Consultation Paper No.10/2021

Telecom Regulatory Authority of India

Consultation Paper

on

Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India

New Delhi, India

16th December 2021

Mahanagar Door Sanchar Bhawan,
Jawahar Lal Nehru Marg,
New Delhi – 110002

Stakeholders are requested to furnish their comments to Advisor (BB&PA), TRAI, by 13th January 2022 and counter-comments, if any by 27th January 2022.

Comments and counter-comments would be posted on TRAI's website: www.trai.gov.in. The comments/counter-comments may be sent, preferably in electronic form, to Shri Sanjeev Kumar Sharma, Advisor (Broadband and Policy Analysis), Telecom Regulatory Authority of India, on the email id: *advbbpa@trai.gov.in* with a copy to *jtadvbbpa-1@trai.gov.in* and *jtadvbbpa-3@trai.gov.in* respectively.

For any clarification/information, Shri Sanjeev Kumar Sharma, Advisor, (Broadband and Policy Analysis), may be contacted at Telephone No - +91-11-23236119

CONTENTS

TABLES

ANNEXURES

CHAPTER 1

INTRODUCTION

1.1 During the last two decades, in an increasingly knowledge-driven globalized world, telecommunication and the internet have emerged as key drivers of economic and social development. They have enabled better connectivity among users, increased the use of Information and Communications Technology (ICT) services, and facilitated the emergence of a variety of new business models. ICT not only contributes directly to the GDP through the production of goods and services but also spurs innovation in the ways of production and delivery, leading to increased employment and labor productivity. India has one of the fastest-growing ICT sectors in the world, with ICTs being used to deliver critical goods and services to millions of Indians.

1.2 Communications services such as voice, video, data, internet, and wideband multimedia have become indispensable in modern society. With the proliferation of technology, for different purposes, the Government, private enterprises, and people in general are relying more and more on ICT services such as digital platforms, online content, and broadband connectivity. The digital transformation is emerging as a key driver of sweeping changes in the world around us. The telecommunication industry is at the forefront of this transformation, adding value to the Digital Economy.

A. Boosting Data Economy

1.3 Data economy is an integral part of modern economy. Data has also become a key asset for innovation. The advantage of controlling data by online platform-based companies is increasingly recognized and such existing companies act as an entry barrier for new entrants, leading to near monopoly in global digital markets. The data gap applies not only at the country level between developed and developing economies. It is also increasingly leading to debates on the need for policy intervention to create level playing field. The gap is growing

wider for small and developing countries that are far behind in their digital investments and capabilities. Moreover, countries are forming different data protection and trade regimes. As per the Organization for Economic Co-operation and Development, *"The Digital Economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services, and data. It refers to all producers and consumers, including Government, that are utilizing these digital inputs in their economic activities"*. Also, the Digital Economy Value Chain is the innovation of the value chain, driven by the following key digital elements:

a. Servers, Storage, and Networking Equipment
b. Data Centres
c. Cloud Computing and Services
d. Content and Applications
e. Connectivity – Leased Circuits, Internet, Content Delivery Networks
f. Interconnection – Internet Exchange Points

1.4 Almost everything has switched to the online mode during the pandemic resulting in an enormous increase in data consumption. With the rollout of 5G, IoT, and AI, more data would be created via widespread, geographically distributed networks and new-age devices. Further, 5G would bring new use cases of Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (MMTC). 5G, along with edge computing, would fulfill the needs for ultra-reliable, low-latency, and high-throughput communications. This convergence of computing and communication services will pave the way for a boon in the data economy for any nation. For undertaking successful data economy initiatives by any nation, having distributed edge computing infrastructure, massive data storage facilities, and a robust, and efficient internet exchange point infrastructure are pre-requisites.

1.5 Figure 1 depicts the notable key drivers for boosting data economy of India.

Figure 1.1: Boosting data economy

1.6 To keep pace with the global data economy initiatives, it would be necessary to formulate reliable frameworks and policies that would encourage development of 5G, IoT, Data Centers, and associated services, data analytics, edge computing, digital platforms, and applications. As these services can be delivered remotely, India can become a global hub for such systems and services.

1.7 As India aims to strengthen its position in the digital economy, it becomes imperative for the country to use futuristic technologies as a lever for growth. This becomes even more important while considering the various policy initiatives that the competing economies have come up with, along with the amount of investment and resources they are committing towards digital transformation. The Digital India program of the Government, launched in 2015, brought the topic of digitization to the forefront of public discourse. Since then, considerable progress has been achieved in several areas such as the construction of

broadband highways, development of local Data Centres, public internet access, e-governance, development of basic information technology skills etc.

1.8 National Digital Communications Policy (NDCP)-2018 also emphasizes that "*Digital infrastructure and services are increasingly emerging as key enablers and critical determinants of a country's growth and well-being.* ***With significant capabilities in both telecommunications and software, India, compared to most countries, stands poised to benefit from harnessing new digital technologies and platforms to unlock productivity, as well as to reach unserved and underserved markets; thus, catalyzing economic growth and development, generating new- age jobs, livelihoods and ensuring access to next-generation services for its citizens.***"

1.9 Digital infrastructure is boosting the data economy, and the services are fast moving beyond the traditional telecom services domain. With large- and small-business companies embracing innovative technologies and more users connecting to the internet, data is the key input for firms to develop and deliver digital services and products. The key contemporary infrastructure that is required to boost the digital ecosystem and facilities include:

I. **Data Centres –** used for edge computing, hosting of content, and delivering cloud-based services,
II. **Content Delivery Networks –** used for delivering the content from the cloud to the edge of the network, and
III. **Internet Exchange Points –** enables networks to exchange traffic with each other in the internet infrastructure.

Together these three form the part of what can be termed as "Digital communication infrastructure and services".

I. Data Centre (DC)

1.10 The world is going digital at a pace faster than expected. Partly, this is driven by the pandemic-induced 'Global Lockdown', which has

resulted in a data surge arising out of increased digital social interactions and online transactions. From enterprises to individuals, usage of cloud services has increased to enable online mobility and easy sharing of data. Cloud services facilitate the flow of user data from front-end clients, through the internet, to the provider's systems, and back. Users can access cloud services with nothing more than a computer, operating system, and internet connectivity, or virtual private network (VPN).

1.11 Data Centre is a physical facility that is used to house applications and data. The value chain comprises a mix of segments, including real estate and construction, hardware equipment, utilities (power, water, cooling), networking and software services. Online platforms and websites' digital data, content, and information are stored in the cloud servers located in Data Centres, and the same is accessed by users through broadband connectivity. On user requests, servers in the Data Centres compute and process the required data to make available desired information to the user. Due to the vital role of Data Centres in the digital world, the development of local Data Centres is a priority for both private players and Governments across the countries.

1.12 The Indian Data Centre market size is projected to reach USD 1.5 billion by 2022[1], growing at a CAGR of 11.4%, and is expected to reach ~$5 billion by 2025[2]. The market is primarily driven by growing internet penetration, increased cloud adoption, Government's digitization initiatives, and the push towards data localization.

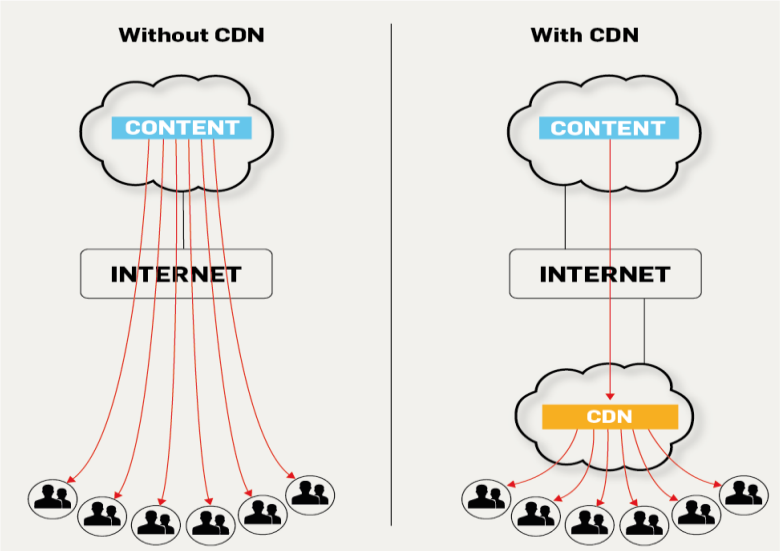
II. Content Delivery Network (CDN)

1.13 CDN is a system of distributed group of servers and networks that deliver pages and other web content to a user, based on the geographic location of the user, the origin of the webpage, and the content delivery server. The group of servers works together to provide fast delivery of

1MarketsandMarkets™ Strategic Insights
2NASSCOM Report – India The Next Data Center Hub, February 2021

internet content. CDNs have emerged as overlay networks on the internet to provide better support for delivering commercial content than was available using basic, best-effort internet packet transport services. A CDN allows for the quick transfer of assets needed for loading internet content, including HTML pages, JavaScript files, stylesheets, images, and videos. The content delivery with and without CDN is shown in Figure 1.2.

Figure 1.2: Content distribution with and without CDN



(Source: globaldots.com)

1.14 To minimize the distance between the users' computer and the websites' server, a CDN stores a cached version of its content in multiple geographical locations (points of presence or PoPs). Each PoP contains several caching servers responsible for content delivery to visitors within its proximity.

1.15 The global CDN market is forecasted to grow by $48.48 bn during 2021-2025, progressing at a CAGR of almost 30% during the forecast period[3]. According to the Cisco Annual report (2018-2023),[4] video comprises more than 50% of the overall data consumed over the internet, which is expected to increase up to 80% by 2025. The demand for various online video formats, such as on-demand video

3https://www.marketsandmarkets.com/Market-Reports/content-delivery-networks-cdn-market-657.html
4https://www.cisco.com/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

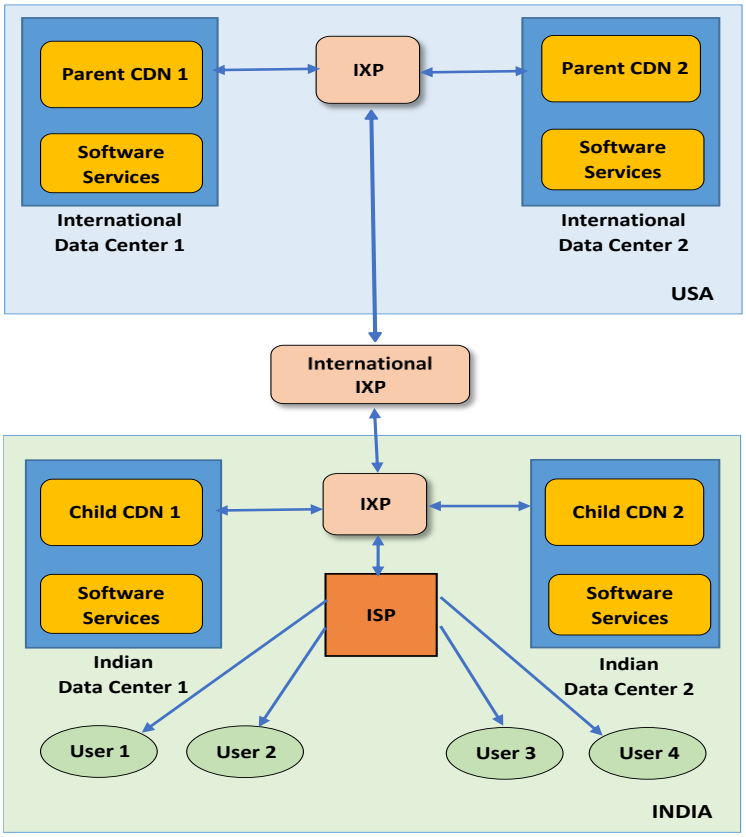
streaming, live video streaming, cloud TV, and over-the-top (OTT), has been continuously increasing over the past few years. Therefore, the rising consumption of web-based, high-definition videos is the major factor contributing to the increase in the adoption of CDN. In addition, the explosion in the use of social networking sites is also one of the major reasons for the increase in videos, photos, animations, and text over the internet. Activities such as transferring, sharing, and posting rich media files, by the content providers as well as individuals have increased the burden on the existing networks requiring the addition of CDN's for smooth operations.

III. Internet Exchange Point (IXP)

1.16 IXP is a technical facility designed to route the traffic quickly and cost-effectively between different network members by enabling interconnection. They are essentially large local area networks that are built with interconnected Ethernet switches. IXPs allow ISPs and CDNs to interconnect their networks locally. This leads to a flatter internet, improves international bandwidth utilization, and reduces the cost and latency of interconnections. IXPs can be grouped into not-for-profit (e.g., industry associations, academic institutions, Government agencies) and for-profit organizations. IXP operators, while still providing public, neutral peering services, may also provide commercial value-added services (VAS), such as security, access to cloud services, transport services, synchronization, caching, etc.

1.17 The traffic exchange between two networks connecting at an IXP is facilitated by an exterior gateway protocol called Border Gateway Protocol (BGP), which makes routing decisions based on network rules, hop counts, and other characteristics configured by network administrators. This saves money on international bandwidth for the ISPs and improves connectivity for their customers by reducing latency. International bandwidth utilization and latency are two crucial factors that affect the end-user experience, when digital platforms and services are used.

Figure 1.3: DC, CDN and IXP elements of an internet ecosystem



1.18 Commercially, the internet consists of a hierarchy of global, regional, national, and local providers. Data Centres hosting CDNs are connected to each other and the internet cloud via IXPs. To enable the access to the content of a parent CDN or website hosted on an international DC, global IXPs interconnect with the local IXPs to pass the traffic to the Indian DCs and thereby to the child CDNs, as shown in Figure 1.3. ISPs provide the last mile connectivity to users for accessing the services. A CDN pays ISPs, carriers, and network operators for hosting its servers in their Data Centres.

1.19 Alongside the operational, interconnection, and bandwidth costs, the number of hops required by a network to reach the destination server on which the content is hosted to process the user request is also critically important. This indicates that there is a necessity for the expansion of the three key digital elements: International DCs, CDNs, and IXPs in India for the advancement of the digital economy.

B. Need for the present consultation

1.20 Out of the notable key drivers for boosting the data economy of India, as shown in Figure 1.1, the Authority (TRAI) has already addressed some of the issues through its following recommendations:

1) Recommendations on Privacy, Security, and Ownership of the Data in the Telecom Sector dated 16th July 2018
2) Recommendations on Cloud Services dated 16th August 2017 and 14th September 2020

1.21 However, not much work has been done in respect of regulatory framework for Data Centres, Content Delivery Networks, and Interconnect exchanges in India. National Digital Communications Policy (NDCP-2018) seeks to unlock the transformative power of digital communications networks to achieve the goal of digital empowerment and improved well-being of the people of India. The missions envisaged in the policy are as follows:

1) **Connect India:** Creating robust digital communications infrastructure to promote 'Broadband for All' as a tool for socio-economic development.
2) **Propel India:** To harness the power of emerging digital technologies, including 5G, AI, IoT, Cloud, and Big Data to enable the provision of future-ready products and services; and to catalyze the fourth industrial revolution (Industry 4.0) by promoting Investments, Innovation and IPR generation.
3) **Secure India:** To secure the interests of citizens and safeguard the digital sovereignty of India with a focus on ensuring individual autonomy and choice, data ownership, privacy, and security, while recognizing data as a crucial economic resource.

1.22 Under the Propel India mission, various strategies have been laid out in the Policy. Strategy no 2.2 mentioned under the Propel India mission relates to *'Ensuring a holistic and harmonized approach for harnessing Emerging Technologies'*. Under this strategy, provision number 2.2(f) envisages that:

2.2 (f) Establishing India as a global hub for cloud computing, content hosting and delivery, and data communication systems and services.

1.1 Evolving enabling regulatory frameworks and incentives for promoting the establishment of International Data Centres, Content Delivery Networks, and Independent Interconnect exchanges in India.

1.2 Enabling a light-touch regulation for the proliferation of cloud-based systems.

1.3 Facilitating Cloud Service Providers to establish captive fiber networks.

1.23 The government has proposed to formulate a scheme to incentivize investments to set up hyper-scale Data Centres in India and boost the capacity of the existing Data Centre ecosystem. MeitY, in November 2020, had released the draft Data Centre policy, which proposed to designate Data Centres as infrastructure and group Data Centres under the essential services category, among other measures. The draft document proposes a policy, including various structural/regulatory interventions, investment promotion in this sector, and seeks to strengthen the "Atmanirbhar Bharat" initiative by identifying possible opportunities for manufacturing Data Centre equipment in the country. The draft policy document discusses issues at a macro level and it may be followed by a detailed implementation scheme. Keeping in mind the above-mentioned NDCP provisions and need for pronouncing concrete action points in making India a global Data Centre hub, the Authority has taken up this initiative on suo moto basis to issue a consultation paper on '*Regulatory frameworks for promoting data economy through establishment of Data Centres, Content Delivery Networks and interconnect exchanges in India*'.

1.24 Through the present Consultation Paper (CP), the Authority intends to seek the inputs of stakeholders on promoting the establishment of (i) Data Centres, (ii) Content Delivery Networks, and the (iii) Internet Exchange Points in the country. The CP has been structured into five chapters. Chapter 1 introduces the background of the subject and sets the context for present consultation. Chapters 2, 3, and 4 discuss the issues in the establishment of Data Centres, Content Delivery Networks, and Internet Exchange Points, respectively. Chapter 5 deliberates on issues related to 'Data Privacy, Security and Ownership' with reference to the past recommendations of TRAI of July 2018, as well as the Personal Data Protection Bill (PDP) of 2019. Chapter 6 summarizes the various issues for consultation.

CHAPTER 2

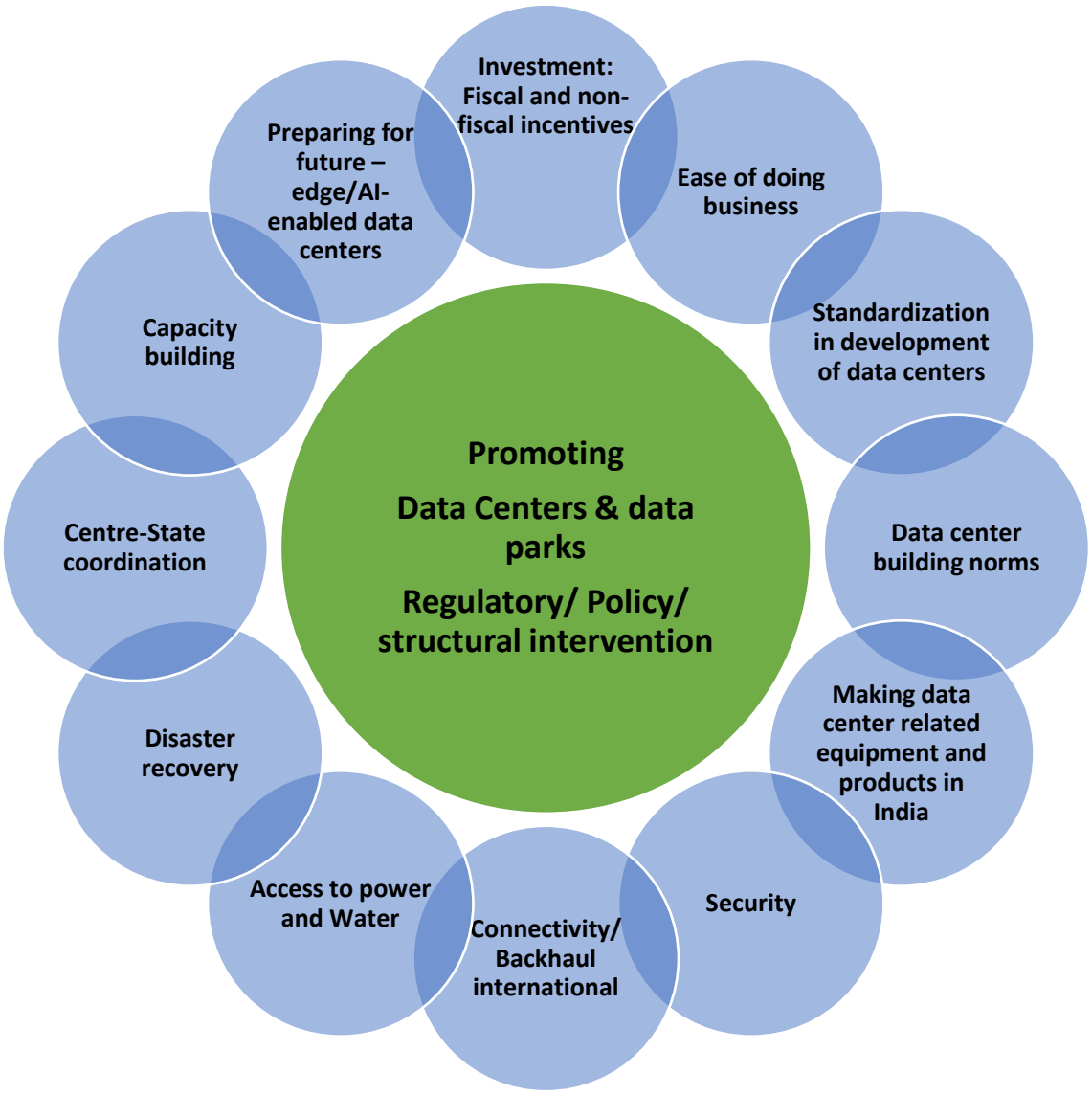
DATA CENTRES

2.1 Data Centres play a crucial role in the digital economy. Everything that happens online is housed in a Data Centre. These Data Centres have become a top priority for businesses across the globe to meet their IT infrastructure requirements. With this shift, Data Centres have moved beyond being just an additional storage facility. It offers scalability, security, efficiency, and state-of-the-art technology that are increasingly demanded by companies and organizations. Also, Data Centres offer a lot, from safety and reliability to energy efficiency and cost reduction.

2.2 The Data Centre infrastructure and services business is a very large emerging business that will boost the digital economy worldwide. These Data Centres are a unique combination of property, energy, and technology. Data Centres have been one of the sectors that are least affected globally and in India due to COVID-19 pandemic, indicating their crucial role in supporting continued business activity. This Data Centre sector is witnessing significant growth in the country and will soon become one of the economic growth engines of India and will generate large-scale investments and jobs. Data Centres (DC) along with Internet Exchange Points (IXPs) and Content Delivery Networks (CDN) together form an important part of digital communication infrastructure and services. National Digital Communications Policy (NDCP)-2018 emphasizes digital infrastructure and services as key enablers and critical determinants of a country's growth and well-being. It seeks to unlock the transformative power of digital communications networks to achieve the goal of digital empowerment and improved well-being of the people of India. The government of India is also becoming increasingly reliant on Data Centres for the Government-to-Citizen (G2C) delivery platforms, such as the National e-Governance Plan (NeGP), e-visa, and National CSR Data portal, to name a few. However, factors like high upfront costs, higher power

tariffs, maintenance-related issues, security, and high real estate costs are increasingly impacting the growth of Data Centres. Also, there are known impediments to its growth such as lack of status as infrastructure, complex clearance processes, time-consuming approvals, lack of published standards, absence of specialized building norms for building the Data Centres, submarine cable network connectivity limited to few states, and high cost of capital and operational expenditure, etc. These elements are shown in Figure 2.1 and are discussed in the following paras:

Figure 2.1: Various elements for promoting Data Centres and parks

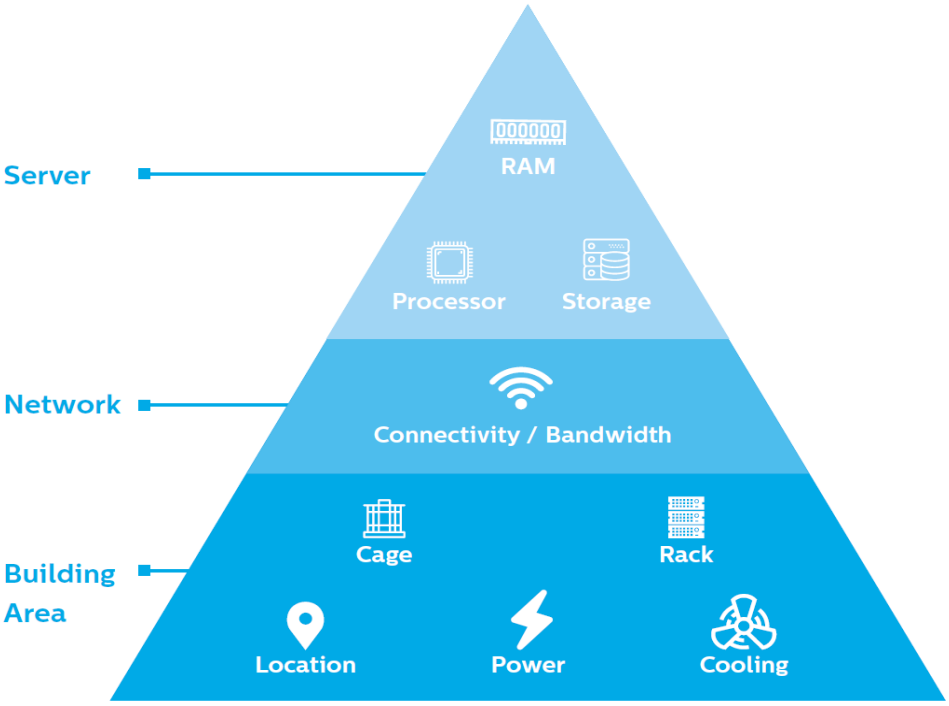


2.3 Data Centres have evolved significantly in recent years. In the past, they were highly controlled physical infrastructures, but the adoption of the cloud has changed that model. When enterprises migrate their data and workloads to cloud Data Centres, they reside in physical infrastructures that are best-in-class on-premises Data Centres. As the data markets continue to move toward on-demand services, the infrastructure has shifted from on-premises servers to virtualized infrastructure that supports workloads across both the physical infrastructure and cloud environments. Initially, only large companies had their own server farms for storing data, but with the increase in web-based applications, a hybrid cloud-based storage industry with third-party storage solutions have come up. India is currently home to 80+ third-party DCs and is witnessing investments in around 15 projects annually, with a growing presence of both local and international players[5].

2.4 In general, Data Centres provide facilities necessary to enable reliable, uninterrupted storage, processing, and transmission of data. The facilities include all kinds of IT equipment, including servers, storage systems to run applications, network equipment like switches, routers, and firewalls, as well as the cabling for connectivity purposes. A Data Centre also contains adequate infrastructure in the building area, such as power distribution and supplementary power systems, racks, electrical switching, ventilation, and cooling systems. The basic building blocks of a Data Centre are represented in Figure 2.2.

[5]NASSCOM Report: India The Next Data Centre Hub – Feb 2021

Figure 2.2: Basic building blocks of a Data Centre



(Source: NASSCOM Cloud)

2.5 The core components of a Data Centre design include routers, switches, firewalls, storage systems, servers, and application delivery controllers. These components store and manage business-critical data and applications. Together, they provide:

a. **Network infrastructure –** This connects servers (physical and virtualized), Data Centre services, storage, and external connectivity to end-user locations.
b. **Storage infrastructure –** Data is the fuel of the modern Data Centre. Storage systems are used to hold this valuable commodity.
c. **Computing resources´ –** Applications are the engines of a Data Centre. Servers provide processing, memory, local storage, and network connectivity that drive applications.

Data Centre — Models

2.6 Various types of DC models are in existence depending upon the ownership and management of the facilities. A specific model depends on whether facilities are owned by one or many organizations, how

they fit into the topology of other Data Centres, what technologies they use for computing, storage, and their energy efficiency. The extent of DC usage generally differs based on size and business operation. Broadly DC investments in India can be categorized into 'Captive' and 'Outsourced' Data Centres. Captive models are Data Centres specifically designed to meet the needs of a business or enterprise, which are not shared with other organizations. On the other hand, the outsourced models are developed and operated by third-party service providers, providing shared services of data management to various organizations. These can be classified as – Colocation Services, Hosting Services, and Hybrid Services. Thus, the DCs can be owned and operated through different models deliberated as under:

A. **Captive Data Centre -** Large enterprises own and operate their own data storage facilities, which are known as captive Data Centres where the data of a single organization is stored and processed. The facility is owned, operated, and maintained by the company whose data is hosted. This DC is also implemented as the Landlord investment model, in which the investor provides basic facilities such as space and/or power. Tenants set up their own servers, facilities, and staff as per their requirements.

   Captive DCs have advantages like control over the infrastructure, security, but are disadvantageous in terms of higher CapEx and OpEx and limited scalability. Investments in captive DCs by private sector enterprises in India have been declining primarily on account of shift of the business to the cloud platforms, even though it's use is growing for Governments and public enterprises. On average, there are new investments in at least 60 captive DC projects annually in India[6]; where demand is primarily driven by the public sector and educational institutions. While it is largely restricted to expansion and up-gradation of the existing facilities for the private sector.

