grounds that users of services like Google and Facebook are, in effect, working for these companies without pay by providing the personal information that lets them sell advertising.[229]

---

224 Jim Corkery et al., Taxes, the Internet and the Digital Economy, Revenue Law Journal, Vol. 23, Issue 1, ,Article 7, Available at: http://epublications.bond.edu.au/rlj/vol23/iss1/7 (accessed on 5 October, 2017).

225 Reuven S.Avi-Yonah, Three Steps Forward, One Step Back? Reflections On "Google Taxes "And The Destination-Based Corporate Tax, Nordic Tax Journal, Vol. 2, 69-76, September 2016.

226 Sachin Dave, Apple, Netflix, Microsoft, Amazon And IBM May Have To Pay 'Google Tax' In India, The Economic Times, 17 December, 2016, Available at: http://economictimes.indiatimes.com/news/economy/policy/apple-netflix-microsoft-amazon-and-ibm-may-have-to-play-google-tax-in-india/articleshow/56027728.cms (accessed on 5 October, 2017).

227 Business Line, The 'Google Tax', The Hindu, 22 march, 2016, Available at: The 'Google tax', http://www.thehindubusinessline.com/opinion/editorial/the-google-tax/article8386082.ece (accessed on 5 October, 2017).

228 Ibid.

229 Eric Pfanner, France Proposes an Internet Tax, The New York Times, 20 January, 2013, Available at: http://www.nytimes.com/2013/01/21/business/global/21iht-datatax21.html?mcubz=0 (accessed on 5 October, 2017).

There are also issues of how the tax rates are calculated. This issue has caught attention at international level as well. At UN International Telecommunications Union (ITU) the European Telecommunications Network Operations Association (ETNO) proposed a *Global Internet Tax* - taxing Internet companies when they deliver content.[230] A *Global E-Commerce Tax (GET)* in the form of flat rate on cross-border transaction for funding global public goods has been suggested.[231] A borderless tax for borderless trade! Though idea of GET sounds promising, its feasibility in light of global political reality is doubtful. As discussed earlier various countries and institutions are trying to find solution to riddle of e-commerce transactions. This effort may culminate into concrete cooperation between countries to update the current tax regime to address the issues of taxing so far un-taxable cross-border data transactions. This movement should also be contrasted with effort to fix custom duties on digital products at zero. Both of these efforts give complete picture of divided interests of the global community.

This section discussed major legal issues plaguing the digital world. The discussion clearly shows that online landscape is complex in nature, and therefore related legal issues are complex too. Nevertheless, two common themes can be observed in all the legal issues. First, new data based services have modified the existing ways of business, and legal rules previously applicable to that sector need updating. For example, sharing economy has altered hospitality and cab-for-hire business. Accordingly, regulators of these sectors need to take into account the changes and update existing regulations. Second, advancement in technology has resulted in completely new areas of business. Services like social media, OTT video streaming etc. were hitherto unheard of and now have become universal. New laws are required to deal with such services.

230 Kelly Phillips Erb, Is the UN Trying to Tax the Internet?, Forbes, 8 June, 2012, Available at: https://www.forbes.com/sites/kellyphillipserb/2012/06/08/is-the-u-n-trying-to-tax-the-internet/#4b7a8e3861e9 (accessed on 5 October, 2017).
231 Supra note 222, Azam, p. 643.

V. CONCLUSIONS

This paper has discussed the physical and technological components of the Internet and the uses of data generating & flowing through the Internet; and legal complexities arising from these two fields.

In order to address the dual challenges of rapidly changing technology and pursuant inequality, mentioned in the Introductory Section, legal efforts have to be made at two levels. First, law has to ensure level-playing field for infrastructure development for the Internet, and for its use. At domestic level, this can be done through combination of competition policy and telecom/Internet sector-specific regulations. Second, level-playing field is also required for the operation of e-commerce companies. At this level, market naturally favours companies with large data collection and processing capacity. Such companies take benefit of virtuous cycle where data analytics enables them to capture more customers, which in turn increases their data analytics capabilities. At present Google, Apple, Facebook and Amazon (GAFA) along with Uber, Twitter, Alibaba and a few others rule the global digital landscape. Billions of people provide data about their personal lives and business activities to these companies, which are using that data as leverage to track and influence human behaviour to their economic advantage.[232] These companies control key technological and economic resources. This control shields them from any future competition too. Breaking the virtuous cycle of data collection may not be practically possible or desirable, but appropriate laws and rules can ensure that such companies do not abuse their market position and entry barriers for new and small entrants are minimized.

It is worth noting that taking the legal route is not an answer for all the complications resulting from omnipresent e-commerce. Law has to take into account purely technical and economic issues along with the international regime. In addition, there may not be possible to have a uniform legal approach for all the issues. While some issues need extensive legal intervention, other issues are better resolved through alternate approaches. So far, globally, three types of regulatory approach can be observed- complete freedom, no freedom and limited freedom for digital business.[233] The

232 Ibid.

233 See Mishi Choudhary and Eben Moglen, Head Off Digital Colonialism: How Indian IT Can Compete With Google And Facebook And Show The World A Better Way, Times of India, 29 May, 2017, Available at: https://blogs.timesofindia.indiatimes.com/toi-edit-page/head-off-digital-colonialism-how-indian-it-can-compete-with-google-and-facebook-and-show-the-world-a-better-way/(accessed on 5 October, 2017).

United States has exercised minimal regulation to allow online giants to develop and for the government to use them as tool of national security and intelligence resource; Countries like China and Russia have adopted an approach of extensive intervention and regulation by encouraging and supporting domestic search engines and social media structures to secure domestic private companies interests; and European Union has taken the path of limited regulation where it allows these companies to function freely subject to competition and data protection laws.

Any country before adopting either of these approaches, must keep in mind the current economic and technological structure and its rapidly changing nature. Overall, lawmakers must keep their minds and options open.