[6]NASSCOM Report – India The Next Data Centre Hub, February 2021

B. **Outsourced Data Centre -** These DCs have advantages in form and of scalability, reduced CapEx, improved physical security but have disadvantages in form of hidden costs and less control over the infrastructure.

i. **Colocation Data Centre:** The organizations buy large spaces and construct the basic Data Centre structure and then lease out space to customers for setting up their own IT equipment. These equipment needs to be maintained by the customers, with the host maintaining the facility. The host also provides additional facilities like engineering services, infrastructure facilities, network services, power, and backup. Tenants pay rent and set up their own servers. Major end-users of colocation services in India include cloud service providers, Banking, financial services and insurance (BFSI), entertainment sector, content delivery network providers and e-commerce organizations.

ii. **Hosting Data Centre:** These Data Centres have servers and related IT equipment that can be leased by customers from the host of a large storage facility. Customers are responsible for the maintenance and operation of these servers, including their organization and security. The majority of the outsourced DC developers/operators, such as NTT Global Data Centres (Netmagic) and CtrlS offer hosting services in India. Also, global cloud service providers such as AWS, Microsoft, Google, IBM, and Oracle offer cloud hosting services for Indian customers through their physical cloud regions in India. On average, hosting services contribute to 50% of the total revenues of the local outsourced DC service providers, while colocation and hybrid services together account for the remaining 50% of the revenue.

iii. **Hybrid Data Centre:** It is a combination of colocation as well as hosting Data Centre. Many larger enterprises continue to rely on on-site Data Centre facilities, particularly for legacy equipment and applications, and some enterprises will combine

cloud with hosting and colocation services, particularly those with a relatively small IT staff. In a Hybrid model enterprise, customers procure infrastructure and host in a colocation facility, while the Data Centre service provider manages the day-to-day operations. In India, the market is still in the nascent stage, with only a few DC operators (such as NTT (Netmagic Solutions) and CtrlS) are able to provide advanced hybrid services. Currently, around 20% of the customers opt for hybrid services. Going forward, this percentage is expected to grow with the increase in the establishment of colocation centres.

These investment models are devised by investors with varying risk exposure. Companies who are conservative about Data Centres may opt for the captive model, while the companies with considerable risk appetite may opt for co-location and hosting models. As per the current market dynamics, demand for co-location models is on the rise in the country.

Benefits of Data Centres on the Economy

2.7 Data Centre (DC) industry has made significant inroads in India. Both Foreign and Indian players have either already launched Data Centres in India or have announced significant DC investments in major cities. India is one of the most capacity-hungry Data Centre markets in the world and holds immense potential to become a Data Centre hub in the Asia-Pacific (APAC) region due to its inherent strengths. Being amongst the fastest-growing major economies of the world, the country also has a rapidly expanding data consumer base. This is further emphasized by the presence of he trained and skilled workforce. Increasing domestic and international demand from sectors such as banking, financial services, telecommunications, technology, and infrastructure is providing further boost to this sector. With the growing reliance on internet services and advanced technologies for data management, there is already a good demand for high-quality DCs.

2.8 By financing capital-intensive projects and Data Centre investments, global and multinational companies such as Amazon Web Services, Microsoft, Google, Equinix, etc. have provided significant economic and employment benefits worldwide. Initial capital investment and the ongoing operational expenditure creates and sustains jobs across the wider economy.

2.9 The thriving Data Centre industry has spilled over benefits to several sectors and industries in form of digitization, which has been a great focus of the Government of India. Data Centres help in creating localized low-cost data storage and processing services which in turn helps the digital start-up ecosystem to get cost benefits. A notable advantage that localized Data Centres provide is the reduction of latency in data access. According to companies that have recently shifted Data Centres to India, there is a 10% latency reduction in shifting from a centre in Singapore[7] and a 30% reduction in shifting from a centre in the U.S. Further, if we compare the cost of manpower, real estate, and bandwidth, India is at least 60% cheaper than the U.S. or Singapore[8]. Thus, storing data locally will reduce network latency. Combined with the impending deployment of 5G, it will further enable low latency and high-speed services in the Indian market.

2.10 DCs being critical hubs for both technological and economic reasons are core for digital infrastructure at a regional, national, and global level. They provide a substantial economic impact to the regions in which they are located through direct, indirect, and induced effects.

2.10.1 The ***direct effect*** is the economic impact directly from a Data Centre construction and operation. Directly supported jobs include positions in management, IT and system technicians, electrical and mechanical maintenance, water management, repair, and hardware operations, etc.

[7] https://www.yotta.com/how-will-data-localization-impact-the-data-center-market-in-india/
[8] ibid

2.10.2 The ***indirect effect*** includes the economic impact through suppliers of goods and services. The Data Centre creation leads to demand for local raw materials. The indirectly supported jobs include positions in security, catering, cleaning and in the construction, and supply industries across the economy.

2.10.3 ***Induced effect*** refers to the economic impact that occurs when employees at the Data Centre and their supplier industries spend their wages throughout the economy. The induced jobs are primarily service-related jobs in industries such as retail trade, transport, accommodation, restaurants, housing, and finance.

2.11 As mentioned earlier in the direct economic effect, Data Centres generate an enormous amount of employment, because they are part of a unique logistics chain consisting of all kinds of companies, from internet exchanges, hosting, and cloud providers, to consulting firms and fiber optic providers. The Uptime Institute has forecasted that Data Centre-related jobs will grow globally from about 2.0 million in 2019 to nearly 2.3 million in 2025. This estimate covers more than 230 specialist job roles for different types and sizes of Data Centres, with varying criticality requirements, right from design to operation[9]. Thus, Data Centres not only provide jobs and create an additional source of income but also strengthen and empower local communities to meet the demands of the modern economy.

2.12 Creation of large campuses/parks for DC purposes leads to allied industries being located closely forming geographic clusters for resource and utility sharing. Forming of DC clusters will likely lead to investments and growth of industries providing solutions for Data Centres such as cooling, uninterrupted power, and high-speed internet connectivity. The establishment of large Data Centres in Tier-2, Tier-3 cities are likely to have the add-on benefits of encouraging ISPs to roll out robust Optical Fiber Cable networks for increased broadband connectivity.

[9] https://uptimeinstitute.com/global-data-centre-staffing-forecast-2021-2025

2.13 The growth of the DC industry leads to knowledge creation and innovation, with major cloud storage providers such as Google extensively training their employees. The suppliers working on the construction and operation of Data Centres also acquire knowledge of the domain, which can contribute to the growth of the industry within India. It also allows these suppliers and employees to export their services to neighbouring countries/locations for DC establishments, that are still in the nascent stages in much of South Asia. This effect has been seen in many countries of Europe where Data Centres were established in Ireland and Belgium.

Effect of Key Data Centre on the Economy – Case of Google in Europe

2.14 To keep all of Google's products and services up and running around the clock, the global tech giant owns and operates Data Centres all over the world. The majority of Google's expenditure (nearly 70%) has gone towards constructing four new Data Centres in Europe. In total, since 2007, Google has spent EUR 2.3 billion in Europe, i.e., on average EUR 200 million per year[10]. On top of the construction expenditure, Google has also spent EUR 0.9 billion on operations of these facilities, i.e., on average almost EUR 90 million per year. Results show that, when considering the direct and indirect economic effects, Google's investments in the four Data Centres and fiber networks have supported an overall economic impact of EUR 5.4 billion in GDP cumulatively over the period 2007-2017, varying between a yearly impact of EUR 0.2 and 1 billion. Broken down as direct, indirect, and induced effects of EUR 1.4, 2.2, and 1.7 billion, respectively.

2.15 Similarly, a larger Data Centre network would imply a bigger economic contribution to the Indian economy. Future growth in user demand for services like cloud, AI, machine learning, and platform services implies that investments in Data Centres will continue to increase over time as in the past. Besides Google, top cloud vendors like AWS, Microsoft,

[10] https://www.copenhageneconomics.com/copenhagen-economics-2018-european-data-centres.pdf

IBM, and Oracle continue to expand their base with the opening of cloud regions in the APAC region and a strong physical presence in China, Singapore, Australia, and India[11]. Five years after opening a Data Centre in Mumbai, Google Cloud announced opening a Data Centre in Delhi soon[12]. In April 2020, Google also announced its planning for a $400m submarine cable that will link India and Italy in 2022. Thus, it is reasonable to expect that Google will continue to expand its investments in Europe and APAC countries like India, and consequently, Google's economic impact would eventually increase across the globe.

International – policy, initiatives for Data Centre industry

2.16 Globally Data Centre investments have grown significantly in the past years, led by key players like Google, Facebook, AWS, Alibaba, and Microsoft. Growth of the digital economy and initiatives for smart cities continue to boost Data Centre investments in many countries. The governments around the globe have been successful in attracting these players to establish Data Centres in their countries. Some of the nations, which have huge Data Centre markets running successfully and wherein the major steps were taken by their respective governments and the incentives provided to the Data Centre players are discussed below:

2.17 **United States –** States of the U.S. are competing to attract Data Centres by offering financial incentives, often by waiving sales or property taxes on the expensive equipment they use. Many states provided sales tax exemption and property tax breaks in some form to enhance the international Data Centre market as follows[13]:

a. Alabama exempts Data Centres from states and local sales and property taxes by a law that offers up to 30 years of tax breaks for

[11] https://www.prnewswire.com/asia-pacific-data-centre-market-outlook-2021-2026.html
[12] https://cloud.google.com/about/locations#asia-pacific
[13] Source: Associated Press research of laws and interviews with economic-development officials in all 50 states

Data Centres investing $400 million and creating at least 20 jobs with an average annual compensation of $40,000.

b. Arizona provided a sales tax exemption for Data Centres that can last up to 10-20 years.
c. In Florida, Data Centres fall under the Florida Enterprise Zone incentives program, which has a qualified target industry tax refund incentive. Under the scheme, companies that create high-wage jobs in the state are eligible for tax reimbursements on their corporate incomes, sales, intangible personal property, and insurance premiums.
d. Georgia offers a sales tax exemption for equipment in Data Centres investing at least $15 million annually, and Atlanta ranks among the leading markets for Data Centres.
e. Colorado provides general job-based tax breaks for Data Centres. H
f. Hawaii offers job creation incentives to Data Centres; however, the dollar value of incentives is confidential.
g. In Wyoming, a law offers Data Centres that invest at least $5 million a sales tax exemption on computer equipment. Data Centres that invest at least $50 million also can get a sales tax break on power supplies and cooling equipment.

2.18 **United Kingdom –** The main reasons behind the UK, especially London being the hotspot for Data Centres are connectivity, a huge demanding customer base, regulatory and legislative stability. Another reason is also the availability of skills where the UK has expertise in sector investments, finance, funding, innovative design, engineering, and construction.

a. **Connectivity**: The UK has unparalleled global fiber connections both in terms of size and reach. The intercontinental fiber reach of London covers global to local needs, and its major internet exchanges provide unparalleled access between multiple continents and Europe.
b. **Investment Security**: The UK's safe structured environment, ownership rights, EoDB, and ROI (return on investment) potentials

attract FDI (foreign direct investment). London, described as the "ultimate place to de-risk", is important considering that Data Centres are among the most expensive real-estate investments in the world.

2.19 **Singapore:** Singapore is the most sought-after APAC Data Centre market and has become a primary hub for cloud services within the region due to its favourable conditions like *robust infrastructure*, *access to fiber*, *talented local workforce,* and great set of community partners. Its telecom sector is the most advanced globally, boasting of first-class connectivity and *admirable network infrastructure*. According to the Singapore Economic Development Board, Singapore is currently home to approximately 50% of Southeast Asia's Data Centre capacity. It has continued to improve in indices and has made substantial improvements in ease of acquiring and registering property. It now takes *less than six days* in Singapore to register a property for building a Data Centre. Similarly, the country's legal framework is strong and substantially well placed to protect its investors against any capital risks. The Government initiated a Next Generation Broadband Network (NGBN) plan in 2015 for a state-wide fiber-based network. NGBN is to increase broadband connectivity, thereby boosting domestic data consumption as well, which in turn increased the demand for Data Centres. Its strong network infrastructure, large content distribution network, diverse connectivity to major APAC markets, pro-business environment, and political stability are some other factors that favour Singapore's preference by Data Centre players. Its *low-tax environment* has also made it an attractive location for large corporations. Zero GST tax rate for international services and exports has attracted many foreign investors. Growth among the small- and mid-size businesses, in turn, increased the demand for public cloud services such as Software as a

Service (SaaS) and Infrastructure as a Service (IaaS). The Government incentive to boost the DC market is[14]:

2.19.1 An approved company under the Pioneer Certificate Incentive (PCI) or Development and Expansion Incentive (DEI) is eligible for a corporate tax exemption or a concessionary tax rate of 5% or 10%, respectively, on income derived from qualifying activities.

2.19.2 Singapore's Data Centre parks also provide power-related infrastructural facilities like on-site power plants, dual power feeds, and redundant sources of network path diversity.

2.20 Singapore established multi-activity zones in the 1960s and specialized SEZs (e.g., petroleum refinery activities) in the 1970s. In the 2000s, its SEZ policy shifted to creating knowledge-intensive clusters through the establishment of innovation-driven SEZs focused on R&D and other high value-added activities. In 2018, the Singapore Cooperation Enterprise, a Singaporean Government agency, signed a tripartite agreement to develop a single electronic window solution to facilitate trade and increase trade efficiencies for the special economic zone in Nkok, Gabon. The other two parties to the agreement were the Gabon Special Economic Zone—an international public-private partnership comprising the Government of Gabon, Olam International (Singapore), and the African Finance Corporation—and the Singapore-based global trade facilitation platform provider vCargo Cloud.[15]

2.21 Nongsa Digital Park (NDP), located in the northeast of Batam, has been upgraded from a technological park to an SEZ. 25 Hectare of the park has been allocated to develop the Data Centres in the first phase, with plans for expansion in the future. This decision has signified NDP as the 'Digital Bridge' between Singapore and Indonesia to grow the digital economy that was identified as a joint growth sector between the two countries during RISING 50 leaders' retreat in Singapore. The Park hopes to become a hub for Data Centres, the Data Centre market

[14] www.edb.gov.sg

[15] https://unctad.org/system/files/official-document/WIR2019_CH4.pdf

growth is expected to intensify in the region, driving demand for "edge Data Centres" located closer to the end-users so they can benefit from lower latency, higher security, and greater control of their data.

2.22 **Malaysia:** Malaysia is one of the preferred destinations for shared services and Data Centres in the APAC region due to various initiatives it has undertaken. The Malaysian DC market is broadly marked by expansion, efficiency, and consolidation. *Ample land*, *good infrastructure*, *educated workforce,* and political stability are the advantages. Due to the presence of many *global network providers*, it has good international network connectivity. Multimedia Super Corridor or MSC Malaysia is a Special Economic Zone initiative for the global IT industry and is designed to be the R&D centre for IT industries. MSC Malaysia status is given to both local and foreign companies that develop or use multimedia technologies to produce and enhance their products and services as well as for product development. The current ecosystem, under which the Government functions, seems to be driving Malaysia's ability to attract Data Centre investments. The incentives are as follows[16]:

I. Freedom to source funds globally for investments.

II. Globally competitive telecommunication tariffs.

III. Income tax exemption (for 5 years and extendable by additional 5 years) on statutory income (or value-added income) derived from services provided about core income-generating activities for MSC.

IV. Unrestrained employment of local and foreign knowledge workers. Malaysia has consistently been ranked as one of the most business-friendly countries in the Ease of Doing Business index. For example, starting a business in Malaysia takes only three days. The country favours DC business investment because of an assured availability of land. Malaysia has the second-fastest process for registering property in Asia. Besides, the country also generates surplus electricity that ensures that an energy-intensive industry

[16] taxsummaries.pwc.com

like Data Centres is assured of a constant supply of electricity. Electricity and energy costs are *minimum* in Malaysia among the South-East Asian countries. Moreover, it has access to renewable power from hydroelectric dams which is appealing for companies with environmental mandates.

2.23 **China:** China leads the world in internet consumption, and the DC market has benefited from the factors of rapid economic growth coupled with the quick adoption of IT and digital services by the Government. Traditional industries are encouraged by policies to embrace digital transformation and ultimately has driven the data market growth, with which China has become the second-largest Data Centre market worldwide—behind the USA. Chinese Government has designated Data Centres as a nationally strategic investment sector since 2017, as part of a policy to encourage further investments in advanced technologies like cloud computing, AI, and Big Data, which is now allowing more Government-supported Data Centre deployments. The regional Chinese Governments are also promoting a Data Centre sector as a means of advancing regional economic development. For example, Hubei Province is aiming to create a Data Centre cluster in China as North Virginia is doing in the USA. Several cooperation projects are signed between the Hubei Government and ZTE Corp. The Hubei Government has set up efforts in a phase-wise manner to provide infrastructure and encourage investment to help ZTE finish the Data Centre project in 2020 and achieve long-term goals. China's regulator Ministry of Industry and Information Technology (MIIT) has formulated a separate license called *Internet Data Centre (IDC) license* in 2015. Operators require an IDC license to build or lease Data Centre services. Investors establishing a Data Centre in China must review a variety of considerations, ranging from the local climate to infrastructure quality and tax incentives. Local authorities in lower-tier cities are generally more open to establishing new centres and often provide tax and land incentives. Data Centres

within China's tech parks also enjoy more favourable Government policies and better amenities.

2.24 **Hong Kong:** Hong Kong has emerged as the key regional Data Centre location because of its low tax rate, well-established legal system, extensive business network, reliable energy supply, reliable network connectivity, blooming start-ups, and IP protection. The Government support for a Data Centre includes land supply by industrial estates, availability of greenfield sites for sale, land earmarked specifically for Data Centres, facilitation units and thematic portal, waiver/fee exemption for using parts of existing industrial buildings, and tailor-made lease modifications of industrial lots for Data Centre use.

Demand drivers for Data Centres in India

2.25 Presently, with the Digital India initiative, the Government is pushing for the growth of the digital economy through supporting Data Centre development. The Government of India recognizes the importance of digital infrastructure and utilizes public and private clouds to deliver solutions to Indian citizens. Increased penetration of the internet (including in rural areas) and the rapid emergence of e-commerce are the main factors for the continued growth of the Data Centre market in the country. Also, many IT and software companies are now migrating to cloud-based business operations that are contributing to the Data Centre co-location and hosting services in India.

2.26 Major workforce was compelled to go remote due to the pandemic, which has led to an increasing number of companies investing in IT and cloud services. This rising digitization has given a stimulus to the demand for Data Centres in the past few years. The need for scaling up the data processing and storage requirements has been underscored by the increased data consumption during the lockdown. A CBRE report[17] forecasts technology, fintech, pharmaceuticals/healthcare, education, and media and content to be

[17] http://cbre.vo.llnwd.net/India_Major%20Report_Data%20Centres_The%20Next%20Charged%20Up%20Wave

the key drivers of the Data Centre segment. On account of more users coming into the fold of technology, technical convergence, the proliferation of Industry 4.0, the upward trajectory will sustain the Data Centre segment in the country. Digital inclusion will play a pivotal role in attracting investment in Data Centres and dispersing Data Centres to Tier-2 or Toer 3 cities and creating skilled jobs.

I. Data Explosion

2.27 India has witnessed a digital thrust since the enhanced focus by the Government on the Digital India flagship program to improve online infrastructure and increase digital literacy and penetration, with several initiatives leading to an unprecedented digital explosion. Digital adoption has become critical for personal and business needs; moreover, this digitization push accelerated during COVID-19, with data-usage-per-subscriber rising at an all-time high of 12GB per month in the quarter ending September 2020[18], amidst increased work-from-home, online education, OTT consumption, online gaming, and casual internet use during the lockdown. With the cheapest data tariffs in the world, affordable smartphones, the data usage would effortlessly increase from 12GB/user/month currently to 25GB/user/month by 2025[19]. To support these overlaying volumes of data explosion, Data Centre storage space growth is inevitable.

2.28 Indian Data Centre market investments are expected to grow at a CAGR of 5% (~2X of the global market) to reach $4.6 billion per annum by 2025[20]. The Data Centre market is witnessing a continuous uptrend owing to growing internet penetration, increased adoption of cloud, rising use of big data analytics and IoT, increased thrust on data localization, and other data economy factors. Below is a peek into the factors that will continue to drive Data Centre investments in India:

[18] TRAI Performance Indicator Report
[19] ANAROCK Navigating the India Data Centre Lifecycle Report
[20] NASSCOM Report: India The Next Data Centre Hub – Feb 2021

2.28.1 **Internet penetration:** Being the second largest internet market, India has an internet user base of over 750 million subscribers by the end of December 2020[21], which is expected to reach one billion by 2025. Digital adoption has increased data traffic and pushed the occupancy rate of colocation Data Centres, with several investors planning to expand their capacities across major locations.

2.28.2 **Cloud adoption:** The pandemic has accelerated the rate of cloud adoption, and India's public cloud services are expected to reach $5 billion by 2023. This shift has pushed increased investments in hyper-scale Data Centres with the global DC market investments expected to reach ~$200 billion per annum by 2025, and India is expected to account for 2.3% of these total investments.

2.28.3 **Big Data and IoT:** Big data analytics is expected to grow at a CAGR around 29% to reach $68 billion by 2025. Number of IoT devices is expected to reach around 75 billion in 2025, generating 79.4 zettabytes of data, accounting for a need for more data storage space. India is expected to be a frontrunner in the Internet of Things (IoT) adoption in Asia-Pacific requiring huge Data Centre space.

2.28.4 **Data Economy factors -** India is set to become a thriving data economy in the APAC region with growing digital services. Indians are the largest audience of social media and OTT platforms. OTT subscribers are 30 million as of July 2020[22], and this number is likely to grow with an increased smartphone and internet penetration. Mobile points of sale transactions are expected to rise from US$ 16 Bn in 2020 to US$ 44 Bn in 2024 (28% CAGR)[23]. Also, digital commerce usage is expected to rise from US$ 57 Bn in 2020 to US$ 94 Bn in 2024 (13% CAGR)[23].

2.29 The NDCP–2018 has emphasized accelerating Industry 4.0 to develop a market for IoT/ M2M connectivity services in sectors including Agriculture, Smart Cities, Intelligent Transport Networks, etc. The

[21] TRAI Performance Indicator Report
[22] https://www.ibef.org/blogs/india-s-ott-market
[23] statista.com

Government of India has also announced many M2M or IoT mega projects, which have the potential to impact socio-economic life. Some of them are:

I. Development of 100 Smart Cities project and rejuvenating 500 others by the Ministry of Urban Development.
II. The Ministry of Power has taken up 14 Smart grid pilots with an average customer base of around 20,000 each.
III. The Ministry of Road Transport has mandated that all commercial vehicles of more than 22 seating capacity be enabled with GPS, emergency calls, etc.

Thus, M2M will continue to see strong growth with technological, political, and economic factors coming together. Also, with the enhancement in M2M communications, the amount of data will increase tremendously, thereby stimulating the growth of the Data Centre industry.

2.30 During the pandemic, the DC sector have played a critical role in keeping the country online, which made service providers to fast track their planned expansions. The investments in capacity expansion by operators worldwide picked up since Q3 2020 owing to the surge in demand in the DC market. Data Centres will also become one of the most preferred forms of alternative real estate asset, with the focus shifting to large hyperscale developments. The widening e-commerce network in India will boost the DC segment, as it increasingly needs help in managing its growing database. Passing policies such as the National E-commerce Policy, NDCP-2018, Personal Data Protection Bill, and the Policy framework on Data Centre by the Government will accelerate demand.

II. 5G rollout

2.31 The Data Centre continued to remain an essential aspect of the Telecom and IT industry. With the increasing data storage demands of the telecom sector, Data Centres are becoming a more strategic asset

for telecom operators. Data Centres that were used primarily to support internal functions, are today used to deliver end-user applications, including content and video. The investments made by the telecom providers in their Data Centre offerings are thus allowing them to leverage their assets to build another segment of business to earn revenue. As networks ramp up their support for 5G and IoT, the DC providers are focusing on the edge and the increasing need to locate more capacity close to the end-users, while TSPs are re-evaluating the role of their Data Centres.

2.32 Introduction of 5G in India will bring forward more content in the marketplace, and thereby generate demand for more storage. 5G technology will transform the industry by revamping its existing processes and infrastructure. Small cell technology will be used heavily to roll out 5G coverage. Moreover, 5G connectivity will introduce the idea of 'many to one' methodology where the user's endpoint device will need to communicate with many towers or antennas of the small cells, at the same time, thereby requiring more Data Centres. Data Centres will need to be close enough to these cells to maintain 5G's low latency performance and meet service-level agreements. Data Centres that have been set up for 4G will have the capacity for handling 5G data; however, they will have to change their infrastructure to cater to 5G's frequencies. Micro Data Centres might even be deployed at the base of cell towers, allowing limited data processing with even faster response times for critical applications.

2.33 The infrastructure of 5G wireless networks will be based on Software-defined networking (SDN), which provides communication arrangements between cloud applications and services and a user's mobile terminal. Network Functions Virtualization (NFV) is another major driver of change in the telco Data Centre. NFV often planned in conjunction with SDN transformation will give TSPs the ability to use network resources more efficiently. The future of Data Centres in the upcoming 5G SDN era will have a major impact on the telco Data Centre networking domain, including the various implementation

scenarios and approaches of new challenges. As TSPs transform their Data Centres to support SDN and NFV, demand escalates for a set of Data Centres especially operating for telecom needs.

2.34 **Telecom Data Centres**: A telecom Data Centre is a facility owned and operated by a Telecommunications or a Service Provider company. These Data Centres generally require very high connectivity and are mainly responsible for driving content delivery, mobile services, and cloud services. Telecom providers may run the Data Centre within a Data Centre similar to a Colocation Data Centre. As India is turning to be a favorite market for the cloud ecosystem (Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service), telecom companies are keen to get a place in the lucrative Data Centre market, partner with global players looking to offer value-added services, and rollout 5G services. For example, Nextra by Airtel has a nationwide portfolio of around 10 large Data Centres and more than 120 edge Data Centres, providing customers with co-location services, cloud infrastructure, managed hosting, data backup, disaster recovery, and remote infrastructure management. Airtel Nextra will invest Rs 5,000 cr to expand Data Centre business plans to build seven hyper-scale Data Centres, which will triple its capacities and help India become a regional hub for Data Centres. As per news reports even Reliance Jio Infocomm Ltd plans to build a data centre in Uttar Pradesh at an investment of around $950 million[24]. This is driving a change to telecom Data Centre demands for network operators.

III. Data Localization

2.35 Data localization laws are gaining prominence, such as GDPR in Europe and Cybersecurity Law in China, owing to their rapid digital development. With many organizations going through a technological shift via Data Centre decommissioning and migration to the cloud, the need to secure data privacy has become more urgent in the context of

[24] https://www.livemint.com/industry/telecom/jio-plans-near-1-billion-data-centre-in-uttar-pradesh-11614039904599.html

organizations, considering the emerging threat scenarios and implications of a data breach. A Gartner release informs that 80% of enterprises are expected to migrate away from on-premises Data Centres to the cloud by 2025. However, the proposed Data Protection Bill may empower the Government to exempt such companies, which only process the personal data of foreign nationals who are not present in India. This move may incentivize these companies to ramp up their Data Centre capacity in the country. Storing data locally will reduce network latency and improve speed. With this, some of the latest providers with resource ownership will be able to build massive capacities of Data Centres at much higher scalability and quality but at much-reduced costs.

Data explosion + Data localization = India –> the new Data Hub in Asia

IV. India- The new Data Centre hub

2.36 With the data localization rules coming in, existing Data Centre capacity will end up being highly constrained. Data localization has laid the stone for the development of hyperscale Data Centres in India to cater to this increasing data consumption demand. India currently needs to ramp up its Data Centre capacity by at least 15 times in the next 7 to 8 years to be able to handle the massive amount of data influx that will enter its borders because of data localization. Service providers like NTT (Netmagic), ST Telemedia, CtrlS, Yotta Infrastructure Solutions, RackBank are investing in DC development to support the unprecedented demand that will arise through data localization policy. India is a more viable and economic place to build and operate large-scale Data Centres. Data explosion along with the Government's decision of data localization will surely make India a Global Data Centre Hub.

2.37 India holds an enormous potential to become the 'next destination' for Data Centres propelled by the policy initiatives, increasing customer

base, and corporate requirements for data storage. Its relative position in the Asia-Pacific region also means that neighboring countries may look to India as a key provider of infrastructure to the region like Singapore. The increasing demand for cloud services induces global internet companies such as Amazon, Apple, Facebook, and Google to amplify global Data Centre capacity growth. This may very well provide an opportunity for the cloud and IT companies to invest in the APAC region, especially India to develop the capacity.

India – policy, initiatives for Data Centre industry

2.38 Despite the wide demand and progress of the Data Centres, in reality, the establishment of a Data Centre has many hurdles from a selection of location, acquiring permissions, building and operational costs, infrastructure, and availability of resources, security, data management, etc., to handle the storage facilities.

2.39 The Data Centre establishment requires tremendous investment at the preliminary stage due to costly real estate, power infrastructure, water requirement and improving wide area network connectivity. Acquiring land, obtaining permits, and ensuring an uninterrupted power supply are major requirements for establishment of Data Centres. Land requirements depend upon the tier, i.e., space capacity *(refer to Annexure I for Data Centre tiers)* of the Data Centre. According to the CBRE report[25], the land required for captive Data Centres is at least 20,000–40,000 sq. ft., and that for third-party Data Centres is at least 100,000–200,000 sq. ft. Similarly, the investment in the construction of a Data Centre would depend on its tier. The investments needed to construct a Tier 4 Data Centre would, on average, be INR 24,000–25,000 per sq. ft. and for a Tier 3 centre, the cost would be INR 16,000–18,000 per sq. ft. Based on the geographies of the location there are differentiations in the construction costs, thereby affecting the site selection process.

[25] https://www.realtynmore.com/India-Is-India-the-next-frontier-for-the-data-centre-industry-June-2018.pdf

2.40 Many Data Centres have been set up in India, but the focus of Data Centre players have been on Tier-1 cities like Mumbai, Pune, Chennai, Delhi for various reasons like the presence of robust connectivity, uninterrupted power supply, excellent local market, availability of skilled manpower, etc. The Tier-2, Tier-3 cities, and the rural areas lack infrastructure, power, and fiber connectivity. The taxes levied on the real estate make it difficult to buy large parcels of land for a Data Centre. This leads to increased costs deterring players from entering this segment. The real estate players can shift their focus to Tier-2 cities, which could prove to be more reliable, offering affordable real estate options and lower labour costs. Tier-2 cities can also be a hotspot for hosting disaster recovery sites for the main Data Centres. Considering the potential of such cities, the only areas of improvement are transport connectivity, internet connectivity, and the power supply in these regions. Table 2.1 gives an outlook of several Data Centres in major cities in India. The area map shows that there is a clear lack of opportunities for Data Centres expansion in the north, northeast, and central regions, though there is a substantial internet penetration and digital services explosion in those regions. As of September 2021, there are 172 colocation Data Centres from 26 areas in India[26].

Table 2.1: Number of Data Centres operating in India as of September 2021

Location	No. of DCs
Delhi-NCR	26
Bengaluru	31
Chennai	14
Pune	10
Mumbai	25
Ahmedabad	8
Kolkata	9
Hyderabad	11
Other cities	38

(Source: datacentermap.com/India/)

Figure 2.3: Data Centres area map

[26] https://www.datacentremap.com/india/

2.41 Annually, the Indian market is witnessing investments in a few Data Centre projects from DC service providers. Maharashtra continues to dominate with an investment share of over 50% in the market. While Mumbai and Chennai remain the foremost choices, the other metro cities of Hyderabad, NCR and Bangalore are also of interest given the huge catchment of urban population and large enterprises. Even Tier 2 and Tier 3 locations offer significant cost advantages and have the potential to overtake Tier-1 cities, especially because of the low labour costs, manpower requirement of the industry, and economically valued real estate available in those regions. The favorable policy offered by some of these states have also played a part. Table 2.2 summarizes fiscal and non-fiscal incentives offered by some of the states. Whilst the data requirements of Tier-2 cities are on the rise because of a decentralized workforce, there will be an increased demand for rapidly deployable smaller colocation Data Centres built closer to smaller cities. Building Data Centres in new Tier-2 cities where internet use is booming is also a strategic business move, as it would help in easing congestion and speed up internet services, creating increased opportunities for edge DCs in the country.

Table: 2.2 Data Centre policies of various states

S. no.	State and DC Policy	Key Provisions
1	**Maharashtra**[27] (IT/ITES Policy – 2015)	a. DCs will be covered under Essential Services and Maintenance (ESMA) Act b. DCs are eligible for the below fiscal incentives that are provided for IT/ITES units: c. 100% stamp duty exemption to new IT/ITeS units d. Electricity duty exemptions for 10 years e. Electricity tariff – power supply at industrial rates f. Property tax is levied at par with residential rates g. Registered IT/ITES units shall be exempt from octroi/Local Body Tax (LBT)/entry tax/escort tax or any other cess h. Allowing setting-up of IT/ITES units in any zone

[27] http://di.maharashtra.gov.in/IT_ITES_Policy_2015_final_English.pdf

2	**Telangana**[28] (Telangana Data Centre Policy – 2016)	**Fiscal Incentives:** 1) Incentives for expansion of IT/ITeS shall be applicable for Data Centre firms a. Allotment of Govt. land based on eligibility criteria b. IT is classified as industrial units for levying industrial power tariff category c. Green initiative: promote energy efficient equipment usage d. 100% reimbursement of stamp duty, transfer duty and registration fee e. Reimburse the cost of filing patents/copy rights to companies having R&D units in Telangana 2) Establish dual power grid networks, renewable energy under open access system, provide power at the cost of generation 3) Up to 50% rebate on building fees 4) Land shall be provided at a subsidized cost **Promoting Startups/SMEs:** 5) Additional preference to Startups/SMEs for procurement of DC services by the Government 6) 25% subsidy on lease rentals for 3 years 7) Specific R&D grants 8) Patent filing costs will be reimbursed up to INR 2 lakhs **Non-Fiscal Incentives:** 9) DC Firms are classified under 'Essential Services' 10) Exemption from power cuts, exemption from inspections under factories act; wages act; Shops and Commercial Establishment Act, etc.
3	**Gujarat**[29] (Establishment of Data Centre – 2017)	All the incentives under IT/ITeS policy (2016) for promoting IT/ITES parks and units are applicable for DCs also a. Allotment of Govt. lands to the IT/ITeS Industry b. Capital subsidy @ 25% of CapEx in buildings and infrastructure, excluding the cost of land. c. 100% reimbursement of stamp duty/registration fee/conversion fee d. Power tariff subsidy at the rate of Re. 1 per unit for 5 years e. 100% reimbursement for electricity duty paid for 5 years f. Lease rental subsidy for eligible IT/ITeS units, at the scale of 50 sq.ft. per employee, for 5 years g. Interest subsidy @ 5% for micro and @7% for SME enterprises for 5 years h. Reimburse tax paid under Section-13 of Gujarat VAT Act i. 100% reimbursement of Central Sales Tax (CST) j. VAT/CST/GST reimbursement for a period of 8 years k. Patent assistance at the rate of 50% reimbursement
4	**Odisha**[30] (Odisha State Data Centre Policy – 2020)	Incentives in the ICT Policy for IT/ITES industries shall be applicable for DC firms **Fiscal Incentives:** 1) Allotment of govt. land 2) Building fees subsidy: up to 50% reimbursement 3) Electricity subsidy – industrial tariff is applicable, electricity duty and inspection fee exemption for 5 years 4) Internet bandwidth subsidy: 50% reimbursement of internet bandwidth/leased line charges per year per unit for 5 years 5) 75% Reimbursement of patent filing costs for R&D IT units **Non-Fiscal Incentives:** 6) DC industries/units are classified as 'Essential Services' under ESMA act and as 'Public Utility' services 7) Exempt from provisions of factories act; Shops and Commercial Establishment Act; labor act, etc.

[28] https://it.telangana.gov.in/telangana-data-centre-policy-2016/
[29] http://vibrantgujarat.com/writereaddata/images/pdf/project-profiles/Data-Centre.pdf
[30] https://startupodisha.gov.in/wp-content/uploads/2021/07/AIA-3.pdf

5	**Uttar Pradesh**[31] (Uttar Pradesh Data Centre Policy – 2021)	**Fiscal Incentives:** 1) Interest subsidy up to INR 50 crore per park 2) Capital subsidy of 7% per DC unit 3) 25%, 50% land subsidies in specified regions 4) 100% stamp duty exemption for purchase/lease of land 5) 100% electricity duty exemptions for 10 years 6) Dual grid lines power supply and exemption from wheeling/transmission charges **Non-Fiscal Incentives:** 7) DC industries are classified under ESMA act 8) 24x7 water supply, special provisions in building norms 9) Open access system to purchase power, deemed distribution license, deemed franchisee status, 24x7 power supply, etc. 10) Exempt from inspections under factories, wages acts, etc. 11) Non disturbance provision, preference in public procurement.
6	**West Bengal**[32] (West Bengal Data Centre Policy – 2021)	**Fiscal Incentives:** 1) 100% exemption of stamp duty and registration fees 2) Electricity duty waiver for 5 years **Non-Fiscal Incentives:** 1) Dual power grid networks, 'industrial status' to electricity supplied to DCs, power and internet facilities to Edge DCs 2) 24x7 uninterrupted power supply and internet connectivity 3) 24x7 water supply 4) Single-window approvals and permits for companies willing to establish captive firms 5) Special provisions in building norms 6) RoW provisions as per 'West Bengal Broadband Policy 2020' for laying OFC to and from DCs

Attracting investments through fiscal and Non-Fiscal incentives, including Ease of doing business

2.42 As per the World Bank, Doing Business Report 2020[33], India is ranked **63** among **190** countries in doing business. Business Regulations affecting 12 areas of a business are covered in this report, which ranges from starting a business, dealing with construction permits, getting electricity, registering property, getting credit, protecting minority investors, paying taxes, trading across borders, enforcing contracts, resolving insolvency, employing workers, and contracting with the Government.

2.43 In the TRPC Data Centre Security Index (DCSI) 2020 report[34], India ranked 14th among 18 APAC countries, which gives a composite

[31] http://invest.up.gov.in/wp-content/uploads/2021/02/Data-Centre-Policy-english.pdf
[32] https://www.eqmagpro.com/2021/09/West_Bengal_Data_Centre_Policy_2021.pdf
[33] https://www.doingbusiness.org/en/data/exploreeconomies/india
[34] The TRPC Data Centre Security Index 2020 Report: https://trpc.biz/the-trpc-data-centre-security-index-2020/

statistical measure of the different risks that can impact Data Centres' activities. It provides a snapshot of exposure of Data Centres to elements that can threaten their integrity, disrupt their activities, and jeopardise their reputation when they operate in a given country. The indicators are grouped under six major types of risk – Infrastructure Risk, Energy Risk, Natural Risk, Business Risk, Political Risk, and Legal Risk – providing a holistic assessment of an economy's risk profile. Small countries like Malaysia, Thailand, and Indonesia are ahead of India in these ranking indices.

2.44 The National Digital Communications Policy, 2018, envisages establishing India as a global hub for cloud computing, content hosting and delivery, and data communication systems and services[35].

2.45 The draft National Data Centre Policy 2020, released by MeitY on 3rd November 2020 aims at creating a favourable climate for investments in the Data Centre Sector, both domestic investments and Foreign Direct Investments, and incentivizing the growth of a robust and sustainable Data Centre sector in the country. The policy aims to promote R&D for manufacturing and development of Data Centre related products and services for domestic and global markets. In addition to promoting domestic manufacturing, including non-IT as well as IT components, to increase domestic value addition and reduce dependence on imported equipment for Data Centres.[36]

2.46 The various policy and regulatory enablers are essential to promote the Data Centre industry and strengthen India's positioning in the global Data Centre market. At the same time, minimum regulation and maximum facilitation policy are critical to incentivizing Data Centres in the country. For encouraging foreign investment in Data Centres, it is important to have a robust and easy-to-comply with licensing and regulatory framework in place. EoDB is more important than incentives, and at the same time, this is essential for building

[35] https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf
[36] https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf

confidence with other countries to have their data stored in India. When looking at the worldwide Data Centre distribution, ease of doing business is one of the primary factors for a company to choose a specific region or country to expand its market. Hence, the bottlenecks in ease of doing business (EoDB) need to be addressed, and suitable incentivizing opportunities need to be created by early framing of desirable and attractive policies of investment in this sector.

2.47 The four critical aspects in Data Centre are Land, Power, Telecom and IT Element/Networks and Ease of Doing business. A new Data Centre requires close to 30 approvals/permissions[37] from different central and state Governments' departments before a Data Centre can start operations. For instance, **Annexure II** shows the large number of clearances required to build a Data Centre even in a Tier 1 city like Mumbai, Delhi-NCR, Bengaluru, Chennai, etc. Specified timelines for clearance should exist to prevent delays. The land acquisition process faces bottlenecks of multiple clearance/compliance, several restrictions based on building codes, industrial zones, etc. Approvals and land acquisitions continue to challenge the Data Centre project propositions, leading many international cloud providers to look back on their capacity expansion plans in India. Promoting ease of doing business in itself is one of the most important non-fiscal benefits that a government can offer to Data Centre players. Accordingly, MeitY's draft policy on Data Centres discusses the issue of simplifying clearances through a single window, time-bound clearance system by State Government/Union Territories. It also mentions publishing a list of approvals/clearances required with the defined timelines for obtaining the same.

2.48 The National Single Window System (NSWS) that has been conceptualized and announced by the Department for promotion of Industry and Internal Trade (DPIIT), will enable investors/entrepreneurs/businesses to identify and obtain all

[37] https://community.nasscom.in/sites/default/files/report/25264-nasscom-recommendations-data-centre-policy.pdf NASSCOM: Recommendations for Data Centre Policy

clearances needed to start a new business operation in India through a single online portal. This platform provides the investors with information on pre-operations approvals required to commence a business. Currently, the portal has more than 560 approvals/licenses from across 28+ central ministries/departments and approvals/licenses from across 14 States. The ministry-wise approvals, which are onboarded, are identified as most critical, critical, and non-critical. Invest India, under the guidance of DPIIT, is managing the Maadhyam (NSWS) project and is involved in onboarding various ministries and states on the portal. In addition, the NSWS will systematically integrate with existing State Single Window Systems as well. From the portal, it can be seen that 45 approvals of the Department of Telecom and 19 approvals of the Ministry of Information and Broadcasting have been identified and are being integrated on the portal. Accordingly, there is a possibility that all the permissions/clearances required by Centre/States/UTs are listed and given through this portal.

2.49 Apart from EoDB, Table 2.2 summarizes various other **non-fiscal incentives** that some of the Indian States are offering. The same are listed below:

a. DC industries are classified under ESMA act
b. 24x7 water supply, special provisions in building norms
c. Open access system to purchase power, deemed distribution license, deemed franchisee status, 24x7 power supply, etc.
d. Exempt from inspections under factories, wages acts, etc.
e. Preference in public procurement
f. Power and internet facilities to edge DCs
g. Single-window approvals and permits for companies willing to establish captive firms
h. Special provisions in building norms
i. RoW provisions for laying OFC to and from DCs
j. Exempt from provisions of factories act; shops and commercial establishment act; labor act, etc.

k. Waiving of import restrictions and duties on essential Data Centre operational equipment.

Fiscal Incentives and Exemptions

2.50 Establishing large Data Centres in India would require a lot of investment. Data Centre costs mainly consist of capital expenditure and operational expenditure:

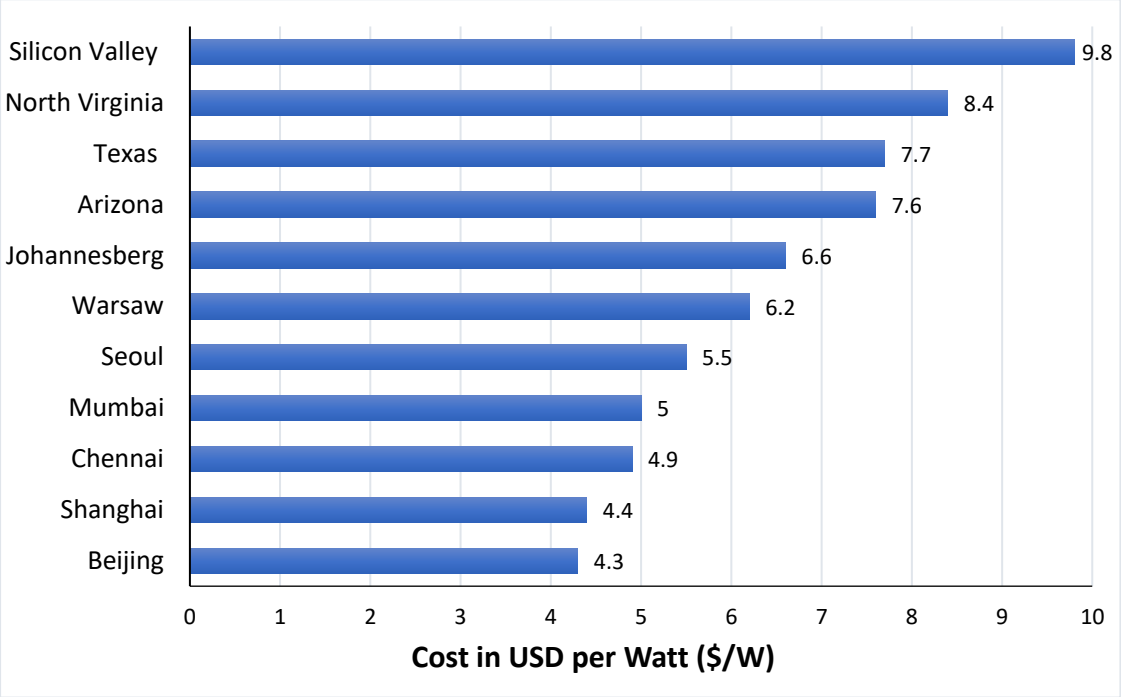
a. **Capital Expenditures** (CapEx) are one-time constructional costs, land costs, investment towards infrastructure setup required to build the Data Centre, wages for construction workers, buying and installing the equipment required for processing and storage, cooling solution, power ancillaries, etc., as part of greenfield rollout.
b. **Operational Expenditures** (OpEx) involve recurring expenditure towards the continued operation of the Data Centre, including the cost of broadband connectivity, cost of power for equipment operation, as well as for cooling, repairs, and annual expenditures like wages for employees.

2.51 In North America, it is observed that building costs in California's Silicon Valley and New Jersey remain high at $9.8/W. The market experts express that U.S. investment and growth would become focused on lower-priced markets such as North Virginia ($8.4/W), Texas ($7.7/W), and Arizona ($7.6/W)[38]. In India, as well, the intra country differences in cost of building and maintaining a Data Centre would vary widely across cities and states, which in turn would be instrumental in directing investment. The construction cost for an average DC in India is calculated at $6.0/W. Chennai ($4.9/W) and Mumbai ($5.0/W) boast lower building costs than most of the developed countries, however, the cost escalates multiple times for other parts of the country (shown in figure 2.3 below). It, therefore,

[38] https://www.turnerandtownsend.com/en/perspectives/data-centre-cost-index-2020/
The cost model includes **equipment, construction labour, materials, etc., and** does not include any client direct costs, land purchase costs, utility works, groundworks, site works, active IT equipment, fibre cabling to support office fit outs or professional services fees.

becomes imperative to incentivize the DC players through various fiscal incentives.

Figure 2.3: Global comparison of Data Centre Construction market



(Source: Data Centre cost index 2020 | Turner and Townsend)

2.52 Data Centres incur one-time and recurring taxes that have a significant impact on long-term costs for any Data Centre. The capital-intensive nature of a Data Centre attracts relatively high sales taxes and property taxes. Moreover, electricity tariff, stamp duty charges, import duties on equipment sourced from outside India, and multi-jurisdiction tax implications further impact Data Centre costing. Friendly tax jurisdictions play a big factor in choosing a place for establishing a Data Centre and complex tax jurisdictions do just the opposite. Tax incentives for building infrastructure for large Data Centres and cloud services within the country should be allowed to encourage data localization.

2.53 In the US, several state Governments offer low property and sales tax rates on power infrastructure, equipment, and electricity to attract Data Centres, subject to certain investment and employment

thresholds. Many countries in one or other way are providing incentives/tax benefits to promote Data Centre sector. Similarly, some states in India like Maharashtra, Telangana, Gujarat, and Andhra Pradesh have formulated their own state DC policies and are already providing considerable incentives in their state-level policies. For instance, the Maharashtra Government announced the GST refund for a maximum period of 10 years for the companies that participate in the development of integrated facilities. Similarly, the Andhra Pradesh Government announced a 50% reimbursement of SGST on the purchase of raw materials and equipment for three years from the date of approval of the project. Likewise interested players may be supported in the form of tax rebates wherever applicable. A country-wide data-centre-specific tax and duty incentive may be adopted to encourage investors to operate here.

2.54 Table 2.2 also summarizes **various fiscal incentives** that some of the Indian States are offering. These are listed below:

1. Power tariff subsidy at the rate of Re. “x” per unit for “y” years
2. “x” % reimbursement for electricity duty paid for “y” years
3. Electricity tariff – power supply at industrial rates
4. Exemption from wheeling/transmission charges
5. Establish dual power grid networks, renewable energy under open access system, provide power at the cost of generation
6. Registered IT/ITES units shall be exempt from octroi/Local Body Tax (LBT)/entry tax/escort tax or any other cess
7. Allowing setting-up of IT/ITES units in any zone
8. Allotment of Govt. land based on eligibility criteria
9. Land provided at a subsidized cost OR “x”% land subsidies in specified regions
10. Property tax is levied at par with residential rates
11. Up to “x”% rebate on the building fees
12. Lease rental subsidy for eligible IT/ITES units, at the scale of “x” sq. ft. per employee, for “y” years

13. Capital subsidy @ “x”% of CapEx in buildings and infrastructure, excluding the cost of land or capital subsidy of “x”% per DC unit
14. Interest subsidy up to INR “XX” crore per park or interest subsidy @ “x”% for Micro and @“y”% for SME enterprises for “z” years
15. “x”% reimbursement of stamp duty, conversion fee, transfer duty and registration fee
16. VAT/CST/GST reimbursement for a period of “x” years
17. Patent assistance at the rate of “x”% reimbursement
18. Internet bandwidth subsidy: “x”% reimbursement of internet bandwidth/leased line charges per year per unit for “y” years

In view of the aforesaid, the Authority would like to know the views of the stakeholders on the following questions.

Q.1: What are the growth prospects for Data Centres in India? What are the economic/financial/infrastructure/other challenges being faced for setting up a Data Centre business in the country?

Q.2: What measures are required for accelerating growth of Data Centres in India?

Q.3: How Data Centre operators and global players can be incentivized for attracting potential investments in India?

Q.4: What initiatives, as compared to that of other Asia Pacific countries, are required to be undertaken in India for facilitating ease of doing business (EoDB) and promoting Data Centres?

Q.5: What specific incentive measures should be implemented by the Central and/or the State Governments to expand the Data Centre market to meet the growth demand of Tier-2 and Tier-3 cities and least focused regions? Is there a need of special incentives for establishment of Data Centres and disaster recovery sites in Tier-2 and Tier-3 cities in India? Do justify your answer with detailed comments.

Data Centre Parks

2.55 Data Centre parks are specialized secure Data Zone, strategically located with the most conducive non-IT and IT infrastructure, and regulatory environment for housing a mix of small scale/large scale clusters of Data Centres to serve the high needs of compute, storage, networking, and provision of a wide range of data-related services[39]. To encourage expansion, a solid strategy for Data Centre parks is required. The Indian Government intends to encourage the private sector to build Data Centre parks in major metropolitan cities, preferably semi urban areas. Data Centre parks are needed to provide capacity for hyperscale investments in India. Furthermore, to increase the country's technological comprehensiveness, a focus on building Disaster Recovery (DR) Data Centre infrastructure, edge Data Centres in Tier-2 and Tier-3 cities needs to be prioritized. The Government has been promoting the establishment of Data Centres even before the COVID-19 outbreak and as a fallout of it, various state administrations across the country have established their own technology parks. They in-turn, invite Data Centre operators and charge a fee to lease the space with electricity and other basic amenities. The Uttar Pradesh Government plans to develop a Data Centre park which will be set up near Greater NOIDA. Another entity in this space has signed an MoU with the Government of Tamil Nadu to set up a Data Centre Park in Chennai. Similarly, the Andhra Pradesh government has accorded clearance to set up an Integrated Data Centre Park, Integrated IT and Business Park, and Recreation Centre in Visakhapatnam.

Q.6: Will creation of Data Centre Parks/Data Centre Special Economic Zones provide the necessary ecosystem for promoting setting up of more Data Centres in India? What challenges are anticipated/observed in setting up of new Data Parks/zones?

[39] https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf

What facilities/additional incentives should be provided at these parks/zones? Do give justification.

Data Centre – Standardization

2.56 The maintenance of minimum standards for Data Centres are essential for operation and for establishing trust with end-users by ensuring a basis for QoS requirements. These standards become even more significant to maintain DC for third-party storage centres. There are multiple standards that Data Centres across the world comply with for both infrastructure and QoS. Presently, there are no guidelines for minimum or specific design requirements and standards that are required for ensuring data integrity, data safety, etc., which is crucial for DCs. This section looks at enabling feasible regulations and standards for Data Centres operating in India.

I. Standards and Certificates

2.57 The most common standards are ISO 27000, PCI DSS, HIPAA, TIA 942, or AICPA SOC. These international standards have been developed, updated as necessary, and tested for many years by experts from different industries and geographies. They have proven to be an effective way to ensure data protection. The standards were developed with the help of manufacturers, end-users, consultants, and architects, according to IEEE. The standards largely specify the telecommunications standards for Data Centres and other similar facilities by standardizing cabling specifications and layout.

2.58 The ANSI/TIA-942 standards also specify design elements such as the designated spaces to be maintained, the cabinets required for equipment, floor layouts, and site selection processes. TIA-942 Data Centre Standards describe the requirements for the Data Centre infrastructure in a thorough, quantifiable manner under four levels (called tiers) of Data Centres, which are specified in **Annexure I**. Akin to ISO, TIA does not itself provide any certification services and nor does it empanel any auditors to do so. Independent auditors can be

used to certify these standards many of which are already doing so domestically. The usual re-certification period for Data Centres is 3 years.

2.59 Quality of service standards are also specified by the Uptime Institute, which classifies Data Centres into tiers based on uptime percentage in a year (**Annexure I**). They define QoS based on the time that a Data Centre is unable to provide services to its customers by allowing them to access the data stored at the centre. There are a set of other associated standards that are recognized in India that Data Centres can comply with. These include ISO 9001 standards on quality management, ISO 14001 standards on environmental performance enhancement and OHSAS 18001 standards on occupational health and safety management. Certification for these standards can be obtained from several private organizations that independently audit and certify compliance.

2.60 Major IT/telecom/networking products being used across Data Centre markets are primarily based on global standards. Harmonization of these standards to work across the Data Centre markets is critical. India being a large and open market for DC launch, it may therefore be necessary that minimum standards for Data Centre operations should exist considering the local needs. Countries like Germany and Mexico have defined their independent DC standards and tiers, which also provide tier certifications. It can be argued that in India too, independent DC standards can be adopted, which will specify the minimum quality and safety requirement/provisions to minimize chances of any disruption. Thus, there can be a case for standardization and certification in form of the Indian national standards. Besides, there is a need for a testing and certification framework for hardware equipment as well as the software used in Data Centre facilities. Additional steps can be taken to form a body that can coordinate for training, certification, and standards. The Government can consider adopting the discussed global standards for certifying Data Centre operations to clear any ambiguities in the form

of impact on the ease of doing business. This will make it easier to confer benefits, tax incentives, exemptions, and security requirements upon Data Centres.

2.61 A list of certifications from both national and international bodies can be spelt out for the operation of a Data Centres in India. Independent Energy and Security auditors can also monitor Data Centre operations.

II. Data Centre Building norms

2.62 Data Centre buildings are unique in many aspects: they require less parking space and have a higher roof height of 5m and above (as they need to stack large generators and large diesel tanks). The Telecommunications Industry Association (TIA), a trade association of USA accredited by ANSI (American National Standards Institute) and BICSI (Building Industry Consulting Service International), specifies the requirement of DC standards and design. In general, core sites have buildings for the installation of indoor rack line-ups as defined by TIA, BICSI, and other data-centre-centric standards. In India, the National Building Code of India (NBC 2016) does not recognize 'Data Centre' as a separate category. In absence of separate building norms, DCs have to follow commercial office building norms. This unnecessarily raises costs as various requirements based on personnel presence that are relevant to other commercial buildings may not be relevant to Data Centres.

2.63 Many countries are either following the above DC standards or have defined their own independent DC standards (like Germany and Mexico). India too can adopt independent DC standards, which will specify the minimum quality and safety requirement/provisions to minimize chances of any disruption. A standard Data Centre building approval guideline across the country for all the municipal corporations can be helpful for Data Centre companies to build their pan-India plans without many variations and get the approvals of regional authorities within stipulated timelines.

2.64 Realizing that Data Centres should be a separate category under National Building Code, draft policy of MeitY on Data Centres states "*Data Centre buildings require different norms as compared to other offices/commercial buildings and therefore, there is a need for the creation of a separate category code for Data Centres in the National Building Code of India (NBC 2016).*" MeitY's policy further mentions that "*As an interim measure, MeitY shall collaborate with authorized Central Government bodies for drafting broad guidelines to be issued for Data Centre buildings, facilitating specialized construction and safety approvals*".

Q.7: What should be the draft broad guidelines to be issued for Data Centre buildings, so as to facilitate specialized construction and safety approvals?

Q.8: Is there a need to develop India-specific building standards for construction of Data Centres operating in India? If yes, which body should be entrusted with the task? Do provide detailed justification in this regard.

Q.9: Till India-specific standards are announced, what standards should be followed as an interim measure?

Q.10: Should there be a standard-based certification framework for the Data Centres? If yes, what body should be entrusted with the task?

Q.11: Should incentives to Data Centres be linked to the certification framework?

Making Data Centre related equipment and products in India

2.65 MeitY's policy intended to promote local manufacturing by encouraging the use of indigenous hardware (IT as well as non-IT equipment) and software products used in the Data Centres, thereby reducing the overall import burden of the country. Moreover, it aims

to strengthen the testing and certification framework for the Data Centre ecosystem, including for the IT and non-IT equipment and software products pertaining to Data Centres operations. One of the objectives of the policy includes strengthening the testing and certification framework for the Data Centre ecosystem, including for the IT and non-IT equipment and software products pertaining to Data Centre's operations, incentivizing global equipment manufacturers to set up manufacturing units of IT/non-IT components in India, catering not only to local demands but also for export purposes.

2.66 The Authority previously submitted recommendations on "Promoting Local Telecom Equipment Manufacturing" in August 2018 that would enable the Indian telecom equipment manufacturing sector to transition from an import-dependent sector to a global hub of indigenous manufacturing. The objective of the recommendations was to help achieve Net Zero telecom imports by 2022 in the country and to have a strategic interest in the domestic manufacturing of telecom equipment.

2.67 The Authority is separately working on further recommendations that can be proposed to the Government for boosting local ICT equipment manufacturing, and therefore, this aspect has not been covered under this consultation paper.

Disaster Recovery (DR)

2.68 A disaster recovery (DR) site is a facility that any organization can use to recover and restore its infrastructure and operations when its primary Data Centre becomes unavailable. Most of the data-based companies carefully plan and decide about what kind of DR site they require, its location, and a balance of costs against any risks. Since operational disruption is a risk for the operatives, the DR site should always be chosen taking into consideration the weather patterns, seismic risk profile, capability of the ground to withstand the foundations, and other natural phenomenon.

2.69 The two fundamental DR site options are: internal and external. A Data Centre company itself sets up and maintains an internal site, while an external site is maintained by an outside provider. Companies with large information requirements and aggressive recovery time objectives are more likely to use an internal DR site. The internal site is typically a secondary DC and allows a company to recover and resume operations following a disaster at the primary DC. But this secondary physical DR site involves investments in additional DC space, connectivity, and servers. This leads to additional OpEx pertaining to power, cooling, site maintenance, and manpower requirements.

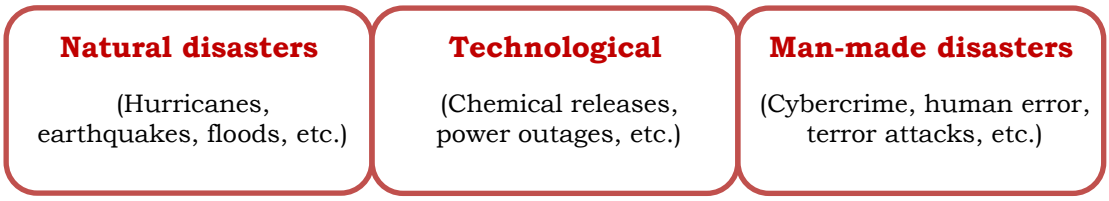
2.70 External DR sites are cost-effective where an outside provider owns and operates an external DR site. External site options are hot, warm, and cold sites:

a. At a *hot site*, an organization has access to a fully functional DC with hardware and software, personnel, and customer data, and is ready to operate in the event of a disaster.
b. A *warm site* is an equipped DC but does not have customer data. Additional equipment is installed to introduce customer data when a disaster occurs.
c. A *cold site* has the infrastructure to support IT systems and data, but no technology until an organization activates DR plans and installs the equipment.

2.71 There can be various disaster scenarios, as shown in Figure 2.4 for which the companies and organizations should be prepared beforehand. The outages can range from a simple application failure to the disaster of the whole Data Centre. Data Centre operators in the northern part of India are running into new challenges posed by the impact of earthquakes and frequent seismic activity. It is worth noting that seismic activity is a concern for anyone building a new DC in northern and northeast regions. Disaster Management is one of the top priorities for all organizations to lay specific emphasis while choosing building designs, location, and standards for a Data Centre.

Disaster mitigation plans should include provisions to address earthquakes, floods, tsunamis, or any other natural/technological/man-made disasters for the setting up of Data Centres.

Figure 2.4: Types of Disasters



2.72 While setting up a new DC, the site should be as protected and made resilient as possible, and secondly, the Data Centres require sufficient server capacity to ensure a high level of operational performance and allow to scale up or scale-out, depending on the requirement. Considering these factors, external DR sites for setting up hot sites that are fully functional DCs and are ready in the event of a disaster can be given thought as a feasible and low-cost option for expanding DCs in non-crowded regions in the country. The hot sites for disaster recovery provide virtual machine snapshots of physical or virtual servers from the primary Data Centre and also functions as a fully operational independent Data Centre.

2.73 As inferred from Table 2.1, the vast majority of Data Centres are currently located in Tier 1 metropolitan areas however, the shrinking of the land bank and the increasing pressure on the power supply is making Tier-1 cities a difficult proposition to build and maintain Data Centres. The internet, on the contrary, has opened the world to Tier 2 and Tier 3 city dwellers. Better networks and affordable tariffs have made them devour the online world. This has prompted a rise of new locations for disaster recovery and edge Data Centres in Tier 2 and 3 cities where data consumption is growing. To ignite growth engines in India, it is needed to consider locating the external DR sites for Data Centres largely in Tier-2 and Tier-3 cities, while comprehending

demographic advantages. There appears to be a tremendous promise in Tier-2 and Tier-3 areas depending on factors such as low land costs and labour expenses, and manpower requirements, amongst other things. Hosting Data Centres and DR sites in Tier-2 and Tier-3 cities meet the demands of disaster management and a possible way for expansion of Data Centre market in low priority states of India coupled with deeper penetration of optical fibre and internet in unserved and underserved areas. Accordingly, Authority has already sought the views of stakeholders on required incentives for promoting establishment of Data Centres and disaster recovery setup in Tier -2 and Tier-3 sites in India in Question 5 above.

Disaster Recovery standards

2.74 ISO 22301 covers the continuity of business as a whole, considering any type of incident as a potential disruption source (e.g., pandemic disease, economic crisis, natural disaster, etc.), and using plans, policies, and procedures to prevent, react, and recover from disruptions caused by them. These plans, policies, and procedures can be classified into two main types: those to continue operations if the business is affected by a disruption event and those to recover the information and communication infrastructure if the ICT is disrupted.

2.75 ISO 27031 is a tool to implement the technical part of ISO 22301, providing detailed guidance on how to deal with the continuity of ICT elements to ensure that the organization's processes will deliver the expected results to its clients. ISO Standard 27031 is focused on the information and communications technology (ICT) requirements for business continuity and disaster preparedness. ISO 27031 includes both crucial data security and enterprise operations of an organization or business.

2.76 Since Data Centre players already provide disaster recovery site planning depending on the type of data handles, uptime required, customer insistence and technical standards, the Authority has not specifically dealt with the aspect in this consultation paper. However,

stakeholders may bring out any specific issue in this regard if they so desire.

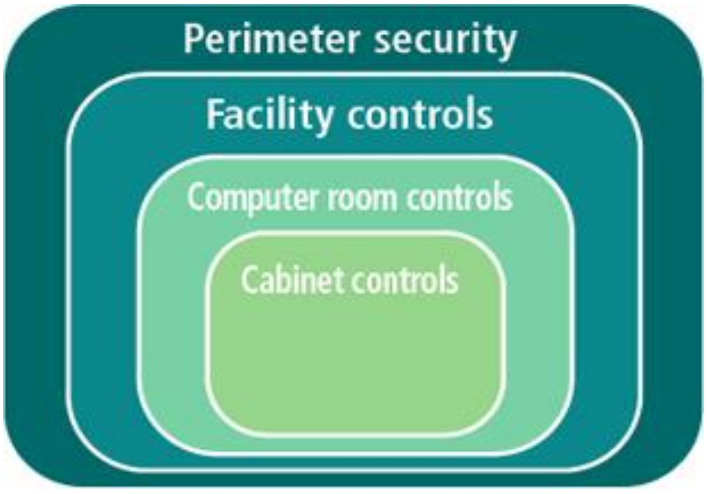
Q.12: Are there any specific aspects of the disaster recovery standard in respect of Data Centres that needs to be addressed? If so, then provide complete details with justification.

Data Centre Security

2.77 Data Centre facilities hold confidential information or proprietary information and hence must be both physically and digitally secure. Compliance and security are top priorities to guarantee that data is protected in a Data Centre. Everything from networks and power generators to the physical infrastructure should be designed and installed, keeping the Data Centre security standards in mind.

2.78 Physical security of a Data Centre comprises various kinds of built-in safety and security features to protect the premises and thereby the equipment that stores critical data for multi-tenant applications. The most optimal and strategic way to secure a Data Centre is to manage it in terms of layers (Figure 2.5). Layers provide a structured pattern of physical protection, thus making it easy to analyse a failure.

2.79 **Figure 2.5: Four layers of Data Centre physical security**



2.80 The security measures can be categorized into four layers:

First layer of protection (Perimeter security): The first layer of Data Centre security is to discourage, detect, and delay any unauthorized entry of personnel at the perimeter. This can be achieved through a high-resolution video surveillance system, motion-activated security lighting, fiber-optic cable, etc.

Second layer of protection (Facility controls): In case of any breach in the perimeter monitoring, the second layer of defense restricts access. It is an access control system using card swipes or biometrics.

Third layer of protection (Computer room controls): The third layer of physical security further restricts access through diverse verification methods, including monitoring all restricted areas, deploying entry restrictions such as turnstile, providing VCA, providing biometric access control devices to verify finger and thumb prints, irises, or vascular pattern, and using radio frequency identification.

Fourth layer of protection (Cabinet controls): The first three layers ensure entry of only authorized personnel. However, further security to restrict access includes cabinet locking mechanisms. This layer addresses the fear of an "insider threat," such as a malicious employee. After implementing the first three layers well, cabinets housing the racks inside the computer room also need to be protected to avoid any costly data breach.

2.81 For the safety and security of the premises, factors ranging from location selection to authenticated access of the personnel into the Data Centre should be considered, monitored, and audited vigorously. To prevent any physical attacks, the following need to be considered:

a. likelihood of natural disasters such as earthquakes, risk of flooding, proximity to high-risk industries in the area, etc. Some of these risks could be mitigated by barriers or redundancies in the physical design of Data Centre.

b. availability of network carrier, power, water, and transport systems.
c. an access control system with an anti-tailgating/anti-pass-back facility to permit only one person to enter at a time.
d. a single-entry point into the facility.

2.82 Software security involves techniques to prevent unauthorized access to the data stored on the servers.

2.83 The standards that make up the ISO/IEC-27000 series are a set of standards created and managed by the International Organization for Standardization (ISO) and the International Electronic Commission (IEC). ISO/IEC-27000 "provides an overview of information security management systems" and first published in 2009, was updated in 2012, 2014, 2016, and 2018.[40]

2.84 The 27000 series are aimed at establishing good practices in relation to the implementation, maintenance, and management of the Information Security Management System (SGSI) or by its name in Information Security Management System (ISMS). These guidelines aim to establish best practices in relation to different aspects related to information security management, with a strong focus on continuous improvement and risk mitigation. ISO 27000 is comprised of six parts outlining the requirements for certification, guidelines for achieving the requirements, and guidelines for accrediting organizations. The standard provides many useful recommendations for companies seeking certification as well as those merely interested in improving their security.

2.85 In view of concerns over national security, the government has mandated that Internet service providers (ISPs) must purchase equipment approved by it. As part of the aforementioned security concerns, DoT in this regard had also amended its License Agreements in March 2021 and National Cyber Security Coordinator (NCSC) has been appointed as the nodal agency by the government for all ISPs to

[40] https://www.iso.org/standard/73906.html

provide information as and when sought. NCSC has also been tasked to notify a list of trusted procurement sources along with the equipment that does not pose any threat to India's national security.

Data Centre Audit

2.86 Internal audits at Data Centres check the implemented systems and processes. An external audit is used to check the commitment of internal audits. Audits should check for any vulnerabilities in the Data Centre facilities that are provided to ensure security. As an outcome of the audit checks, any facility requiring extra protection should receive additional security. There are also standards that Data Centres need to meet. Some of the standards are ISO 27001, ISO 20000-1, or SOC 1 Type 2, SOC 2 Type 2, and SOC 3. Also, it is important to conduct a risk assessment study in compliance with standards and implement appropriate security controls to ensure the overall security of a Data Centre. A security audit and certification boost the confidence of entities in a Data Centre for hosting their data there. Such a framework can help in making India a favorable destination for hosting International Data Centres.

Q.13: Whether trusted source procurement should be mandated for Data Centre equipment? Whether Data Centres should be mandated to have security certifications based on third-party Audits? Which body should be entrusted with the task? Should security certifications be linked to incentives? If so, please give details with justifications.

Fibre Connectivity

2.87 High-quality fiber connectivity is a must requirement for Data Centre operations as they run critical applications that need 24x7 uninterrupted connectivity to store and distribute the data. That is why DCs are generally constructed in areas with dense fiber networks that can connect them to reliable and high bandwidth internet access components. Good network connectivity is playing key criteria in

deciding the site for a DC construction in India, and thereby majority of the Data Centres are concentrated in Tier-1 cities like Mumbai, Chennai, and Hyderabad.

2.88 As newer Data Centres are constructed, and the utilization of optical fiber cable grows, more capital expenditures on the creation of new fiber infrastructure will be required. The development of proper connectivity could thus enhance the establishment of Data Centres. As the average broadband speed in India is very low and uneven across cities, this affects the performance (QoS) of the Data Centres. Lack of access to quality broadband and capacity restrictions of the fiber and cable is the critical challenge faced by many clouds and DC service players.

2.89 The Data Centre provider needs to offer seamless and scalable fibre connectivity between the infrastructure of enterprises and between the two or more Data Centre buildings. In India, the state of intercity and intracity fibre networks are far from what exists in other developed countries. Data Centre providers or Cloud Service Providers or CDN providers presently are forced to procure generic network connectivity services from local TSPs. This is problematic because traditional networks operated by TSPs are principally designed for voice or public data services, such as IP services. They are not suitable for many new services, which require very high bandwidth availability and low latency for extremely high amounts of data. Achieving these outcomes using TSP services is especially difficult given India's vast geography and relatively limited existing technology infrastructure and broadband connectivity speeds. The Authority in its recommendations[41] on **"Delivering Broadband Quickly: What do we need to do?"** in 2015, has issued a list of action points to facilitate a 'Host in India' campaign in the spirit of 'Make in India':

a. *"The Government needs to encourage local and foreign companies to build 'Data Centre Parks' on the lines of industrial parks, SEZs, etc.,*

[41] https://trai.gov.in/sites/default/files/Broadband%3D17.04.2015.pdf

by providing them land, infrastructure and uninterrupted power supply at affordable rates."

b. *"Presently, telecom companies are subject to license fee on Data Centres, but non-telecom companies are not. The anomaly needs to be addressed at the earliest."*
c. *"Adequate policy initiatives for attracting global content hosting should be formulated. The global data hosting, which does not pertain to India, should be kept beyond the purview of Indian laws."*

Recently, TRAI in its Recommendations on "*Roadmap to Promote Broadband Connectivity and Enhanced Broadband speed*" dated 31st August 2021 has recommended for action/ measures for creation of robust Digital Communications infrastructure creation as stated below:

a. *Creation of National RoW Portal to overcome the issues of RoW permissions for telecom infrastructure as well as for other essential utility services.*
b. *Incentivize establishment of common ducts and posts, to be shared on non-discriminatory basis with service providers and infrastructure providers.*
c. *Establish a central entity, 'Common Ducts and Posts Development Agency (CDPDA)' for planning and development of common ducts and posts infrastructure across the country, on non-exclusive basis.*
d. *Mandates co-deployment of common ducts during the construction of any roadway, railway, water pipelines, and gas pipelines receiving public funding.*
e. *To facilitate the sharing of passive infrastructure such as ducts, optical fibers, posts, etc., all the passive infrastructure available in the country should be mapped by each service provider and infrastructure provider using Geographic Information System (GIS). The Telecom Engineering Centre (TEC) should notify the standards for this purpose.*
f. *Establishment of e-marketplace(s) on common GIS platform to facilitate leasing and trading of passive infrastructure.*

Access to Dark Fibres

2.90 Dark Fiber is an existing optical fiber line that is not in use currently and can be used to create a privately operated optical fiber network. The need for greater network connectivity and faster performance puts demand pressure on existing telecom infrastructure, thus increasing the value of unutilized dark fiber as an alternative option for Data Centres. Over the past year, dark fiber has become a hot commodity, as cloud computing platforms seek more network capacity to deliver data across their massive Data Centre campuses. Globally, several companies have targeted this opportunity by deploying new dark fiber routes to connect major Data Centre hubs.

2.91 Indian Data Centres may use dark fiber to overcome degraded network performance. Though expensive, these avoid latency, provide greater bandwidth, stability, and security. However, a dark fiber network is considered telecom infrastructure and can only be accessed through a licensed partner. In India dark fiber can be acquired through IP-I registration, and the license holder, i.e., the Telecom Service Provider has the authority over dark fiber for sale or lease or share to the interested agency based on agreements. Consequently, companies who want to operate Data Centres should undergo commercial agreements with TSPs, even if the services they provide are of non-telecom connectivity. Moreover, services provided by TSPs are significantly expensive, which substantially increases Data Centre costs. Attracting investments and promoting competition in this segment is, therefore, a challenge. The entities like Data Centres providers can be allowed to construct, operate, and efficiently manage their own captive optical fiber networks.

International connectivity

2.92 Some of the biggest enterprise Data Centre developers—Google, Facebook, Microsoft, and Amazon—now are also major investors in new submarine cables. The amount of capacity deployed by these providers has outpaced internet backbone operators in recent years.

These Data Centres/content providers accounted for less than 10% of cable capacity prior to 2012, but their share of total capacity surged to 66% in 2020[42]. Submarine cables connect the digital economy across the world. If Data Centres are the heart of the digital economy, then submarine cables are the arteries of modern connectivity. These cables terminate in the country through cable landing stations (CLS). Access to submarine CLS is an essential input for services requiring international connectivity. As of December 2020, there are 17 under-sea cables landing in 15 cable landing stations in 5 cities across India[43]. Mumbai and Chennai have the maximum concentration of such landing points. The cables connect Mumbai and Chennai to various strategic cities in South and Southeast Asia, the Middle East, Africa, and Europe. Given the higher cost of pulling the cable inland, these two cities remain the favourites for most operators to locate their initial Data Centres. Hence, Mumbai and Chennai, which have a fair share of existing and upcoming landing stations, will be the preferred locations for future supply also. The non-availability of submarine cables and fiber networks for international connections is the main drawback for the companies not establishing DCs in the north, central, and northeast regions.

Q.14: What regulatory or other limitations are the Data Centre companies facing with regards to the availability of captive fiber optic cable connectivity, and how is it impacting the Data Centre deployment in the hinterland? How can the rolling out of captive high-quality fiber networks be incentivized, specifically for providing connectivity to the upcoming Data Centres/data parks? Do justify.

Q.15: What are the necessary measures required for providing alternative fiber access (like dark fiber) to the Data Centre

[42] https://blog.telegeography.com/2021-submarine-cable-map
[43] https://www.submarinenetworks.com/stations/asia/india

operators? Whether captive use of dark fiber for DCs should be allowed? If so, please justify.

Q.16: What are the challenges faced while accessing international connectivity through cable landing stations? What measures, including incentive provisions, be taken for improving the reliable connectivity to CLS?

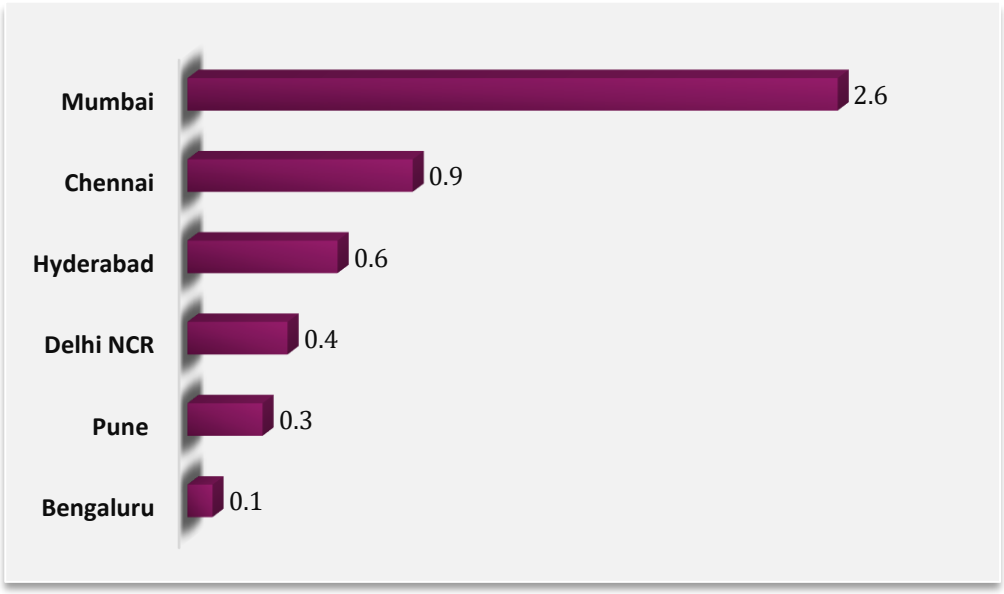
Access to Power and water

2.93 The most important and often overlooked criteria when selecting a DC facility or colocation provider when evaluating DCs is power. Data Centre market demand and supply is often measured in terms of electricity absorption and consumption, respectively, specifically in Kilowatts (kW) and Megawatts (MW). The growing importance of power is remaking the business of leasing DC space, with megawatts (indicating IT power load) replacing square feet as the primary benchmark for real estate deals.

2.94 India's Data Centre capacity is expected to grow from 375 MW in H1 2020 to 1,078 MW by 2025[44], presenting a USD 4.9 billion investment opportunity (refer figure 2.6 below). Mumbai is expected to garner a significant share of this impending opportunity owing to its existing Data Centre infrastructure, followed by Chennai and Hyderabad. India's sustainable growth is being challenged by the increased energy consumption of DCs, and with the IT activities, the energy challenges are bound to increase.

Figure 2.6: Distribution of USD 4.9 bn Greenfield investments by 2025

[44] https://www.jll.co.in/content/dam/jll-com/documents/pdf/research/apac/india/jll-re-imagine-data-centres-running-india-s-digital-economy-h1-2020.pdf



(Source: JLL Research)

2.95 Despite making remarkable progress in electricity distribution over the years, India still faces challenges in meeting its growing power demand. In FY 2020-21, the country's energy supply deficit stood at 1,441 MU.[45] The reliable supply remains low in the country with unstable grid connectivity in many parts. Rural areas in many northern and eastern states typically receive less than 20 hours of grid supply.[46] The average daily supply in urban areas (22 hours) is longer by a couple of hours than in rural areas (20 hours), with an overall average of 20.6 hours of power supply from the grid per day due to which Mumbai is a preferred location for most of the DC vendors, with the presence of multiple Power Generation companies offering services. The power issues must be expeditiously sorted out to skyrocket the DC expansion in all the cities.

2.96 **Power expenses:** The power supply alone, with approx. 50%-60% of the total operating cost creates the largest cost heads for a DC business. The power and cooling segment of the Indian Data Centre power and cooling market is expected to reach $1,065.5 million by 2025, growing at a CAGR of 9.4% during the forecast period 2019–

[45] https://powermin.gov.in/en/content/power-sector-glance-all-india
[46] https://www.ceew.in/publications/state-electricity-access-india

2025[47]. Further, the integration of renewable energy into the power grid is fundamental for improving the sustainability of Data Centres but causes significant challenges for grid management that will possibly increase the operational costs in near future.

Provisioning of Power tariffs and subsidies

2.97 Considering the power deficiency situation that exists in various parts of the country, the establishment of dual power grid networks to ensure uninterrupted quality supply of electricity to the Data Centre is required. Additional power generation capabilities through captive power sources such as solar and wind farms should be installed to supplement power sourcing.

2.98 In India, the majority of Data Centres are in Maharashtra, Karnataka, Tamil Nadu, Telangana, Uttar Pradesh, and New Delhi. The State Governments have already laid down power tariffs and subsidies, and this has become instrumental for DC's growth. Table 2.2 lists some of the initiatives taken by State Governments in respect of power availability and tariffs for incentivizing the DC players.

2.99 Given the significant consumption of fuel by backup power sources such as generator sets, fuel subsidies to the eligible players will improve the Data Centre foundation in rural and Tier-2 cities and divert the concentration of Data Centres in already crowded Tier-1 cities. Certain Data Centre companies have shown an interest in funding research on renewable-energy-based solutions for Data Centres. For example, companies like Netmagic are experimenting with renewable energy for bundling or part-powering their units. Energy or duty tax may be exempted to benefit the industry in a situation where many outsourcing companies are experimenting with renewable energy for bundling or part-powering their units.

[47] https://www.researchandmarkets.com/reports/4866498/indian-datacenter-power-and-cooling-market?utm_source=dynamic&utm_medium=GNOM&utm_code=zs68sm&utm_campaign=1345565+-+India+Datacenter+Power+and+Cooling+Market+Outlook+2019-2025+-+Growing+Demand+for+IaaS%2c+SaaS%2c+and+PaaS+Among+Organizations&utm_exec=joca220gnomd

Promoting Green Data Centres

2.100 In Europe, there is the climate-Neutral Data Centre pact, which has the goal of making Data Centres climate-neutral by 2030 as part of the European Green Deal, a law that aims to make all the European Union Climate-neutral by 2050. Green Data Centres are the modern-day Data Centres that can keep emissions low. For India, it plays a more important role, since India suffers due to the energy and water crisis. Most big Data Centres could slash their greenhouse gas emissions by switching to efficient, off-the-shelf equipment, and improved energy management. The green Data Centres need to be brought to a strong place in the country. Tulip Telecom, a green, energy-efficient, and cloud-ready Data Centre that was built by IBM in just nine months, is a clear example that this is not a hindrance with green technology in place.

2.101 The push towards Green Data Centres has been a combination of incentives provided for Data Centres that use energy-efficient mechanisms, certification for voluntary standards that give businesses a better selling point, and environmental requirements mandated by the Governments. There is a fine balance maintained in most countries across the three approaches to ensure that Data Centres become environmentally efficient without greatly increasing the burden of compliance and diminishing the ease of doing business.

2.102 The incentive-based program has been successful in several countries in reducing energy usage and developing renewable energy solutions for powering the Data Centre industry. In US, companies get a tax break of nearly $2 per square foot for buildings that save at least 50% of the heating and cooling energy of a system, or a building that meets standards specified by the Government[48]. Additionally, the US administration has extended 30% tax incentives for facilities researching in or using certain renewable energy sources. The UK provides a variety of rebates on the purchase of equipment for the

[48] https://www.energy.gov/eere/buildings/tax-incentives-energy-efficiency-upgrades-commercial-buildings

usage of renewable energy in Data Centres. The Malaysian Government[49] is also providing tax exemptions of up to 100% on capital expenditure for companies that undertake Green Data Centre projects.

2.103 There should be a Government initiative to promote green technology-enabled DCs. The DC players interested in setting up Green Data Centres can be given supplementary benefits like easy approvals and permits, ease of restrictions in availing existing renewable energy resources, buying renewable energy through open access, or investing in renewable energy power plants. Several criteria can be used to incentivize energy savings and green energy at Data Centres. These include cooling optimization by the creation of Data Centres in naturally cooled regions, using or investing in research on renewable energy resources for Data Centres, and Data Centres designed on green computing principles that use natural cooling and natural light in addition to having low energy requirements processes. The naturally cooled regions in India which remain vastly unexplored for Data Centre ventures are the best-suited alternatives for greenfield rollout owing to their low CapEx and OpEx and relatively lesser land cost, cheap labour, low water-based cooling requirements, and abundance of opportunities for investment in renewable energy power plants for powering Data Centres.

2.104 There are certifications for green Data Centres that can be obtained from several agencies that are used around the world. The LEED (Leadership in Energy and Environmental Design) certification is an important certificate for green buildings that are used in multiple countries and was developed by the US Green Building Council. In India, the Indian Green Building Council (IGBC), a part of the Confederation of Indian Industry (CII) gives certification to companies wishing to obtain a LEED certificate. In addition to this, the IGBC also has a Green Data Centre certification, which looks specifically at Data

[49] https://taxsummaries.pwc.com/malaysia/corporate/tax-credits-and-incentives

Centres and uses multiple criteria for adjudging efficiency. These certifications can be used as a criterion for providing tax breaks and are important for Data Centres to attract business as well.

2.105 **Renewable Energy Certificates (RECs):** Renewable energy certificates (RECs) are tradable commodities that are purchased in voluntary markets and then retired/redeemed once that electricity is consumed. For every unit of electricity generated from renewable sources, a unique REC is created. RECs tend to be purchased in units of a 1-megawatt hour (MWh). Thus, a Data Centre using 10,000 MWh (10 gigawatt-hours) of electricity in a year would need to purchase 10,000 RECs to match that usage. The Renewable Energy Certificate Registry of India is managing all policies between solar power companies and industries in India where consumption is very maximum, such as factories, manufacturing plants, etc. To promote green Data Centres the DC investors can be allowed to buy power from large generating/distributing companies (DISCOMs) having RECs directly without any restrictions.

2.106 **Reliable access to Water:** An enormous volume of water is required to cool high-density servers and data racks, which is making water management a growing priority for Data Centre operators. A 15-megawatt Data Centre can use up to 360,000 gallons of water a day, and as the scale increases Data Centre, operators have to depend heavily on water supply[50]. Due to the huge computing power in Data Centres containing hundreds of thousands of servers, in many designs, all the heat from those servers should be managed through cooling towers. The water serves to cool the air as it enters the Data Centre. In the process, however, some of the water evaporates and is lost. Thus, there is a need for a reliable, continuous source of water for these systems to be effective. This is the reason a Data Centre construction is feasible only when an adequate water supply is available nearby.

[50] https://www.datacentreknowledge.com/archives/2012/08/14/data-centre-water-use-moves-to-centre-stage

Q.17: Is the extant situation of power supply sufficient to meet the present and futuristic requirements for Data Centres in India? What are the major challenges faced by Data Centre Industry in establishment of Data Centres in naturally cooled regions of India? What are the impediments in and suggested non-conventional measures for ensuring continuous availability of power to companies interested in establishing Data Centres in the country? What incentivization policy measures can be offered to meet electricity requirements for Data Centres?

Q.18: Should certification for green Data Centres be introduced in India? What should be the requirement, and which body may look after the work of deciding norms and issuing certificates?

Q.19: Are there any challenges/restrictions imposed by the States/DISCOMs to buy renewable energy? Please elaborate. Please suggest measures to incentivize green Data Centres in India?

Q.20: What supportive mechanisms can be provided to Data Centre backup power generators?

Q.21: Availability of Water is essential for cooling of Data Centres, how the requirement can be met for continuous availability of water to the Data Centres? Are there any alternate solutions? Please elaborate.

Other miscellaneous challenges

I. Capacity building

2.107 The labour cost in India is much lower than in developed countries, thereby reducing the construction cost to a considerable extent. However, the consolidated challenges faced at present arise heavily from a lack of expertise, little or no retrofit industry knowledge, and standardization. The limited availability of expertise and efficiency opportunities in the country makes it imperative to involve expert

consultants in design, especially during the early project initiation adding to the investment requirements significantly. There are new kinds of demands being placed around resource controls, facilities management, and Data Centre optimization. To compete with the new demands of the market, the Data Centre industry is investing in new talent, which will also create new positions and evolve others.

2.108 The critically essential Data Centre skills that require pan-India emphasis and promotion in this sector, beyond a university degree are:

a. Cloud Skills

b. Cyber and Data Security Skills

c. Data Centre Infrastructure Management (DCIM)

d. Data Analytics

e. Network LAN/WAN and Cable Design Skills

2.109 The skillset demand in the Data Centre sector is high, and the competition is fierce. This calls for the planned implementation of suitable capacity building initiatives as part of vocational training along with the extant university education. Introduction of vocational-vendor neutral certification courses in the field of Computing System, Data Centre Infrastructure Management, Certified Network Associate/Network professional will give due impetus to the much-required capacity-building initiatives in the field of DCs in the country. As fostering the required technical skills for Data Centre operations is necessary, suitable investments are required in training and skill development so that India can move faster on embracing these new-age technologies. For this, subsidizing the education for specialized cloud/data operations and training and certifications of Data Centre professionals may be considered. New curriculum development and training of the faculty may also be a focus area. To develop the country's data hub in Guizhou[51], the Chinese Government encourages tertiary institutions to offer courses in big data. Likewise, the tech

[51] https://www.datacentredynamics.com/en/news/chinas-new-big-data-hub/

companies may be encouraged to skill the students, conduct workshops, and upskill the existing workforce in India. All of this will translate to increased career opportunities and growth within the Data Centre space of the country.

Q.22: Whether the existing capacity building framework for vocational or other forms of training sufficient to upskill the young and skilled workforce in India for sustenance of Data Centre operations? What dovetailing measures for academia and industry are suggested to improve the existing capacity building framework, and align it with the emerging technologies to upskill the workforce in India?

II. Centre-State coordination

2.110 The draft National Data Centre Policy 2020, released by MeitY is a welcome step. This policy framework shall be followed by a detailed scheme with an implementation guideline document detailing incentives to be provided to the DC sector by the Central and State Governments. However, the industry representatives in response to the aforesaid draft policy are of the view that policies should be jointly framed with states, as there is a lack of cooperation in certain states and many departments don't coordinate with each other. Most Data Centres favouring states already have economic development processes in place that offer tax incentives, investment assistance, loan guarantees, and other forms of business assistance designed to attract business development. But with the huge investments that Data Centres can represent, the playing field has changed. This calls for a greater thrust on Centre-State coordination favouring the implementation of uniform tax abatement code, analogous labour laws, and a common framework to facilitate ease of doing business.

Q.23: Is non-uniformity in state policies affecting the pan-India growth and promotion of Data Centre industry? Is there a need for

promulgation of a unified Data Centre policy in India, which acts as an overarching framework for setting Data Centres across India? What institutional mechanisms can be put in place to ensure smooth coordination between Centre and States for facilitating DC business? Do support your answers with detailed justification.

Q.24: What practical issues merit consideration under Centre-State coordination to implement measures for pan-India single-window clearance for Data Centres?

III. Edge Data and AI-enabled Data Centre

2.111 Edge Data Centres are smaller facilities located near the populations they serve that provide cloud computing resources and cached content to end users. They are typically linked to a larger central Data Centre or a network of Data Centres. Edge computing enables organizations to reduce latency and improve the customer experience by processing data and services as close to the end-user as possible. End users and devices expect anywhere, anytime access to the applications, services, and data stored in today's Data Centres, and latency is no longer acceptable. As a result, organizations in a variety of industries are establishing edge Data Centres as a high-performance and cost-effective way to provide content and functionality to customers. Edge Data Centres are deployed in support of several uses, including 5G networks, Internet of Things rollouts, and content delivery networks.

2.112 Artificial intelligence (AI) is a proven way for Data Centre operators to maximize uptime, optimize energy consumption, detect potential risks quickly, and defend against cyber-attacks. AI can be applied to mechanical and electrical equipment in Data Centres to enable actionable insights and automation, saving the operator money. AI's biggest benefit for Data Centres is the considerable reduction in energy consumption. Google, with its AI-interest acquisition of DeepMind in 2014, has incorporated a machine-learning algorithm to manage Data Centre equipment that resulted in 15% reduced energy overhead and

40% reduced cooling energy. The Google stats of reduced energy consumption discussed above also imply saving worth millions of dollars. This means that be it on a small or large scale, AI-based Data Centre systems and solutions are imperative to become energy efficient.

2.113 Data Centres require a high level of electrical reliability, and uninterrupted power availability continues to be a significant concern for Data Centre managers. Power quality issues can cause equipment failure, downtime, data corruption, and are obstacles for DC operations. It is frequently the case that Data Centre managers tend to overprovision power to avoid downtime. This leads to unnecessary wastage of power and space. As India plans the expansion of Data Centres, such wastages need to be eliminated. To optimize the cost of operation, it is significant to create an efficient Data Centre Infrastructure Management System (DCIM) to correctly assess the requirements of the concerned Data Centres. DCIM not only streamlines the costs but also ensures sustainability by reducing its carbon footprint. However, creating and maintaining a robust DCIM might pose cost concerns, especially in a country like India, which still does not possess the necessary framework for technical and designing expertise as compared to the developed countries of the world.

2.114 Given that new technological developments will keep happening in the DC space, policy measures must be put in place to promote the adoption of future technologies for Data Centres.

Q.25: Is there a need for Data Centre Infrastructure Management System (DCIM) for Data Centres in India? What policy measures can be put in place to incentivize Data Centre players to adopt the futuristic technologies? Elaborate with justification.

IV. Data digitization and monetization

2.115 Digitization is quite simply the creation of a computerized representation of a printed analog. Data Digitization is the process by

which physical or manual records such as text, images, video, and audio are converted into digital forms. There are many methods of digitizing, but the main focus rests primarily on texts and images, as these are the main objects in the digitization process. In this context, some of the fundamental things like scanning and image capture, necessary hardware, and software selection are crucial for the process of digitization.

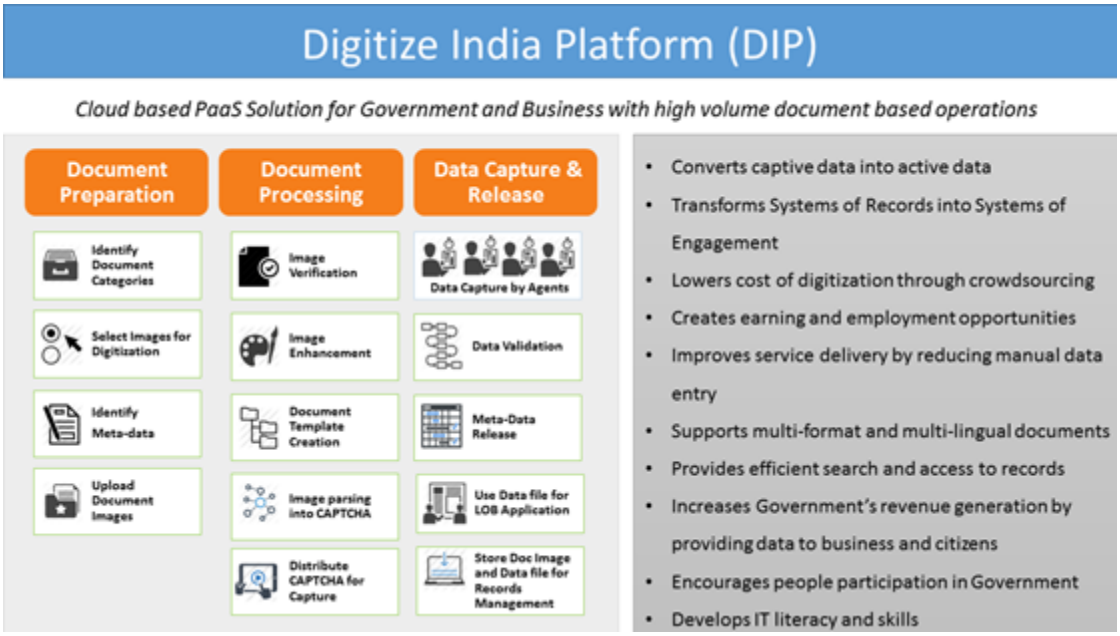
2.116 Digitization of records has been a priority for Government of India as digitized data offers the long-term preservation of documents, orderly archiving of documents, easy and customized access to information, and easy information dissemination through images, text, CD-ROMs, internet, intranets, and extranets. Digitized data offers the possibility of monetization by introducing the discovery, capture, storage, analysis, dissemination, and use of that data. Converting physical records into the digital form will not only facilitate easy access of Government records and services but will also enable easy access and data analysis for informed decision making. Data digitization would further help data principals in data sharing to gain beneficial terms or conditions from businesses, information bartering, selling data outright (via consent managers or independently), etc.

2.117 Digitize India Platform (DIP)[52] is an initiative of the Government of India under the Digital India Programme to provide digitization services for scanned document images or physical documents for any organization. The aim is to digitize and make usable all the existing content in different formats and media, languages, digitize, and create data extracts for document management, IT applications, and records management. DIP provides an innovative solution by combining machine intelligence and a cost-effective crowdsourcing model. It features a secure and automated platform for processing and extracting relevant data from document images in a format that is usable for meta-data tagging, IT application processing, and analysis.

[52] https://digitizeindia.gov.in/about-dip

If one organization already has the scanned documents/images, DIP can help them to extract the relevant data from the same and provide the data extracts in a usable format. DIP provides an innovative solution for all these challenges by combining Machine inputs with human intelligence to deliver logically verified data. If one organization is still using the paper-based document, DIP can convert them into images and digitize them. The process of data digitization under DIP is depicted in Figure 2.7

Figure 2.7: DIP



2.118 The DIP platform provides a facility to digitize various kinds of physical records through crowdsourcing (www.digitizeindia.gov.in). The platform uses an innovative algorithm, which ensures the accuracy of the digitized document at a significantly reduced cost. It also improves the quality of record-keeping and reduces the real estate required for maintaining large record rooms for legacy records. The DIP initiatives, taken in 2015, is helping the State Governments, which are the custodian of huge volumes of legacy data in forming land records, land registry, birth and death records, exam results at school and university levels, service records of government employees, etc. However, there are still many physical records that need to be digitized. For ensuring

that the digitization of all records is completed in a time-bound manner some institutional mechanism needs to be put in place.

Q.26: What institutional mechanism needs to be put in place to ensure digitization of hard document within a defined timeframe?

Q.27: Would there be any security/privacy issues associated with data monetization? What further measures can be taken to boost data monetization in the country?

CHAPTER 3

CONTENT DELIVERY NETWORKS

3.1 A Content Delivery/Distribution Network (CDN) is a geographically distributed network of proxy servers and their Data Centres at various points of presence (PoP), working together to deliver pages and other web content to a user based on the geographic location of the user. The distributed servers are called cache or edge servers, which store a cached version of the content in Data Centres operated by IXPs and Internet Service Providers (ISPs). Content delivery networks accelerate the delivery of diverse content, especially video delivery, to the user.

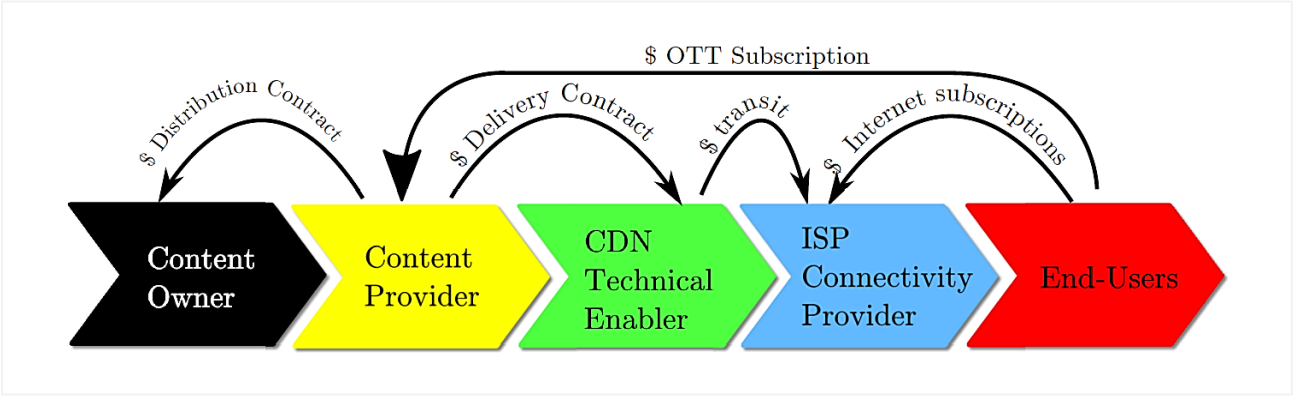
3.2 The major factors driving the growth of the CDN market include the rising need for effective solutions to enable live and uninterrupted content delivery over a high-speed data network, increasing demand for enhanced QoE (Quality of Experience) and QoS (Quality of Service), the proliferation of video and rich media content over websites, increasing demand for enhanced video content, latency-free online gaming experience, increasing internet penetration and adoption of mobile devices leading to rising opportunities for mobile CDN.

3.3 CDNs have been used to improve the video streaming experience to end-users while at the same time limiting the need for Content Providers (CP) to own infrastructure. By massively deploying servers in strategic locations, CDN providers assign users to a close-by server, thus reducing hop count and avoiding potential congestion occurrences while ensuring scalability and reliability. Shortening the physical distance between a user and the webserver is the main job of CDN, resulting in faster load times, increased server uptime, reduced bandwidth usage, improved security, and better website performance.

3.4 Figure 3.1 displays the value chain for video content distribution. On the one hand, the Content Owner sells its content to online Content Providers (CP). On the other hand, ISPs sell plain connectivity to end-

users, and CPs sell them access to OTT content. Finally, CDNs are placed between CPs and ISPs as a technology enabler.

Figure 3.1: Value Chain for delivery of content[53]



3.5 CDN topology distinguishes between the two types of servers: origin server at the source location ensuring the efficient intra-CDN distribution of content, and cache servers for handling end-user to server communications.

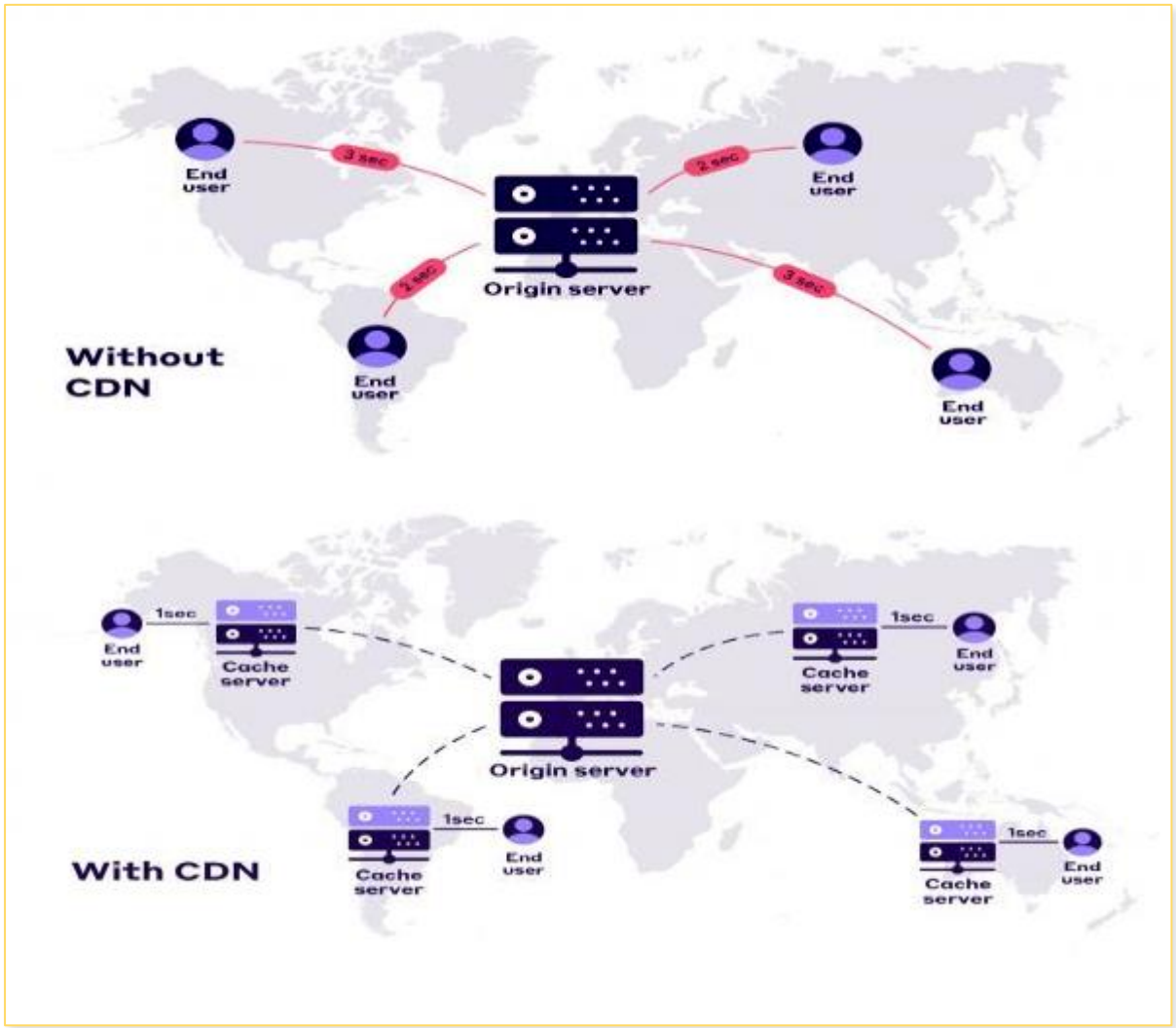
3.5.1 ***Origin server:*** An origin server is a web server that handles all the internet traffic, processes incoming requests from end-users, and responds to them. An origin server takes on all the responsibility of serving up the content for an internet property such as a website or video. The physical distance between the origin server and the user adds latency to the connection during the data transmission.

3.5.2 ***Edge/Cache server:*** A CDN edge or cache server is a computer that exists at the logical extreme or edge of a network, i.e., closer to the user. The primary purpose is to store content as close as possible to a requesting user device, thereby reducing latency and improving page load times. CDN edge servers store cache content in the strategic locations or PoPs to off-load one or more origin servers; they also keep a track of changes at the origin server. Content delivery across the globe with and without CDN is presented in Figure 3.2 for a better overview. It can be seen that content transfer directly from the origin

53 Nicolas Herbaut, Daniel Negru, Yiping Chen, Pantelis Frangoudis, Adlen Ksentini, "Content delivery networks as a virtual network function: A win-win ISP-CDN collaboration." 2016 IEEE Global Communications Conference

server to the end user adds more latency due to large distances, whereas latency is reduced using cache servers at various PoPs near the end user. CDN providers employ complex software to match incoming requests for content to the 'best' server for meeting each end-user request.

Figure 3.2: Using cache servers to speed up content delivery



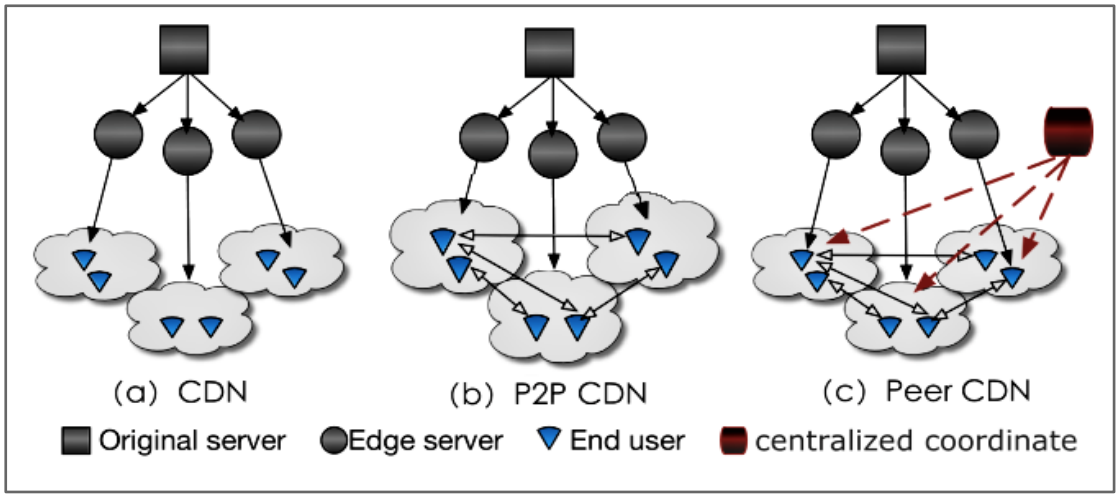
Types of CDN providers

3.6 CDNs could be private or public networks. There are essentially two basic setups in distributing the content by CDN: A Peer/Private model and a Peer-to-Peer (P2P) model.

a. ***Peer-to-Peer (P2P) provider:*** A P2P CDN provider leverage users for the distribution of content. When an end user visits a website that has been cached by this CDN, their browser's HTTP requests will be

redirected to the edge server closest to them and the site will load faster to the user. A P2P CDN works by creating a mesh network *(refer to Figure 3.3 (b)* consisting of users who are watching the same content and coordinating these users so that they share video data segments with each other instead of everyone always fetching the segments from an edge server. Due to fewer hardware and resource requirements, many CDN providers tend to offer P2P services free of cost.

Figure 3.3: System architecture for CDN, P2P CDN and Peer CDN



b. ***Private/Peer provider:*** The peering/private CDN model is the more traditional and preferred approach by CDN companies maintaining a network of servers across a wide geographic area. These server nodes in a router-based peer CDN are closely coordinated by the centralized knowledge, as shown in *Figure 3.3 (c).* Each server will have copies of the data saved, and whenever a user requests for data, it will download the data from the edge servers that are physically closest to them, reducing the loading time and preventing request timeouts. Compared to the conventional CDN approach, a peer CDN provider employs network resources much closer to users, and this model can serve as much as 80% of the content requests by peer nodes.

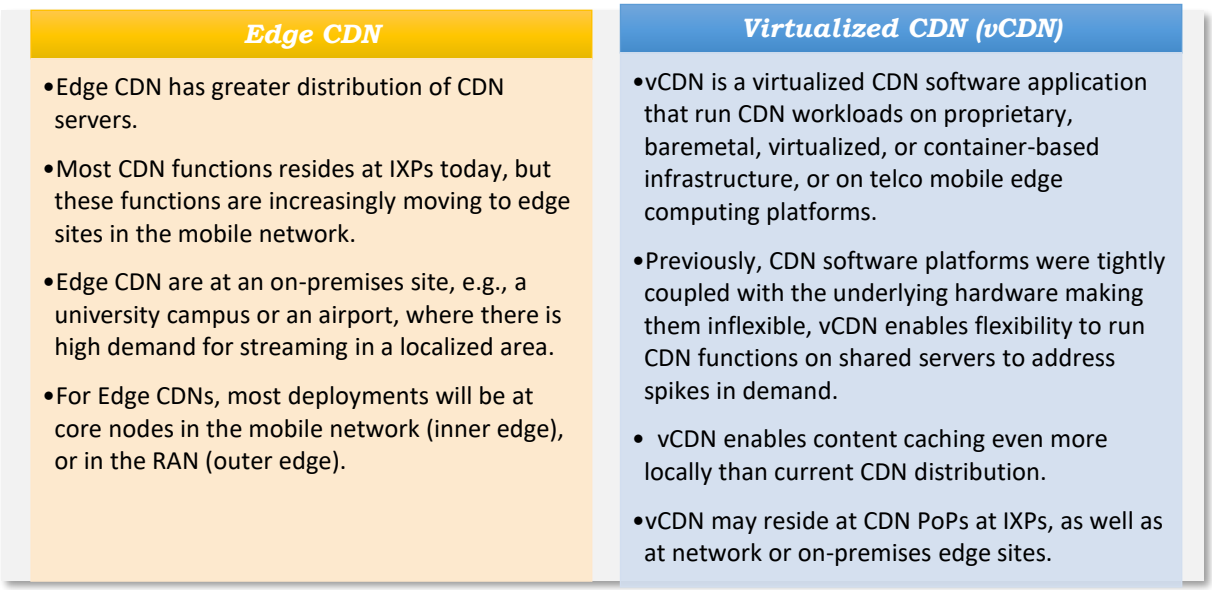
Edge CDN and Virtual CDN (vCDN)

3.7 Currently, most CDN servers are located at PoPs in the IXP/ISPs or distributed Data Centres, enabling content to be cached and replicated close to end-users. However, in the face of growing demand, the current distribution of these servers becomes too centralized and

impairs CDN and gaming providers in ensuring a high quality of experience (QoE) to the end-users. For an optimal experience in advanced applications, servers would need to be within a few hundred miles of each end-user. There are two key trends emerging: edge CDN and virtual CDN (vCDN).

3.8 By deploying servers at the edge of the network, CDN providers can assign users to a close-by server, reducing hop count and avoiding potential congestion occurrences, while ensuring scalability and reliability. The use of Edge CDNs and vCDNs will further help in reducing issues of peering points congestion, inefficient routing protocols, network unreliability, and the inefficiencies of existing communication protocols and thereby aiding faster delivery of content to users.

Figure 3.4: Edge CDN & vCDN



Both edge CDN and vCDN are set to change the landscape of content delivery, providing new opportunities for Telcos to play a more significant role in the CDN ecosystem and take advantage of new monetization opportunities.

Why the demand for CDNs is growing?

3.9 The growing demand for low-latency, seamless, and easily integrated content delivery across the internet has created opportunities for an increasing number of CDN providers. The shift to mobile content and multi-platform viewing has created a tremendous market opportunity for new CDN companies and considerable product and business innovation among the companies. The increased dependencies on ICT infrastructure post-pandemic for requirements of work, education, and entertainment are further pushing the demand. The following sections explain various benefits of CDNs that are contributing to their increased demand.

3.10 CDNs provide ***numerous benefits for users and also for the network infrastructure***. Some of the benefits of using a CDN are:

A. Improved page load speed and website performance
B. Ability to handle high traffic loads and sudden peaks
C. Localized coverage and improved availability
D. Reduced bandwidth consumption
E. Load balance between multiple servers or locations, causing decreased load times and latency
F. Secure encryption and counters denial-of-service (DDoS) attacks

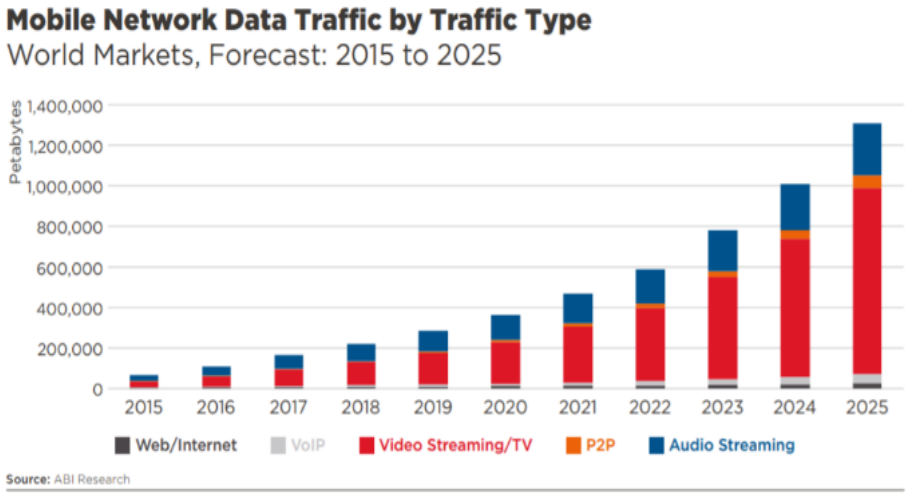
3.11 **Faster Web hosting:** CDNs' primary customers are website or platform owners, allowing for quick transfer of information that is required for loading various internet content. Enterprise companies require a CDN to give fast web performance to their end customers. In the recent past CDNs have gained significant popularity delivering traffic for the majority of sites such as Amazon, Facebook, Netflix, etc. CDN envisages widespread application in non-video domains as well (websites, local hosting, file downloading, e-services, e-commerce solutions, etc.) for faster page loading, reducing bandwidth consumption, securing websites from attacks, and blocking spams. This leads to positive user experiences expressed as:

High* content *loading speed* = *Positive User Experience

As more and more companies are making a noticeable shift from traditional web hosting, CDNs are handling a majority of the load. By storing the static content on edge servers, CDNs can handle traffic spikes with scalability. This is another reason behind prominent or popular web hosting companies increasingly using CDNs.

3.12 **Increased Video consumption:** With the rise of smartphones availability and usage, video consumption is growing at a much faster rate. Presently, video accounts for about two-thirds of downstream peak period traffic with ever-increasing trends. Figure 3.5 depicts mobile traffic growth in terms of video and non-video consumption in Petabytes (PB) per year according to GSMA & ABI research report[54]. The non-video traffic includes file sharing, web/data, VoIP, and gaming applications. As mobile video content has much higher bit rates than other mobile content types, video is expected to generate the majority of the mobile traffic growth through 2022.

Figure 3.5: The GSMA & ABI research mobile data traffic forecast



3.13 The COVID-19 pandemic has further led to increased media consumption due to billions of people seeking in-home entertainment.

[54] https://www.mobiliseglobal.com/wi-fi-offload-in-numbers/

As per the ABI data research forecasts, mobile data traffic is anticipated to grow at a CAGR of 28.9% to surpass 1307 exabytes on annual basis in 2025 wherein, 4G and 5G mobile subscribers will represent 91% of total data traffic generated in 2025.Given that video is currently the most requested content format on the internet, its delivery requires new technologies and faces new challenges. CDN has been critical in delivering video, large files, and other web content to users quickly and reliably. Distributing video using CDN requires a different approach than distributing other types of content because of latency sensitivity and high bandwidth utilization of video data. Owing to the rise of high-bandwidth content and data-hungry smartphones in less than 10 years, CDN demand has skyrocketed. The increase in demand for uninterrupted video and website content is expected to continue to reflect the growth of the CDN market.

3.14 **Impact of the COVID-19 pandemic:** The pandemic has accelerated India's digital reset, which has seeped into almost every aspect of life. The use of media and online content services has heavily increased during the lockdown. The COVID-19 outbreak has led to adopting new technologies and ways for business houses, education institutions, analytics, computing, and data management methods. Online courses involving live streaming of classes require unhindered and continuous access. The ed-tech platforms are partnering with CDNs to allow students unhindered access to quality education and have empowered them to continue their academic journey despite being at home.

3.15 **Popularity of Over-the-top (OTT) Services —**The popularity of OTT services provided by media giants like YouTube, Netflix, and Amazon Prime, on-demand video/music streaming, and live streaming of sports, news, and events, resulted in huge video consumption and expanded the scope of the video landscape. The Indian OTT market is likely to outperform the global market and may be ranked among the top 10 by 2022. There are currently about 40 OTT providers in India, which distribute streaming media over the internet. According to

KPMG Media and Entertainment Report 2019[55], there will be 580 million OTT consumers by FY24 spending 30+ minutes on online platforms every day, making India the second–biggest market after the US. CDN providers are set in motion to deliver faster speeds and better quality. At present most of the OTT companies have their own infrastructure and leverage upon CDN services to maximize speeds. During COVID-19 lockdown, all OTT platforms and new websites have seen 2x-3x times growth on average, and CDNs have ensured an uninterrupted user experience.

3.16 **Uptake of E-commerce business and Financial services:** E-commerce, banking, and financial companies make use of CDNs to improve their site performance and make their products or services available online. According to Computer World, CDN provides 100% uptime of e-commerce sites, and this leads to improved global website performance. With continuous uptime, companies can retain existing customers, leverage new customers with their enhanced services, and explore new markets, to maximize their business outcomes. E-commerce companies setting up their stores in the cloud are looking forward to partnering with the Indian edge providers (PoPs). Businesses in the field of banking, financial services, and insurance (BFSI) can use a CDN not only to improve application performance but also to secure their infrastructure.

3.17 **Reducing Bandwidth costs:** One of the most obvious cost benefits to companies using CDNs is the lower bandwidth costs. CDNs that offer access to key PoPs optimize the bandwidth efficiency across multiple servers and improve the delivery of rich media content, providing noticeable performance benefits to end users. This offloads the bandwidth strain on the origin server, and the bandwidth costs go down as efficiency improves. Therefore, installing CDN servers will

55 KPMG India's Digital Future: (India's Media and Entertainment Report), August 2019
https://assets.kpmg/content/dam/kpmg/in/pdf/2019/08/india-media-entertainment-report-2019.pdf

reduce the international bandwidth requirement by ISPs, improve their network performance and efficient bandwidth usage.

3.18 **Other cost benefits:** Content provider companies currently using CDNs gain additional operational benefits on being able to focus better on developing meaningful content to offer to customers. Whether the company is in the gaming or IPTV industries or provides rich media content on the web, it certainly benefits from using a CDN in its network strategy. A provider can concentrate on the content and let the CDN focus on getting it to the customers quickly and efficiently. A CDN provides seamless scalability, allowing companies to gain the cost benefits of economies of scale as they grow.

Establishing CDN servers in the networks decreases the server load on interconnects, peering points (public and private peers), and backbones, freeing up the overall capacity and decreasing delivery costs. Essentially, the content is spread out across several servers, as opposed to offloading them onto one large server, reducing the network traffic loads and leading to efficient traffic management, especially during surges.

Why India needs to focus on CDNs?

3.19 As discussed in the preceding section, there are several driving factors, which are fueling the CDN demand in India. With the second-largest user base and continuously growing internet users, the service providers are compelled to build and install content servers in their networks. The internet user's growth and penetration rate in India is shown in Figures 3.6 and 3.7. Various mobile operators and ISPs have launched CDN initiatives during the last few years.

3.20 The change in consumer behavior has led to more business-to-business data transactions in the field of finance, advertising, healthcare, and agriculture in the country, compelling the need for CDNs to boost Indian businesses and digital efficiencies. Many industry verticals, including the advertising industry, media and

entertainment, gaming, education and healthcare, online music retailers and consumer electronics, etc., are adopting content networks.

3.21 In recent times, India's broadband infrastructure has significantly improved, leading to enhanced broadband connectivity and adoption. Moreover, the growing proliferation of high-speed internet and affordability of related services is expected to accelerate the consumption of internet content. Additionally, the implementation of NDCP-2018 policy unleashes multiple opportunities for TSPs, ISPs, infrastructure providers, manufacturers, innovators, and startups. The viability and success of the proposed Digital Communications Infrastructure will also depend on its users getting enabled to access uninterrupted content and applications at the time, place, and medium of their choice. Better availability of broadband increased speeds, and lower prices are factors that are fueling the growth of CDN platforms from the demand side.

3.22 India is witnessing an increased demand for online streaming of video content. Today, consumers are making a shift from conventional and cable-based video subscriptions to OTT Internet-based delivery platforms. Numerous players have emerged in the OTT market space, directly resulting in increased Internet traffic. Buffering is seen as a major reason for user dissatisfaction and low experience levels, causing more OTT and VOD-based CDN services.

Figure 3.6: Internet users' growth in India

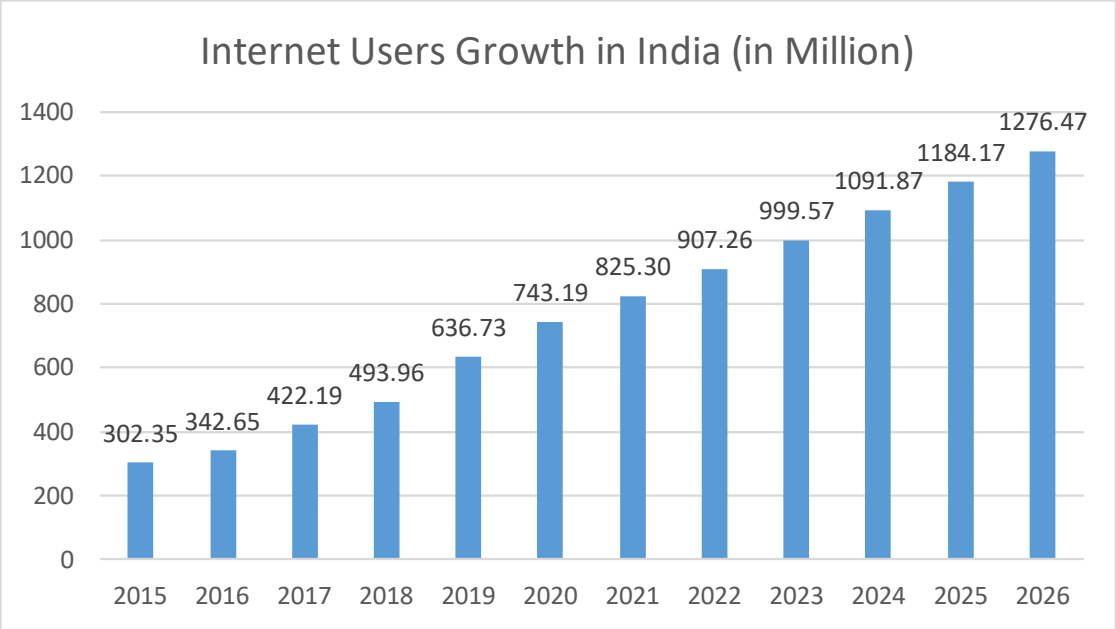
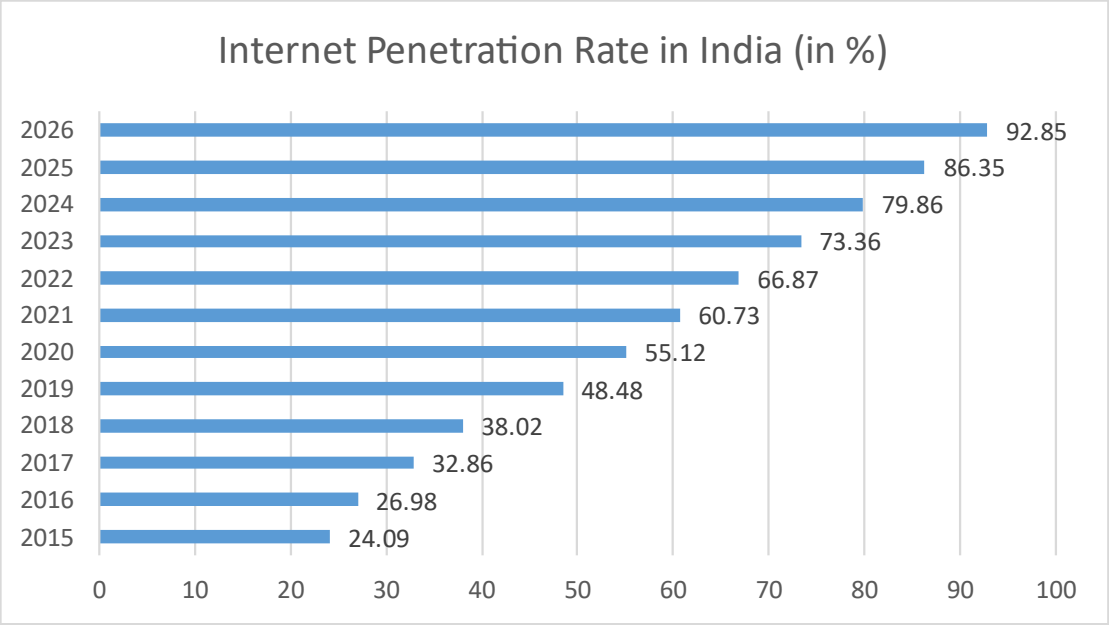


Figure 3.7: Internet Penetration Rate in India



Rollout of 5G and new futuristic technologies

3.23 5G, the next generation of mobile connectivity, promises significant speed increases, ultra-low latencies, and immense capacity to handle Internet of Things (IoT) devices. 5G encompasses multiple

technologies, increases network performance improving flexibility and scalability. It also brings new capabilities, such as network slicing, which allows the creation of multiple virtual networks on the same infrastructure, each securely isolated and with different performance characteristics.

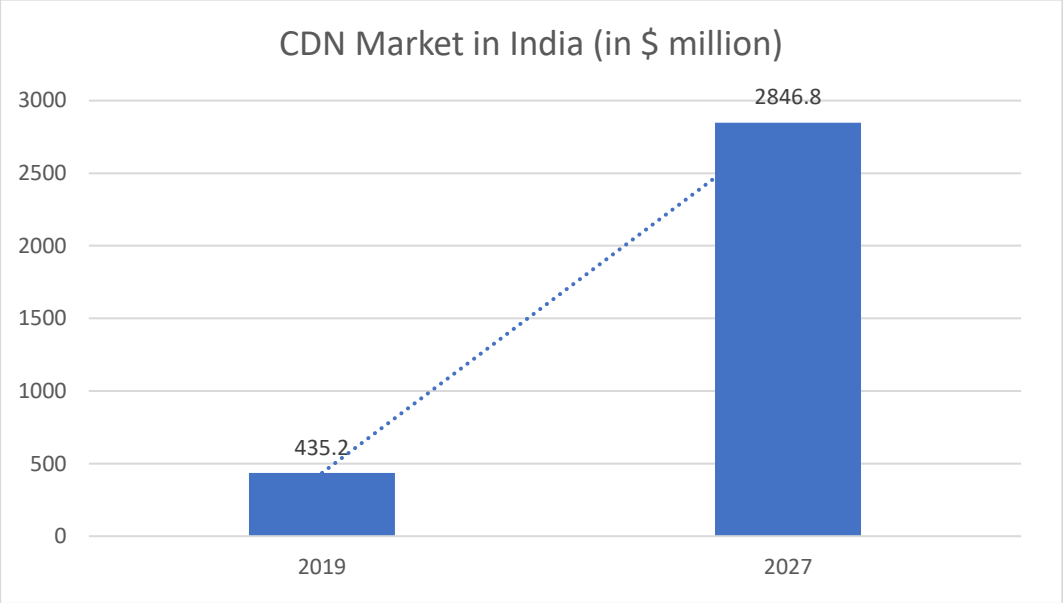
3.24 The main drivers of CDN in the 5G era will be the digitization of everyday processes. The use cases in 5G, including autonomous vehicles, Industry 4.0, video surveillance, cloud-based gaming, and telemedicine, etc., will require very low latency delivery of content at the edge. As 5G network rolls out, migration of storage from end-user devices to 5G edge locations and the public cloud, where storage and processing are cheaper is expected. One of the most significant drivers will be the increased use of video data (more cameras everywhere) and the improved resolution of image sensors. The increased use of video data, the improved resolution of image sensors, underlying virtualization of the infrastructure, and the move towards cloud-native architectures will bring more and more focus on CDNs.

3.25 Further widespread use of AI/ML will necessitate CDNs at the edge for large volume data processing for sensors, logs, image data in AI training, and quick delivery of automated decisions. CDNs will also impact the way compute and software architecture caters to the need of new 5G use cases.

3.26 The Indian CDN market was valued at $435.2 million in the year 2018 and is expected to be valued at $2846.8 million by 2027 (refer figure 3.8 below). Looking at Indian CDN market statistics and forecast, it is seen that Asia-Pacific dominated the global market in 2020 and accounted for a revenue share of over 39%. The regional market will expand further at the fastest CAGR from 2021 to 2028, as it is characterized by the presence of emerging economies, such as India and China, and is also one of the fastest-growing consumer markets. Moreover, the growing population has resulted in an increased demand for technological advancements in networking

infrastructure to fulfill the needs of online media consumption. Various initiatives by the regional governments, such as Digital India, have enabled fast and secure management of data delivery, owing to which the usage of CDN solutions is expected to increase.

Figure 3.8: CDN Market in India



International experience related to CDNs

3.27 The Global CDN market size is expected to grow from USD 14.4 billion in 2020 to USD 27.9 billion in 2025, at a Compound Annual Growth Rate (CAGR) of 14.1% during the forecast period[56]. As the CDN services are picking up, global practices and regulatory frameworks, etc., are also evolving, the same has been discussed in the following sections. Table 3.1 below mentions of global practices in CDN regulation of few countries.

Table 3.1: Global practices: regulatory framework for CDN service providers

S. No.	Country	Authority/Regulator/Regulatory Framework Status	If yes, licensing or registration regime
1	China	The National Communications Commission/Regulated	Internet Content Provider Registration is required for CDN Services[57]

[56] https://www.marketsandmarkets.com/Market-Reports/content-delivery-networks-cdn-market-657.html
[57] https://nhglobalpartners.com/what-is-icp-license-how-to-get-one/

2	Germany	BNA (Bundesnetzagentur)/ Lightly Regulated	CDN services are considered as critical Infrastructure services, and therefore comes under the purview of German BSI Act[58] whereby the CDN Service Provider has to perform third-party audit.
3	Norway	Norwegian Post and Telecom Authority/Not Regulated	Registration with the Norwegian Post and Telecom Authority is not required for content service providers and CDNs[59]
4	Brazil	ANATEL (The National Telecommunications Agency)/Regulated	License of Multimedia Communications Services is required from the Local Regulator[60]
5	Australia	Australian Communications and Media Authority/Lightly Regulated	CDN service providers are subjected to certain regulatory obligations under the Telecommunications Act but do not require to be licensed[61]
6	South Korea	Korea Communications Commission/Not Regulated	CDN has not been recognized as a licensable service, rather it is the underlying transmission services (Internet/Video Connect) which is regulated, i.e., CDN itself is not subject to any telecom licence requirement.[62]
7	Kenya	The Communications Authority of Kenya/ Regulated	Content Service Provider license is structured in the Unified Licensing Framework (ULF) developed by the Authority[63]

European Union (EU)

[58] https://www.akamai.com/legal/compliance

[59] https://www.nkom.no/english/duty-to-register

[60] https://www.dlapiperintelligence.com/za.co.heliosdesign.dla.lotw.telecoms/handbook.pdf?country-1=BR.

[61] [1] https://thelawreviews.co.uk/title/the-technology-media-and-telecommunications-review/australia

[62] http://opennetkorea.org/en/wp/kcc-guidelines-on-net-neutrality-and-internet-traffic-management?ckattempt=1

[63] https://www.ca.go.ke/industry/telecommunication/licensing-procedure/

3.28 European CDN market stood at $ 3.6 billion in 2019 and is projected to grow at a CAGR of over 29% to reach $ 16.79 billion by 2025[64]. This rapid expansion is owing to the increasing number of smart devices, growing internet penetration, rising adoption of CDN by various enterprises and SMEs, and increasing demand for SMAC (Social, Mobile, Analytics and Cloud) technologies along with growing traction of AR and VR applications across gaming, media and entertainment, and other sectors. Based on the solution, the European Union market can be categorized into Media Delivery, Web Performance Optimization, and Cloud Security. Among these, the media delivery segment dominates the market. This is attributed to the growing digital media-supported devices, increasing internet penetration, and surging adoption of OTT applications, which has fueled the adoption of content delivery networks for seamless media delivery over the internet.

3.29 *Regulation of Content and Application providers:* The EU regulator BEREC (Body of European Regulators for Electronic Communications) has defined Content Application Providers (CAPs) first in its net-neutrality guidelines. BEREC's Open Internet Regulation[65] establishes rights in relation to the open internet for 'end-users' and the rights are available to both individual consumers and businesses using internet access services. CAPs are covered and protected by the Regulation as they use an internet access service to provide content or applications to other end-users. This Open Internet Regulation covers the provision of internet access services, and some defined specialized services, however, the interconnection services provided by the CDN companies and large content providers (e.g., YouTube, Netflix), who operate their own CDNs are excluded from the scope of the Regulation.

China

3.30 Asia-Pacific countries, especially China, Singapore, South Korea, Japan, etc., have contributed hugely to the expansion of CDN, and the

[64] https://www.globenewswire.com/Europe-16-79-Billion-CDN-Market-Competition-Forecast-2025.html
[65] https://berec.europa.eu/eng/open_internet/scope/

market is expected to reach $2.5 billion by 2026 at a CAGR of 19.8% during the forecast period 2021-2026[66]. The market is expected to grow at an even higher rate than present due to the ever-increasing consumption of content in emerging economies such as India, China, Japan, Hong Kong, and Singapore. All major CDN vendors have their Data Centres installed in APAC to cater to this demand.

3.31 *Internet Content Provider (ICP) licence:* China being ranked the first in the internet consumption globally, has several mandated licenses for the internet and telecom sector. Foreign website owners must obtain an Internet Content Provider (ICP) licence[67] from the Chinese Ministry of Industry and Information Technology (MIIT). An ICP license is issued to China-based websites and allows licensees to legally operate, host websites on servers in mainland China. Without an ICP license, sites hosted on a Chinese server will not load on browsers located anywhere in the country. Having an ICP license also allows to access a Chinese content delivery network.

CDNs – Issues to be addressed

3.32 This section deliberates on the issues and challenges faced by the existing CDN players in the country, the collaboration between CDN-ISPs, previous policy, and regulatory initiatives relevant to CDN providers, and the need for regulatory intervention in the CDN market.

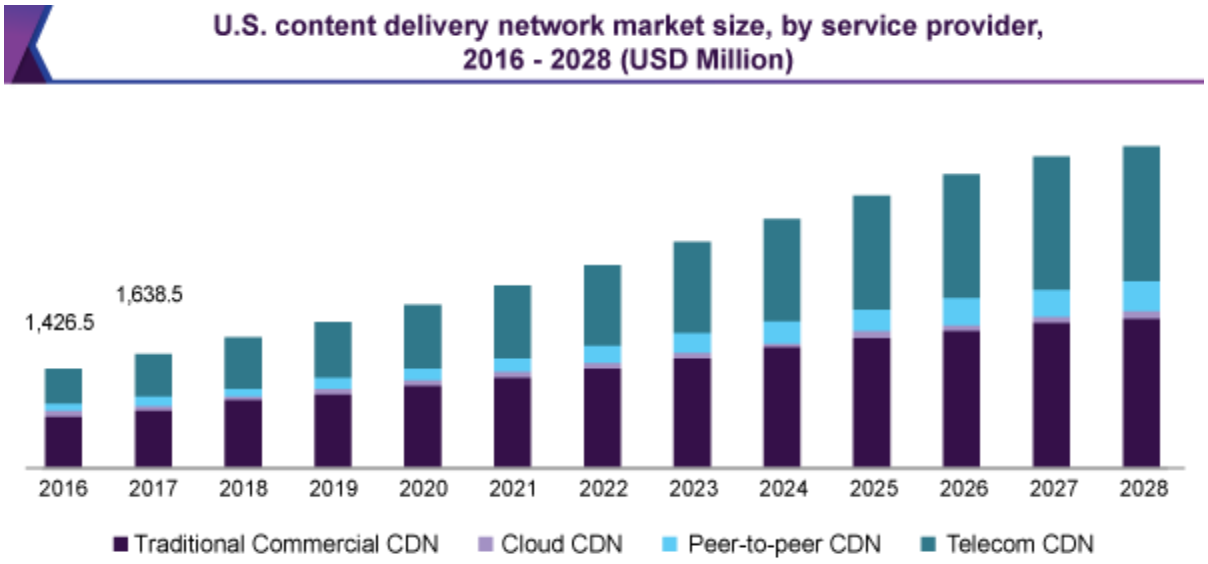
i. CDN – ISP interconnect and collaboration

3.33 CDNs form a layer in the internet ecosystem, where the content owners such as media companies and e-commerce vendors pay CDN operators to deliver their content to their end-users. In turn, a CDN pays ISPs, carriers, and network operators for hosting its servers in their Data Centres. The large deployment of the CDN-based solution has induced blurred borders on the content delivery market and TSPs/ISPs sometimes build their own distribution network.

[66] https://www.industryarc.com/Report/18783/apac-content-delivery-network-market
67 https://nhglobalpartners.com/what-is-icp-license-how-to-get-one/

Deployment of a distributed Network Function Virtualization (NFV) platform at the edge of the Internet Service Provider's network where a virtual Content Delivery Network (vCDN) can cater to the needs of end-user, is a model that is prominently emerging. The emerging technical architecture of edge CDNs and vCDNs suggests a global trend where Telco CDNs are likely to grow faster in the coming years than traditional CDN, as shown in Figure 3.9.

Figure 3.9: Expected growth of different types of CDN players in the USA[68]



3.34 CDN-ISP collaboration is a win-win situation where the CDN players make use of servers, storage capacities, space, power, and network site locations to host their cache servers, whereas ISPs, in turn, are benefitted from reduced bandwidth costs, security from DDoS attacks, and enhanced QoS to their customers. Many new models are proposed by IEEE and other prominent research academia for CDN players to collaborate with ISPs over a Virtualized Infrastructure, fairly balancing the revenue stream created. It is expected that vCDN is set to change the landscape of content delivery, providing new opportunities for ISPs to play a more significant role in the CDN ecosystem. For these models

[68] https://www.grandviewresearch.com/industry-analysis/content-delivery-networks-cnd-market

to flourish and contribute to the Indian digital economy, some issues need to be addressed.

3.35 **Revenue share between CDN-ISPs:** The relationship between CDN players and ISPs is that of a mutual facilitator. While CDN providers help ISPs in terms of helping them save bandwidth cost and in enhancing the user experience, ISPs provide the access without which CDNs cannot deliver the content. While the CDN providers are investing in the server hardware, the ISP is also arranging space, power, and bandwidth for fetching cache content, etc. Thus, both the players invest in their own systems and in process they help each other improve their commercial viability. The market for the interconnection of CDNs and ISPs is at a nascent stage. There is a need to see that the market is not misused to create dominance, hurting the business of smaller players by way of arbitrary demands. Such a market may require regulatory interventions.

3.36 **Lack of equal access to CDN:** Some of the big OTT players have started their own content delivery platforms. Such dominant players can dictate terms for interconnection with smaller ISPs refusing them direct peering. For any Digital Communication network to function smoothly, it is imperative to have a regulatory framework for interconnection between various players which is fair and just and gives equal opportunities to each player. Further, Large ISP players, who are also in the CDN space, can create exclusive tie-ups with large content providers like OTT platform companies excluding other players from direct access on equal terms.

3.37 **Net-neutrality issue:** If the access to CDNs is not on equal terms, the issue of net-neutrality may arise whereby customers of preferred players may be provided with better quality CDN services. While the ISPs are subjected to net-neutrality-specific license terms and conditions, a formal mechanism to enforce the same on CDN players does not exist. It can be argued that for compliance with net-neutrality principle, a proper regulatory framework for Content delivery networks

may be required. In its recommendations of 28th November 2017, though the Authority has recommended that the CDNs should not be included within the scope of any restrictions on non-discriminatory treatment, which are designed specifically to cover the providers of Internet Access Services, at the same time Authority has also said that there is a need for more transparency relating to the arrangements between TSPs and CDNs. Knowledge of such arrangements would be useful for gaining a proper understanding of the factors affecting the flow of traffic on the Internet, the potential for anti-competitive practices, and monitoring violations of the non-discrimination requirements by TSPs. The Authority may frame appropriate regulations to specify the disclosure and transparency requirements in this regard.

3.38 In a study paper published by the Competition Commission of India on 'Market study on the Telecom Sector in India - Key Findings and Observations' dated 22nd January 2021, it has been deliberated that Internet companies often utilize Content Delivery Networks (CDNs), to facilitate faster delivery of their content to users. In turn, CDNs have agreements with ISPs or TSPs to host servers on their network. CDNs reduce congestion in the last mile, lower transit costs, and improve overall network utilization. With data traffic set to grow and a limited number of players controlling a significant proportion of internet traffic, chances are there for anti-competitive agreements between CDNs, ISPs/TSPs, and internet companies. Since commercial arrangements between internet companies, CDNs, and ISPs/TSPs are not disclosed, monitoring of such arrangements and traffic patterns would help in ensuring net-neutrality principles and fair competition. However, for monitoring any such interconnect agreement, some regulatory framework will be required.

3.39 **DNS filtering, Content blocking and Security:** The Domain Name System (DNS) is a naming database in which internet domain names/URLs are located and translated into IP addresses so that browsers can load the internet resources/websites/ requested URLs.

DNS directs the websites' traffic to the CDN servers instead of directly to the origin servers hosting the website. When user computer wants to find the IP address associated with a domain name, it first makes its request to a *recursive DNS server* or *recursive resolver* that is usually operated by an ISP or other third-party provider, and it asks the exact DNS servers to resolve the name of a site with its IP address. The servers that actually have the needed information are called *authoritative DNS servers*. The Unified License Agreement for ISP services does not specify whether the recursive/authoritative DNS servers are to be setup/maintained by Licenses or not. Currently, some of the ISPs have setup their own DNS and many of the ISP Licensees are using other DNS server including public DNS servers like Google, Cloudflare etc., in their network for their users. The security of DNS system used by ISPs for delivering services, also affects the overall cyber safety of the end users.

3.40 DNS based content filtering and URL blocking allows or blocks access to the website´s or URLs as per the Government orders under Section 69A of the IT Act. URL blocking is implemented effectively in DNS system maintained by ISPs, but some of the blocked websites/URLs still remain accessible to subscribers of ISP networks who are using public servers or other third-party DNS servers or DNS-based CDN servers. In absence of any regulatory and security framework, it has been observed that few CDN providers are hosting their contents co-locating them with ISP gateways through direct peering or at Private IXPs. This arrangement results into bottleneck in effective blocking of contents under the direction of Hon'ble courts or under provision of IT Act and there is possibility of by-pass of Lawful Interception system also. Further, a CDN essentially acts as a DDoS protection and mitigation platform with edge servers distributing the load equally across the entire capacity of the network, which is encouraging the ISPs to install CDN servers and provide content services. But there are numerous problems such as selecting server locations and the hidden troubles of security while investing for a CDN establishment. This

discussion makes it is pertinent to regulate the security practices and content blocking directives followed by the CDN players for which they are equally responsible.

3.41 **Non- Level playing field between telco CDNs, and other CDN players:** While Telco CDNs are subjected to various license-conditions imposed responsibilities like lawful interception, content blocking, etc., other CDN players are not. It can be argued that they can always operate CDN services under a different company. But, with evolving technology, where the same server space is partitioned to give telecom service under a license and also to offer vCDNs, it will not be easy for Telco CDNs to hive off their assets into a separate company. This causes an issue of a level playing field.

3.42 In view of all the above discussions, it can be argued that for facilitating the growth of CDN services in India, a regulatory framework is required. Therefore, the Authority seeks the view of the stakeholders on the following issues:

Q.28: What long term policy measures are required to facilitate growth of CDN industry in India?

Q.29: Whether the absence of regulatory framework for CDNs is affecting the growth of CDN in India and creating a non-level-playing field between CDN players and telecom service providers?

Q.30: If answer to either of the above question is yes, is there a need to regulate the CDN industry? What type of Governance structure should be prescribed? Do elucidate your views with justification.

Q.31: In case a registration/licensing framework is to be prescribed, what should be the terms and conditions for such framework?

Other Challenges for CDN establishment

3.43 Like Data Centres, CDNs also face multiple technical and economic challenges due to infrastructure issues. Indian players have been slower to integrate with CDNs compared to many developed countries.

One of the major challenges for a service provider or network operator to launch a CDN is the initial investment for the basic infrastructure. The basic infrastructure includes the streaming web servers with the content, the proxies, and the caching servers in addition to the network management software. Consequently, high-bandwidth costs for data transmission are also the major consideration for most CDN providers.

3.44 The costs of maintaining servers (including energy to power and cool the servers) and maintenance staff costs are also significant. Implementing and maintaining CDN servers and equipment is therefore challenging for many small- to medium-sized internet providers who have limited resources. A favorable regulatory environment can help in attracting huge investments required to set up a large number of CDN servers in India and in eliminating various other roadblocks for CDN service providers.

3.45 Broadly CDN has two types of costs. First, the CDN servers' costs that include the storage capacity, aggregating hardware, estate, and energy costs. Second, the cost of peering and IP-transit

3.46 **Costs of Peering and IP transit:** Both peering and IP transit are key technical and monetary cost components in operating a CDN network.

a. ***Peering:*** It is an arrangement between two ISPs or stakeholders to let the traffic destined to each of them pass through to reach its required destinations (end-users). Peering can be either public or private, and it allows for packet exchange on a horizontal level (without crossing from a higher to a lower-tier ISP or vice versa).
b. ***IP Transit:*** CDN transit fees are paid to transit networks to get the content from the origin servers of the Content Providers for making it available to the end-users. This cost is a function of the volume of data exchanged. The transit cost per unit of data volume can be low if the CDN owns the transit network; otherwise, these costs can be considerable. These transit costs can differ Content Provider wise, as they may have different origin servers to fetch data, and, therefore, the

path between the origin server and the corresponding ISP may differ. However, when the data is taken from the edge servers, the cost is significantly lower.

3.47 The cost of peering or IP transit is substantial and can be a barrier to the launch or success of a CDN. These costs depend on the volume (e.g., committed, consumed, etc.) of multimedia data traffic transferred or exchanged. Pricing for CDN services and charging the customers is governed by bandwidth costs, traffic distribution, content size, etc., along with the expenses incurred for peering or transit.

3.48 Apart from the above costs for CDN players, there are cost constraints involved for ISPs also to connect to CDNs or IXs. High costs of National long-distance (NLD) charges and high costs incurred in Domestic Leased Circuits (DLC (P2P)) link charges are also a major constraint for ISPs to connect to CDNs or IXs at the Data Centre. Stakeholders are requested to provide their response to the following question:

Q.32: What are the challenges in terms of cost for growth of CDN? What are the suggestions for offsetting such costs to CDN providers?

3.49 **Connectivity issues:** There are certain challenges in setting up CDN servers close to the users, including real-estate costs, the need for a large and uninterrupted power supply, and bandwidth considerations. In remote and rural parts of India, wireless connectivity is more popular than fixed-line connectivity. Dependence on wireless networks to transmit data puts a constraint on handling large data loads (video content, live-media, on-demand data, etc.) To add to this, some rural parts still have either no mobile coverage or are still being served through 2G/3G networks

3.50 In contrast, developed countries like the USA, UK, and China, have a high penetration of fixed broadband connectivity, and a majority of their data and CDN services are carried on high-speed fixed networks in the last mile. The last mile plays an important role in the CDN value chain and can stream content efficiently only when internet access

networks are fully developed and have good speed of internet access in all parts of the country. Thus, it may be argued that because of poor broadband penetration in rural areas, CDNs are not getting established there. The recent recommendations submitted to the Government by the Authority on **"Roadmap to Promote Broadband Connectivity and Enhanced Broadband speed"** dated 31th August 2021 focuses on incentivizing investment in the last mile linkage for fixed-line broadband. Apart from other measures, the Authority has also recommended a pilot direct benefit transfer scheme in rural areas for proliferation of fixed-line broadband connectivity. Faster implementation of these recommendations will ensure higher investments in fixed broadband infrastructure creation, which in turn will help in the further development of the CDN networks in the country. However, the Authority would like to understand from the stakeholders that what other measures can be taken for establishing CDNs in smaller cities.

3.51 **Location constraints:** The performance of CDNs depends on the geographical location of edge servers and PoP locations. Until and unless the users are served through CDN servers operating near them, the user experience will only marginally improve. Most of the PoPs are located in major cities like Chennai, Mumbai, Bangalore, Delhi, etc., due to power availability and enabling ecosystem for server establishment. To be viable to support CDN services, the Data Centres, and IXPs must be strategically located to provide access to multiple upstream providers (e.g., content providers or transit ISPs) and peering PoP locations.

3.52 As has been discussed in different chapters of this consultation paper, the Digital communication infrastructure ecosystem comprises various stakeholders, including CDN service providers, Data Centre operators, and Interconnect Exchange providers. These players can flourish and grow together well if the ecosystem for their presence exists in different parts of the countries. Currently, the ecosystem is flourishing mostly in Tier1 cities, these players must grow in different

States and smaller cities so that the digital economy gets boosted there also. Considering this, the Authority would like to know the views/suggestions of the stakeholders on how to overcome the location constraints and facilitate the expansion of CDNs in various Tier-2 cities.

Q.33: Do you think CDN growth is impacted due to location constraints? What are the relevant measures required to be taken to mitigate these constraints and facilitate expansion of ecosystem of Digital communication infrastructure and services comprising various stakeholders, including CDN service providers, Data Centre operators, and Interconnect Exchange providers expansion in various Tier-2 cities?

3.53 Currently most CDN, IXP (those catering sizable traffic), and Data Centres are situated mainly in metro cities like Mumbai, Delhi, and Chennai. Regional ISP (Category "B" and "C") can connect their network with CDN and IXP, only by hosting their Border Gateway Router in Data Centre or IXP premises located in these metro cities. The investment required for bandwidth connectivity from their regional point of presence to metro cities precludes most ISPs to peer directly at these locations. For providing the benefits of CDNs for subscribers of smaller ISPs, it is imperative that the connectivity between the ISPs operating on a regional basis and CDNs is promoted. Stakeholders are requested to provide their response to the following question:

Q.34: What measures can be taken for improving infrastructure for connectivity between CDNs and ISPs, especially those operating on a regional basis?

Need for Incentivization

3.54 As deliberated in the challenges section, the initial costs associated with establishing a CDN are quite high, while it takes time to get the returns on investment. Private investments are required to set up a large number of CDN servers in India. Suitable fiscal incentives

through policies can support the companies during initial investment. Stakeholders are requested to provide their response to the following questions:

Q.35: Is there a need to incentivize the CDN industry to redirect private investments into the sector? What incentives are suggested to promote the development of the CDN industry in India?

Q.36: How can TSPs/ISPs be incentivized to provide CDN services? Please elucidate your views.

3.55 Apart from the issues discussed in above sections, the Authority would like to know, if there are any other relevant issues/suggestions from the stakeholders.

Q.37: Are there any other issues that are hampering the development of CDN Industry in India? If there are suggestions for the growth of CDNs in India, the same may be brought out with complete details.

CHAPTER 4

INTERCONNECT EXCHANGES

4.1 Internet Exchange Points (IXPs) are the physical internet traffic exchange nodes, wherein ISPs and other Autonomous Systems (AS) exchange traffic between themselves. IXPs are regarded as a key component of modern internet infrastructure and contribute to global network resilience and efficiency. By keeping domestic internet traffic local, IXPs help reduce transit costs, reduce latency in the network and provide a better user experience. This is even more relevant when complementary services such as CDNs exist within the country. In the absence of an IXP, the Internet Service Providers (ISPs) should either directly interconnect with each other or exchange their local traffic through an IXP abroad. In addition, in the absence of a national IXP, the ISPs would need to connect with international ISPs for accessing the global Internet cloud.

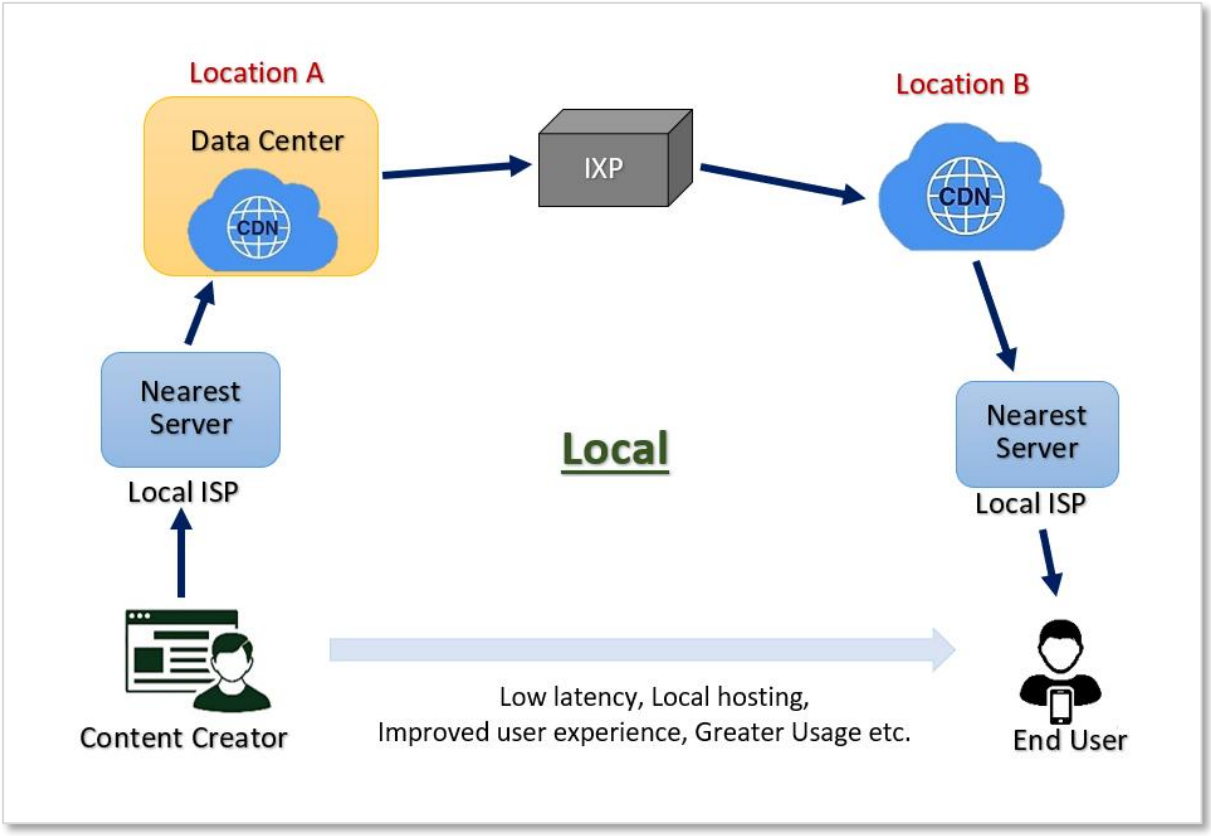
4.2 Internet Exchange Points (IXPs) have the physical infrastructure to allow two or more ISPs, CDNs, or Enterprises to transfer data between their respective networks. IXPs facilitate the transmission of data between end-users of two different provision networks. Members connected to IXPs can rent out ports, which are the physical gateways to the exchange of information. Ports may have varying speeds, which influence the rents paid for them. TRAI has previously defined an IXP as[69] :

A network infrastructure operated by a neutral, not-for-profit entity, with the purpose to facilitate the exchange of Internet traffic between Internet Service Providers (ISPs). The number of ISPs connected to an IXP is required to be a minimum of three. There must be a transparent open, and non-discriminatory policy for any ISP to join the IXP.

Figure 4.1 depicts a data transfer through an IXP

69 https://trai.gov.in/sites/default/files/9.pdf

Figure 4.1: Local data transfer through an IXP

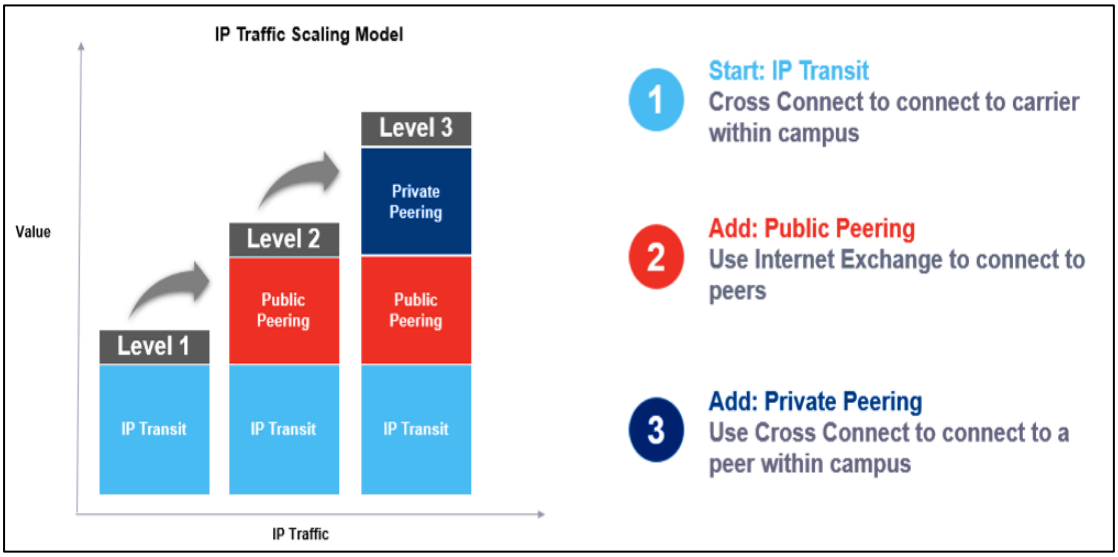


4.3 For a developing country like India, which has the second-largest population globally but has low wireline Internet penetration, Internet exchanges are essential. As more and more users demand fast, reliable, and consistent Internet connections at homes for fulfilling their entertainment, work, and educational needs accessed over multiple devices, delivering high-quality connectivity is necessary for which Internet Exchanges are required.

4.4 **IP transit and Peering:** IP transit is when one entity pays another for the right to transit its upstream network. In this arrangement, one entity has a higher status than the other in the hierarchy, so there is no longer a peering relationship from an internet standpoint because both parties do not benefit equally from the exchange. When enterprises or smaller ISPs connect to a bigger ISP to reach the entire internet, it is known as IP transit. Whereas IP peering is a mutual

exchange of data between two ISPs, and the amount of data exchanged is typically close to equal. The respective ISPs do not charge for this arrangement as both parties benefit equally – this type of data exchange is known as settlement-free. IXPs provide the necessary infrastructure to allow 'peering' between members connected to it. Internet exchange points thus facilitate public peering between multiple stakeholders. Connected via ports, peers are usually ISPs but can also include CDNs and Data Centres among other service providers, who have rented ports on the IXP. The costs associated with operating IXPs are usually shared between the participating infrastructure and network providers. IXPs facilitate public peering arrangements between multiple stakeholders, permitting exchange of internet traffic for free. Some large networks, with greater market share, may charge smaller networks for peering services. Public peering via IXPs continues to grow in terms of traffic carried and the number of ports required at IXPs. As the amount of data exchanged between two stakeholders increases, they may think of private peering. These stages have been shown in Figure 4.2.

Figure 4.2: A Peering Life Cycle model



(Source: blog.equinix.com)

Demand drivers for IXPs

I. Effect of Internet Ecosystem

4.5 **Rapid digitization and increased user base:** In the last few years, rapid digitization in the country is leading to increased domestic IP traffic. Under Digital India Initiatives, a massive countrywide infrastructure has been evolving, and large-scale digitization is taking place to enable easy, reliable access over the internet to the citizens. The internet users base in India is about 800 million by the end of FY 2020[70], and according to the new Cisco Annual Internet Report[71], India will have over 907 million internet users by 2023, accounting for 64% of the total population.

4.6 **Growing domestic IP traffic:** The role of Internet Exchange became prominent during the pandemic as most of India's workforce and students worked from home and data traffic and use of the internet increased heavily. The domestic IP traffic has surged tremendously; there was a significant increase in traffic in categories like gaming, OTT streaming services, ed-tech, and Cloud services, among others. One of the Internet exchanges in India has mentioned that during the lockdown, OTT traffic surged 198.68 percent, hosting traffic (storage space and access for websites) went up by 62.78 percent, ISP traffic increased by 54.38 percent, among others.

4.7 **Applications requiring reduced latency and enhanced broadband speeds:** The demand for video streaming, gaming, virtual reality, etc., warrants high broadband speeds and low latencies. The transmission of data over long distances to foreign IXPs often leads to a significant increase in latency. The data would have to travel upstream to the IXP and then again downstream to the end-user. The long transmission path causing increased latency affects services relying on low latency connections. With the creation of a local IXP, the transmission path reduces and leads to reduced latency. Experiences have shown that for ISPs, local links offer up to 10 times faster transmission speeds, as the data makes fewer hops to reach its destination. The working paper of the United Nations ESCAP (Economic and Social Commission for

70 TRAI's Telecom Subscription data as of 31st December 2020

71 https://www.cisco.com/vni-forecast-highlights/mobile/pdf/India_Internet_Users.pdf

Asia and Pacific), highlighted a statistically significant and positive relationship between the number of IXPs and fixed-broadband performance parameters like speed and latency[72]. For every 1% increase in the number of IXPs per 10 million inhabitants, the download speed (Kbps) of fixed broadband is expected to increase by about 0.8%. In addition, the preliminary findings emphasized a significant and negative correlation between the number of IXPs and latency that for every 1% increase in the number of IXPs per 10 million inhabitants, the latency *(delay in milliseconds)* of broadband is expected to decrease by about 0.4%. As the latency decreases it ultimately increases the upload and download speeds.

II. Technical benefits

4.8 **Network benefits:** The network operators using IXPs will have more autonomy and control over their own resources, including routing and traffic management because it decreases a network's dependency on third-party networks. IXPs play an important role in providing better networking capabilities and strong network connections. As technology advances the QoS expectations, performance, scalability, control and rising speed of the internet exchanges, the requirement of new IXPs will arise. A secondary effect of IXPs is that they improve competition, which is often a key policy objective of liberalized telecom markets and policymakers.

4.9 **Improved resilience:** IXP improves the stability and continuity of internet access by redirecting the Internet traffic when there are connectivity issues. In the context of service interruptions, IXP improves a country and region's overall resiliency that can occur outside their area. When an upstream service provider experiences an outage, the stability and continuity of local traffic can be maintained because the IXP can provide additional flexibility in redirecting internet traffic when these connectivity problems occur. Big Enterprises also connect to IXPs because of these direct network

72 https://www.unescap.org/resources/estimating-effects-internet-exchange-points-fixed-broadband-speed-and-latency

advantages. This partnership between enterprises and IXP operators is mutually beneficial and amplifies the need for IXP establishment.

4.10 **National Security:** As the data remains local, interception by foreign agencies over the internet is avoided and hence security is improved. Once IXPs achieve critical mass, they become the centre of a vibrant Internet ecosystem in the country, involving most of the ISPs, content providers, business, academics, and Government users through better, faster accessible services.

III. Economic Benefits

4.11 **Reduced costs and savings of Foreign Exchange:** The flow of data to upstream foreign internet service providers requires payment to the IXP located abroad, losing foreign exchange for every transmission that is made, as for both, i.e., sending the ISP as well as receiving the domestic ISP have to pay their upstream foreign service providers. A local IXP can aggregate requirements of Indian ISPs and exchange international traffic at lower negotiated rates saving foreign exchange.

4.12 **Promotes local economy:** IXPs build up confidence in providers by attracting key internet infrastructure providers for hosting the content locally. Local IXPs improve the existing digital infrastructure connectivity and have the potential to become a hub for local and international operators. As more people come online, the demand for hosting internet services locally rises, which necessitates the presence of local IXPs.

4.13 **Lower bandwidth utilization costs:** Networks that need to lease connections from licensed TSP to reach an IXP faces a local bandwidth cost, especially in a developing country[73]. Creating local IXPs enables efficient bandwidth utilization for routing of the domestic traffic. More choices become available to ISPs for sending upstream traffic to the rest of the internet contributing to a more competitive wholesale transit market. Further, the IXPs have the potential of lowering the

73 https://www.internetsociety.org/wp-content/uploads/2012/12/promote-ixp-guide.pdf

operating costs for local ISPs, while increasing the traffic, which leads to optimization of revenues of ISPs.

4.14 **Positive spinoff of increasing Data Centres:** IXPs and content providers often share space in Data Centres and facilitate access of content to local users. Moving content closer to business and customers is getting reflected in the growth of content networks and regional Data Centres. As the deployment of Data Centres is increasing and networks are shifting towards more and more local traffic, overall traffic on IXPs is increasing, thereby Internet exchanges are becoming an attractive customer to carrier-neutral Data Centre operators. As the number of Data Centres increases, the IXP market will also grow.

4.15 **Content peering:** The majority of the content consumed by end-users is available presently by peering with the big content providers (like Google, Facebook, etc.). At an IXP, CDNs connect with each other where local internet traffic is exchanged and routed locally. Content providers and CDN operators globally are pushing service providers to connect to IXPs for faster content movement. With huge content consumption and evolving markets, more CDN providers would connect to IXPs and this, in turn, will increase demand for a greater number of private IXPs in near future. There is a need for Data Centres, ISPs, CDN operators, content creators, and even consumers to come together to overcome challenges like connectivity, resiliency, and security, adopt new IX models and enforce new IXPs to improve the landscape of internet peering and interconnect.

4.16 **New business opportunities:** IXPs can be instrumental in developing the local internet ecosystem, by attracting a range of local and international operators. Enterprises also join IXPs as part of their digital transformation strategies. Moreover, IXPs play a major role in digital innovations like AI, Cloud, Blockchain, Big Data, etc., by increasing operational efficiency, aiding in migration to business-critical applications and services, and triggering more business opportunities. The increasing importance of cloud infrastructure and

application services across the corporate world is driving the enterprise toward the internet exchanges, looking for lower latency.

International Experience

4.17 Globally, a number of approaches and implementation methods are being realized to boost the IXP establishment and traffic exchange operations. Many independent IXPs have been set up for ISP peering, for the purpose of routing the local IP traffic within the country. The international best practices of a few successful case studies have been discussed in this section based on the information from the IXP websites, case studies that serve to demonstrate the benefits of expanding the IXPs, and what policy or recommendations the countries have implemented for supporting private IXPs.

a. Singapore: Singapore Internet Exchange (SGIX), 2010[74]

4.18 To promote Singapore as a major information hub for the region, the Singapore Internet Exchange (SGIX), a not-for-profit exchange, was established in 2010 as a neutral Internet exchange to enhance the environment for local and international network traffic[75]. SGIX (Singapore Internet Exchange) is one of the largest not-for-profit Internet exchanges (IXs) in the region. Launched in 2010 as an initiative under the Singapore government's Intelligent Nation 2015 (iN2015) master plan. Offering an efficient central point of traffic exchange for ISPs, the SGIX has catalyzed the growth of Singapore's information industry by encouraging content hosting and related developments such as the establishment of Data Centres. The new IXP arrangements enabled customers of the ISPs to access local content from other ISPs even during cable outages, which occur on the international network. Using a local exchange like SGIX also helped cut connectivity costs and improved the resiliency of their networks. It

[74] https://www.internetsociety.org/resources/doc/2021/effective-ixp-strategies-for-the-asia-pacific/
75 https://www.sgix.sg/

also reduced the latency their customers experienced when accessing local content.

4.19 Singapore's regulatory environment encourages all network operators, including those with significant market power (SMP), to interconnect on agreed terms. SGIX enjoys participation from a full range of brand-name peers, including operators from global and domestic network providers, social media, and video streaming companies, as well as cloud infrastructure providers, CDNs, online gaming companies, educational institutions, and research organizations. SGIX does not see these other operators as competitors. Its mandate is to promote Internet peering in Singapore and to complement other exchanges in the ecosystem. Practicing full transparency both operationally and financially it assists potential members to evaluate the exchange fairly against the alternatives.

4.20 In a recent study, the cost of routing the local traffic through SGIX was estimated to be almost 95% cheaper than using international transit service, local latency is reduced and an aggregate of over 500 Gbps of data is transferred domestically among SGIX members as of May 2021. Moreover, each domestically exchanged transaction frees up an equal amount of international bandwidth, thereby improving connection speeds and reducing latency over Singapore's international links as well.

b. London: UK – London Internet Exchange (LINX), 1994

4.21 London Internet Exchange (LINX) is one of the world's largest and oldest internet exchanges. LINX was founded in 1994 by a group of ISPs and educational networks and is a founder member of Euro-IX, a Europe-wide alliance of Internet Exchanges. It is currently one of the largest neutral IXPs in Europe in terms of average throughput. Initially, LINX membership was restricted to operators of traditional ISPs. In 2000, this restriction was relaxed and today a wide variety of networks peer at LINX exchanges, including Google, Akamai, Yahoo, and the BBC. The LINX network consists of Ethernet switching

platforms installed across various United Kingdom locations[76]. As of March 2021[77], LINX facilities have about 1700 connected member ports with more than 950 member ASNs, interconnecting high traffic volumes. The products and services at LINX are designed to reflect the changing network and interconnectivity requirements, to help members expand and grow their own networks.

4.22 The LINX exchanges have been established on an open, neutral, settlement-free peering facilities model, working for the interests of its members. This not-for-profit model is widely adopted in the developing world as it builds trust and infrastructure and fits well with capacity-building programs. LINX observes significant expansion demand, port orders, and increasing peak traffic volumes throughout the year. Built on a robust network infrastructure the LINX successfully meets its objectives of increasing network capacity, geographical and port expansion demands, and development of offered products. LINX aims to meet member needs better, service more interconnection products and deliver a continued digital transformation.

4.23 LINX Products and Services are focused on developing new products for LINX members such as Public Peering Network traffic exchange over a shared network; Private Interconnect Member point-to-point connections; LINX connection with partners via vLAN; Access Points connections with Data Centres; Private vLAN allowing members to connect to other members from LINX.

c. Equinix: United States, US-IX, 1996[78]

4.24 A great deal of global traffic traditionally passes through the United States. Traffic from Europe joins traffic from the U.S. on the West Coast, where a series of landing stations feed traffic to Asia. The Atlantic submarine cable systems are home to the most advanced and densely served subsea links on the planet. While Europe has double

76http://www.linx.net

[77] https://www.linx.net/wp-content/uploads/2021/07/LINX-Annual-Report-2020.pdf

[78] https://www.internetsociety.org/resources/doc/2021/effective-ixp-strategies-for-the-asia-pacific/

the number of exchanges than any other region, the United States has more exchanges than any single economy.

4.25 United States is the home of the earliest Internet exchanges. PAIX, the Palo Alto Internet exchange, was the first commercial, carrier-neutral exchange point in the United States. Launched in 1996, it was owned and operated by Digital Equipment Corporation. Today it is owned and operated by Data Centre operator Equinix. The North American market is dominated by commercial exchanges, but there are community-led open exchanges also in the USA of which the Seattle Internet Exchange (SIX) is the largest with more than 270 peers. The not-for-profit Seattle IX (SIX) handles more traffic than any other public exchange in the U.S., with peak speeds approaching 2 Tbps as of May 2021.

4.26 As Equinix runs a commercial operation, it has certain advantages over associations and other not-for-profit exchanges. Equinix bundles a range of Data Centre and interconnection services. Equinix has quickly become the leader in the Internet exchanges. As a commercial exchange, Equinix doesn't publish traffic statistics. It is not known how much traffic is being exchanged under either its bilateral or multilateral peering services, however, Equinix's global traffic is substantial.

d. Kenya: KIXP, 2000

4.27 In Kenya, the Kenya Internet Exchange Point[79] (KIXP) grew rapidly and now ranks among the world's top 15 IXPs in terms of growth in traffic exchanged. After nearly a year of preparatory work, including the design and implementation of a capable technical operation, funding model, and legal framework, the KIXP was launched in late November 2000 and is located in Nairobi. To leverage the value of KIXP, Google installed a Google Global Cache in Kenya, which can be seen as an instance of a local Data Centre. This had a significant impact on traffic levels in Kenya and a dramatic surge in traffic exchange was seen after

79https://www.tespok.co.ke/?page_id=11651

the Data Centre was installed. The benefits of the KIXP extend beyond the Kenyan borders, KIXP members are beginning to attract customers from neighbouring countries due to the increased bandwidth and low latencies. In addition, Kenya is starting to attract external ISPs to exchange their own traffic at the KIXP further boosting its revenue.

e. The Bahamas

4.28 The Bahamas regulator the Utilities Regulation and Competition Authority (URCA) released a consultation[80] on 'Framework for Establishment of IXPs in the Bahamas' in May 2019. At that time, there were no IXPs in The Bahamas. As a result, local ISPs routinely routed locally generated internet traffic destined for local users through intermediary networks and digital infrastructure in another country. URCA initiated the Consultation intending to stimulate the market entry of IXPs in The Bahamas and set out its initial thinking on the regulatory measures for the setting up of IXPs. The creation of a local IXP was cited as one of the critical factors if the Government is to realize the Grand Bahama 'technology hub' ambitions. The consultation aimed to promote public awareness of the contributions that IXPs can make to the development of the internet and digital economy in the Bahamas; to alert potential IXP users of URCA's framework for the entry of IXPs in the market, and to ensure that the regulatory framework is favorable for IXPs to operate successfully. For this URCA proposed strategies regarding IXP location, governance and decision-making, participation, business model, and funding.

4.29 In the final paper issued on 21st August 2019, URCA clarified the regulatory framework for market entry of IXPs in The Bahamas. URCA favored the light-touch regulatory measures, as per the statutory framework of their Communications Act. URCA aimed to put in place fit-for-purpose measures for market entry of IXPs, and to foster dialogue/consensus on IXP implementation factors among stakeholders, in a twofold process. URCA also proposed to set up a

80https://www.urcabahamas.bs/framework-for-establishment-of-ixps-in-the-bahamas-consultation-ecs-07-2019/

Working Group to facilitate further discussions and consensus on IXP governance and operational factors amongst the stakeholders.

f. Others

4.30 Several countries have an independent body like the IXP Association (IXPA) for coordination of all the IXP operators and regional IXPs for easy management, interconnection, cooperation, knowledge sharing, promoting competition, and global development. The IXPAs are established on a regional basis: AFIX for Africa, APIX for Asia and the Pacific, Euro-IX for Europe, and LAC-IX for Latin America and the Caribbean. Along with the internal functioning of the exchange, the external environment to the exchange is equally important. An IXP grows with its large geographical user base, the service providers that address that user base, and the infrastructure and regulatory environment in which it finds itself. A compilation of Global practices in IXP services from other countries is given in **Annexure III**.

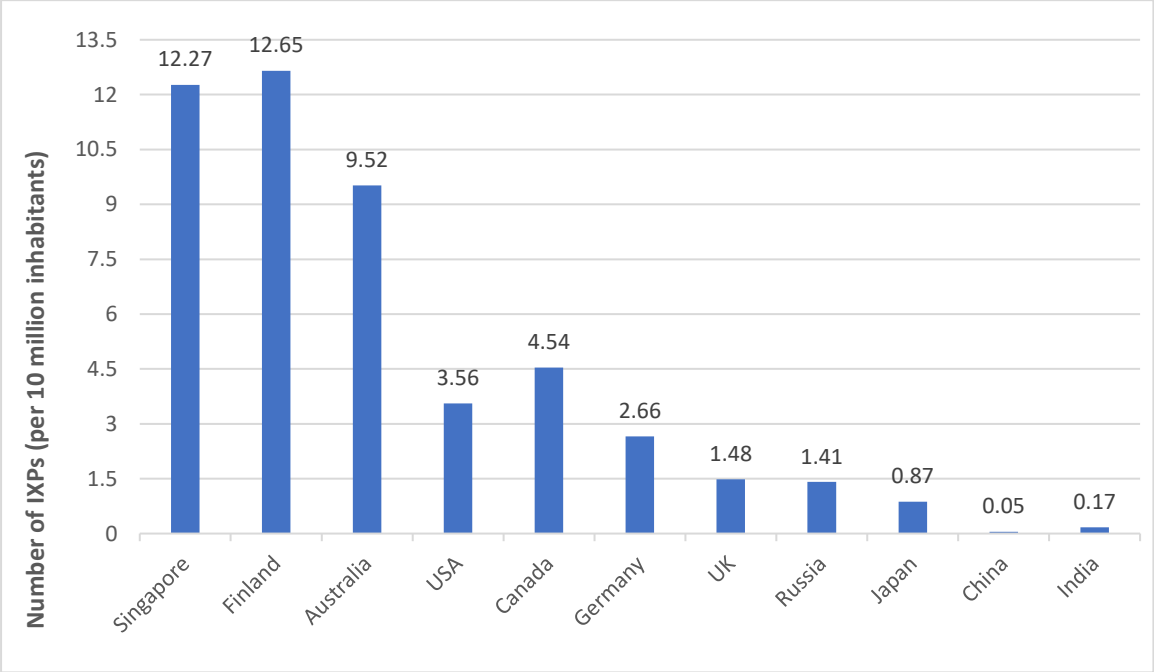
Need for more Interconnect Exchanges in India

4.31 An IXP is an essential part of the internet ecosystem in countries with multiple ISPs and other content service providers. Operation and maintenance of a high-capacity and robust IXP is crucial for providing low-cost internet to end-users. With no IXP, internet traffic will go outside the country to foreign IXPs for peering. As the number of ISPs as well as their traffic is increasing, there is a need to localize the internet traffic and avoid using foreign IXPs to peer domestic ISPs. According to ITU, the Government can further encourage the creation of IXPs by advising ISPs and other service providers on the benefits of connecting to an IXP. This can aid both ISPs and non-ISPs to rent ports to connect to IXPs.

4.32 Most of the developed countries already have IXPs operating in their network. The developing countries are in the process of deploying self-sufficient IXPs and saving the foreign exchange. Figure 4.3 represents the number of IXPs by countries per 10 million habitants wherein India is having less than 1 IXP per 10 million habitants. Having more

than 800 million internet users at present and expected to reach 975 million by 2025[81], the existing number of IXPs in India may not be sufficient to meet the internet traffic demands. Establishing more IXPs not only helps in managing traffic but encourages more local content development, creates incentives for local hosting of Internet services due to the larger pool of local users, who will be able to access online content faster and cheaper. Need for setting up more IXPs in the country arises, so that the ISPs peer together to route the domestic IP traffic within the country.

Figure 4.3: Number of IXPs per 10 million inhabitants (2021)



(Source: 'Inclusive Internet Index 2021' produced by Economist Intelligence Unit Limited)

4.33 The boom in internet usage and content consumption online has necessitated the expansion of internet exchange infrastructure. The Data Centre industry in India would further require exchanges that allow for transmission and interconnection at cheap rates and without any delays or congestion in the network. There is a need for encouraging IXPs to be set up and expand capacity at exchanges. These can further allow a variety of new peers such as CDNs, Content

81 https://www.statista.com/statistics/255146/number-of-internet-users-in-india/

Providers, and Data Centres to connect and allow low latency services. Several other aspects that demand operating an IXP are deliberated in the subsequent section.

4.34 IXPs help in improving network design and infrastructure for service providers. However, the IXPs in India are situated in Tier-1 cities only, resulting in a scalability issue of individual interconnections and confining the peering and internet landscape to limited areas. As traffic exchange is required closer and closer to the edge, more exchanges might be needed in smaller cities and locations. Alternatively, an ISP can connect directly to content providers, resulting in lower costs and helping smaller ISPs compete with larger players.

As the data traffic is increasing in the country, more IXPs will be required to meet the growing traffic demands. The Authority, therefore, seeks the views of the stakeholders on the following question:

IXP Business Models

4.35 IXP business models vary depending on whether an IXP is for-profit or not-for-profit. In general, a for-profit IXP aims to be profitable and distributes this profit as a dividend, or payment, while not-for-profit IXPs exchange traffic, without the intention of distributing profit, but to invest any surplus funds in the future development of the IXP. Some not-for-profit IXPs charge fees for their services based on a cost-recovery model, whereas others seek external support such as sponsorships, subsidies, or donations. Normally, a not-for-profit IXPs operates under one of the following models: **free, subsidized, or independent**.

Table 4.1: Non-profit IXP business models[82]

Model	Free	Subsidized	Independent
Description	• Relies on contributions from IXP network members and volunteers. • Contributions can be in the form of labor, equipment, time, money, or other as per the IXP needs. • No membership, joining or monthly fees are charged to the IXP participants.	• Based on subsidies from the Government or an external entity that sponsors the IXP, mostly for a sustained period. • The IXP meets some of the operating costs by charging members a nominal fee. • In some cases, contributions from IXP members gradually allow to cover OpEx and members to take ownership of the IXP and eventually to the transition to a fully independent model.	• Based on income generated by fees paid by members on a recurring basis. • Additional revenues from value added services, one-time fees, etc. • All operational expenses are met by the IXP. • Typically, this model is introduced when the IXP matures and has proven its value to operators and the ecosystem.
Advantages	• Low cost of peering for members with no additional costs other than capacity to IXP.	• Low-medium cost of peering for members in addition to the cost of leasing capacity to the IXP. • Sustained revenue to meet operational expenses. • Easy to scale and grow due to ability	• Neutrality of the IXP is guaranteed in a self-sustained model. • Sustained revenue to meet operational expenses. • Easy to scale and grow due to ability to implement and maintain

[82] https://www.itu.int/en/ITU-D/IXPs | Governance and Financial Models : Best practices for sustainability.pdf

	• Low operating costs for the IXP organization. • Volunteer driven; less complexity on organization and management.		to implement and maintain management/operational structures.	management/operational structures.
Examples	• IXP in Seattle and Washington in the USA. • IXP in Uganda (UIXP)	• Nigerian IXP (IXPN). • IXP in Malaysia.		• Most of European IXPs • Kenya IXP (KIXP) • IXP in Johannesburg (JINX)

4.36 While community-led exchanges have to treat all members equally, put the interests of members first, and avoid competing with its members, a commercial internet exchange can make itself an attractive colocation site over and above the interconnection offer. A for-profit commercial exchange can have favorable pricing suiting to the prospective member. The differential pricing practices allow for better margins than the cost recovery charging at not-for-profit exchanges. Further commercial exchanges have the potential to raise capital or take debt to grow through acquisition

4.37 For the non-commercial IXPs, the choice of business model is an important factor that impacts the management and sustainability of its operations. Ensuring the presence of a local interconnect exchange (IX) has become an increasingly important economic priority for many countries. IXPs help in developing the local internet industry, improve the market competitiveness and serve as a hub for new technical

activities by ensuring better and more connectivity, particularly in less connected areas of a country.

Policy and Regulatory initiatives In India

4.38 The requirement of creating an Internet exchange point for peering of the ISPs was felt in India as early as 2002 when TRAI set up a Task Force involving experts from DIT, IIT Delhi, IIM Ahmedabad, C-DOT, TEC, and ISPAI, with an objective to prepare an action plan to achieve faster growth of the internet in the country. The Taskforce recommended the establishment of IXP for the exchange of internet traffic within the country.

A. National Internet Exchange of India (NIXI)

4.39 TRAI forwarded the recommendations of the task force to the Government in August 2002, it included setting up of NIXI in the country under the umbrella of an Industry representative not-for-profit, neutral body. The taskforce emphasized that this would result in cost-saving on international connectivity, lower internet usage prices for the consumers, and also improve the quality of service. The Government accepted the recommendations for setting up NIXI under a grant by the Department of Information Technology.

B. Present Status of NIXI[83]

4.40 National Internet Exchange of India (NIXI), registered as a Section 25 company under the Companies Act of India, is a public-private partnership between the government of India and industry ISPs. NIXI offers different ports capacity to ISPs, CDNs, with different billing cycles. Initially, four nodes of NIXI were made operational at Noida, Mumbai, Chennai, and Kolkata, which were physically hosted at the premises of Software Technology Parks of India. Currently, NIXI has 8 nodes[84], one each at New Delhi (NOIDA), Mumbai, Chennai, Kolkata,

[83] www.nixi.in

[84] https://nixi.in/en/noc-locations

Bangalore, Hyderabad, Ahmedabad, and Guwahati, with a plan to interconnect Mumbai IX to Hyderabad IX. NIXI is presently working on expanding to two more IXP nodes at Lucknow and Mohali.

Table 4.2: Number of ISPs connected at NIXI nodes over the years

Year	Total ISP operators *	ISPs connected to NIXI
2003	135	27
2011	167	36
2019	358	67
2021	449	91**

(* Number of ISP operators as per TRAI Performance Indicator Reports, ** by the end of August 2021)

4.41 Presently, 91 ISPs are connected with the various nodes of NIXI by the end of August 2021, and the aggregated maximum traffic exchanged at all the nodes is 245 Gbps as of May 2021[85]. Table 4.1 shows the trend of ISPs joining NIXI since its launch.

4.42 It was observed that despite NIXI's infrastructure having been established in 2003, only few operational ISPs had joined NIXI nodes at various locations and the total number of connections to NIXI from these ISPs was very less. There were many issues in the efficacy of NIXI and a big chunk of domestic traffic was still not routed through NIXI, negating the very purpose. The Authority expressed concern over the limited number of ISPs linked with NIXI resulting in sub-optimal utilization of the infrastructure.

C. The Authority's earlier regulatory interventions

4.43 To promote a better utilization of NIXI infrastructure, TRAI sought views on the need to establish NIXI nodes at all state capitals to support small ISPs and made the recommendations on "Improvement in the Effectiveness of National Internet Exchange of India (NIXI)" to

[85] https://www.nixi.in/static/nixi_pdf/NEWS/Expression_of_Interest-NIXI_VendorEmpanelment.pdf

DIT and DoT, in April 2007. Recommendations[86] focused on improving interconnections between NIXI and ISPs, which were accepted by DoT in June 2009. Some of the recommendations regarding the announcement of routes by ISPs, connection by regional ISPs to NIXI through upstream ISP over a single link, and upgradation of ISP link to NIXI were implemented. NIXI has also reduced various charges, including connectivity charges.

4.44 TRAI issued another Consultation Paper on "Issues related to Telecommunications Infrastructure Policy" on 14th January 2011. Issues were raised for consultation regarding the need for effective IXPs in the country to efficiently route domestic IP traffic; on the licensing framework of the entities for setting up IXPs in India; and whether to permit the Unified licensees to setup IXPs in the country, who have no vested interest in the routing of the IP traffic. TRAI issued Recommendations in 2011, dealing with the issues related to IP infrastructure covering IXPs. The Authority recommended that:

a. *IXPs may be brought under Class license. Once this recommendation is accepted, detailed terms and conditions of the Class license for IXP services will be provided by TRAI.*
b. *Data Centres may be permitted to connect directly to the IXPs.*
c. *National level ISPs and International Internet bandwidth (IIB) providers may be mandated to connect to all IXPs.*

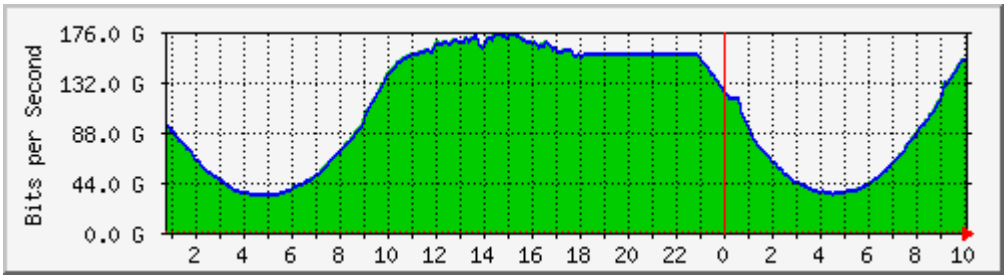
Although ISPs and IIBs are mandated to connect to all IXPs, the number of ISPs connected to NIXI is still few. *(refer to Table 4.1)*

4.45 The significant difference between NIXI and most IXPs around the world is in charging according to the amount of data peered. Most exchanges across the world have flat rates for membership or a rental per port according to the speed of the port. NIXI charges customers who wish to peer on a volume basis, according to the amount of data peered by them, which is paid for by the requester of data. NIXI initially adopted mandatory multilateral peering, enforced a system of

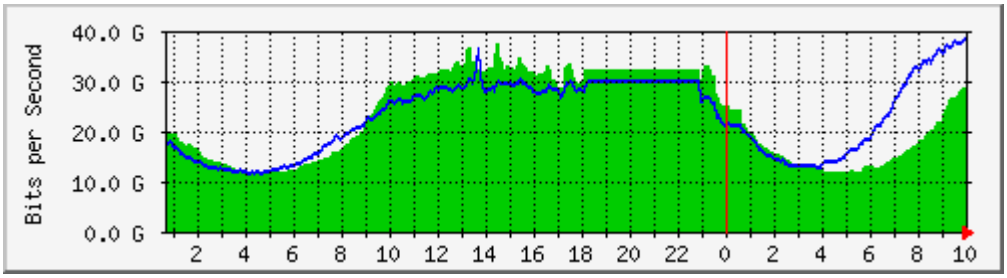
[86] https://www.trai.gov.in/sites/default/files/recomen20apr07.pdf

settlement fees, and barred content providers from joining the exchange. Only ISPs, as recognized and licensed by DoT, were till recently allowed to peer on NIXI, which excluded the content providers. The delay in allowing cloud and content providers has accordingly shaped the ecosystem. The largest content and cloud companies have established their peering facilities at competing exchanges, or within ISPs. NIXI has only recently changed this policy to allow CDNs to peer. The daily traffic graph of various NIXI nodes is depicted in Figure 4.4.

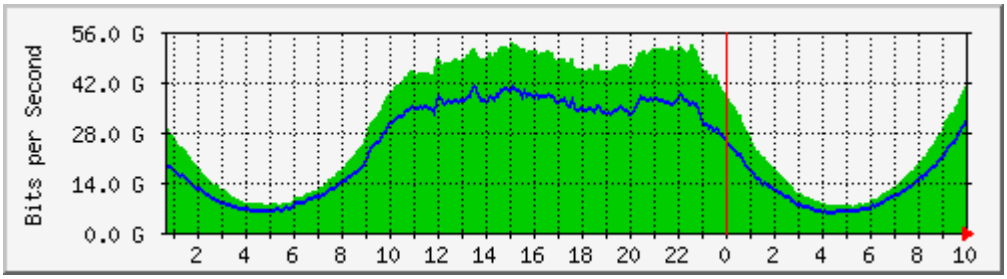
Figure 4.4: Traffic analysis of NIXI



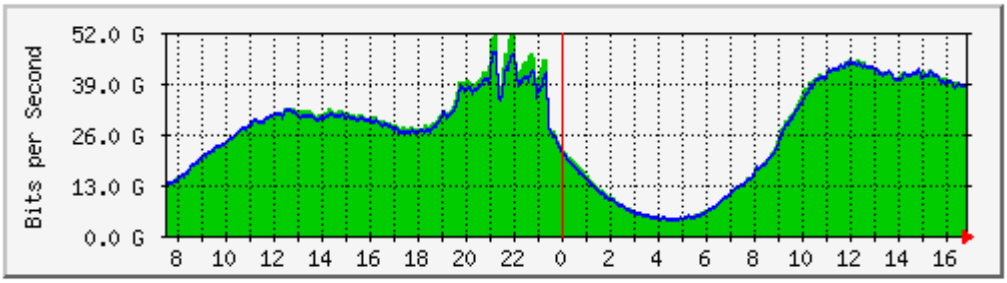
a. Aggregated daily graph for all locations



b. Aggregated daily graph for Delhi (NOIDA) port



c. Aggregated daily graph for Chennai port



d. Aggregated daily graph for Mumbai port

(Source for all 4.4 a-d: mrtg.nixi.in

Note: MRTG bandwidth data (5-minute average): GREEN Incoming Traffic and BLUE Outgoing Traffic in bits per second as on 11-Oct-2021.)

NIXI as an IXP has not been as effective as some of the similarly placed global players have been. Presently NIXI is not a telecom licensee and therefore is not directly under the regulatory purview of TRAI and DoT. There is clear resistance of the service providers to join NIXI, which cannot be mandated as NIXI is not a service provider.

D. Existing regulatory framework Issues

4.46 During the Consultation on *"Roadmap to Promote Broadband Connectivity and enhanced Broadband speed"* in 2021 the stakeholders raised concerns about the performance of core networks affecting the performance of the fixed and mobile broadband together and solicited that for matching the global average broadband speed, delivery of maximum content to users at the edge of the network becomes a necessity. This delivery however is dependent on the design and resilience of core networks as well as on how much of the traffic originates outside the nation. Further concerns have been expressed regarding frequent congestion of National Internet Exchange of India (NIXI) ports for some TSPs and stepping up of investment in NIXI and increase in capacity at the peering sites have been suggested to avoid latency and give a boost to the domestic traffic.

4.47 The Authority has noted the concerns expressed by the stakeholders regarding frequent congestion of NIXI ports and the suggestion of stepping up of investment in NIXI to increase capacity at peering sites

for avoiding latency, and it was stated that a separate consultation on the issue of Internet Exchange Point (IXP) along with content delivery networks and Data Centres will be done with the industry.

4.48 Presently there is ambiguity in Licensing framework of IXP in India, leading to confusion. While some IXP players in India are operating under ISP license, one of the major players, i.e., NIXI does not have any license. Another IX player who was operating without license has litigated against DoT. Lack of clarity and confusion has resulted in litigation and new private investment is getting affected. Therefore, clarity in respect of licensing framework for operating IXPs is required.

4.49 Those IXPs who are operating under Internet Service Provider licence to provide interconnect exchange facility to the users (most of whom are other ISPs), cannot be considered to be neutral players. Being in the same business and competing with other ISPs, they can discriminate and refuse/delay interconnectivity. This conflict of interest may lead to a problem of trust with the competitors and can result in abuse of their position as IXP. Another issue discussed with respect to the CDN content blocking is that the blocked contents ordered for blocking under Section 69A of IT Act have been found hosted at IXPs which are neither regulated nor mandated to implement the blocking system at exchange points. This scenario may result into bypassing of blocking directions of Hon'ble courts and MeitY under the IT Act in matters of national security. For unbiased peering, interconnection and security, it can be argued that there is a need for a regulatory framework whereby a separate license may be given for IXPs. This can help in promoting IXPs in the internet ecosystem.

Observing the present status of NIXI and in view of the above discussions stakeholders are requested to provide their response to the following questions:

Q.38: Do you think that presently there is lack of clear regulatory framework/guidelines for establishing/operating Interconnect Exchanges in India?

Q.39: What policy measures are required to promote setting up of more Internet Exchange Points (IXPs) in India? What measures are suggested to encourage competition in the IXP market?

Q.40: Whether there is a need for separate light-touch licensing framework for operating IXPs in India? If yes, what should be the terms and conditions of suggested framework? Do justify your answer.

Q.41: What business models are suitable for IXPs in India? Please elaborate and provide detailed justifications for your answer.

Other Challenges for growth of IXPs

4.50 The presence of Internet Exchange benefits the entire Internet ecosystem and encourages broadband penetration in India. However, the establishment and operation of IXPs encounter several technical, economic, and policy-related issues that are deliberated in this section.

Location and Resource availability

4.51 The internet exchange must be located in a building that is can fulfil its space, power, cooling, and security needs. Before setting up IXP at a location, availability of electric power, backup supply or generator, availability of reliable telecom links to the site, access to fiber facilities or rights-of-way, ability to build antenna towers or dig trenches for fiber, ease of access, etc., need to be ensured among others. Identifying potential site locations and managing them is one of the primary issues faced by an IXP.

4.52 In India, the majority of IXPs are located in coastal states and metropolitan cities where submarine cable infrastructure exists for connecting to foreign exchange. Figure 4.5 and table 4.3 shows that very few IXPs are located in the northern, central, and northeast regions, though there is significant penetration of internet and use of digital services in these areas. The growth of IXP in India has been

confined to Tier-1 cities like Mumbai, Chennai, Kolkata, Delhi, etc., only.

Figure 4.5: Internet Exchange Map

(Source: pch.net – Internet exchange directory)

Table 4.3: IXPs operating in India (as of September 2021)[87]

S.no.	Location	Name of the IXP	Connected Peers/ ISP Participants
1	Mumbai (5 IXPs)	National Internet Exchange of India (NIXI)	44
		Mumbai Internet Exchange (Mumbai IX)	359
		Extreme IX Mumbai	189
		AMS-IX India	48
		Bharat IX - Mumbai	10
2	Chennai (4 IXPs)	National Internet Exchange of India (NIXI)	24
		Extreme IX Chennai	19
		DE-CIX	19
		REDIX	4
3	Kolkata	National Internet	10

[87] https://www.pch.net/ixp/dir

	(4 IXPs)	Exchange of India (NIXI)	
		Extreme IX Kolkata	10
		IIFON IX Kolkata	10
		DE-CIX	7
4	New Delhi (4 IXPs)	National Internet Exchange of India (NIXI)	34
		Extreme IX New Delhi	135
		DE-CIX	45
		ANI Peering Exchange	15
5	Hyderabad (2 IXPs)	National Internet Exchange of India (NIXI)	8
		Extreme IX Hyderabad	13
6	Guwahati	National Internet Exchange of India (NIXI)	7
7	Amaravati	Amravati Internet Exchange (AMR-IX)	4
8	Ahmedabad	National Internet Exchange of India (NIXI)	4
9	Bangalore	National Internet Exchange of India (NIXI)	4

(Source: pch.net – Internet Exchange Directory)

4.53 India is a vast country with many internet service providers, who serve around 800 million internet users. Such operating scale requires highly distributed IXP locations and sites. However due to lack of connectivity and infrastructure, most states and Tier-2 cities do not have IXP presence, and they miss on the incidental benefits that an IXP presence can give. Companies or small exchange operators need to be encouraged/incentivized to set up IXPs at locations closer to the Tier-2 cities. This would lead to more efficient and economical interconnection and will serve the customers at the edge itself.

4.54 The content distribution and media networks often attempt to reduce their transit traffic by deploying peering relationships as much as they can through implementing an open policy with many IXPs, allowing other providers to peer with them. On the other hand, ISPs require connection to IXPs for the exchange of local IP traffic and resilience purposes. To derive the advantages of IXPs and public peering relationships, their growth, and sustainability, the number of connected members should be a good percentage. The successful

interconnect exchanges will then progressively expand from their initial Tier-1 site, to create new nodes in second-tier metro areas. In view of the aforesaid the Authority solicits the views of the stakeholders on the following questions:

Q.42: Whether TSPs/ISPs should be mandated to interconnect at IXPs that exist in an LSA? Do justify your response.

Q.43: Is there a need for setting up IXP in every state in India? What support Govt. can provide to encourage setting up new IXPs in the states/Tier-2 locations where no IXPs exist presently?

Connectivity and Infrastructure limitations

4.55 Once an IXP is established, ensuring connectivity with Internet Service Providers is the first important step. IXP operators just provide ports on their switches to the respective ISP to form a connection. ISP should bring their own fiber or buy point-to-point links from some telco and reach the exchange. However, the cost of this connectivity up to IXP is at times prohibitive, and most small ISPs are left with no other option but to transit their traffic through bigger ISPs who may interconnect at a location that suits their own traffic rather than the small ISP's. In the bargain, smaller ISPs lose the advantage of control over their network design and also on reduction in latency. Further, the major internet service providers (ISPs), with selective policy, try to increase the cost of transit traffic of smaller ISPs. For a well-functioning IXP local IP transport capacity must be available for a reasonable price to allow stakeholders to connect to the exchange.

In view of the above discussions stakeholders are requested to provide their response to the following questions:

Q.44: Whether leased line costs to connect an existing or new IXP is a barrier for ISPs? If yes, what is the suggested way out? What are other limitations for ISPs to connect to IXPs? What are the suggestions to overcome them?

Autonomous System Numbers (ASN)

4.56 An autonomous system number is necessary for any interconnection between two peered networks at IXPs. ASNs are important because the ASN uniquely identifies each network on the Internet. A unique ASN is allocated to each ISP for use in Border Gateway Protocol (BGP) routing.

4.57 For joining an IXP in India, the member ISP must have its own ASN and use BGP for peering. The peering ISP must be identified at the local Internet registry of Asia Pacific Network Information Centre (APNIC). An IXP does not assign or provide IP addresses, AS Numbers, etc. The Internet Assigned Numbers Authority (IANA) is responsible for assigning ASNs to Regional Internet Registries (RIRs), which are organizations that manage Internet number resources in a particular region of the world. Asia Pacific Network Information Centre (APNIC) is the RIR, with which Indian ISPs have to make their own arrangements for obtaining an ASN.

4.58 There are two options to obtain AS number from APNIC: As a non-member of APNIC or as a member of APNIC. An ISP, who is a non-member of APNIC, has to pay AUD 500 (INR 28,027.83) as a one-time sign-up fee and a membership fee per year to obtain AS Number. This does not include allocation of any IP address. An ISP who is a member of APNIC has to pay member fee charges however allocation of AS number is free. The high fee required to obtain the AS number is the main barrier. The present cost structure (as of January 2021) for a new ISP member for obtaining an ASN of APNIC is as follows:

Table 4.4: APNIC cost structure for a new member for obtaining ASN

IPv4	IPv6	ASN	Sign-up fee	Annual fee
/24 (256 addresses)	/48	1	INR 28,027.83	INR 66,145.68
/24 (256 addresses)	/32	1	INR 28,027.83	INR 1,11,774.98
/23 (512 addresses)	/48	1	INR 28,027.83	INR 85,989.38

/23 (512 addresses)	/32	1	INR 28,027.83	INR 1,11,774.98

(Source: apnic.net)

4.59 APNIC charges a very high fee for its membership based on the size of operation of the ISP. The lowest slab of the annual membership fee is AUD 1180 (INR 66,145.68) per year as per present rates. The high cost to obtain AS number, APNIC membership, and leased line to connect to an IXP are the reasons for many ISPs not joining the existing NIXI. Only ISPs who have their own AS number and have substantially high domestic traffic find it economical to connect to an IXP.

4.60 In its earlier Recommendation on "Improvement in the Effectiveness of NIXI (2007)", TRAI suggested an option to overcome the AS number allocation problem is by using private AS numbers from the upstream provider. As discussed above, small ISPs usually depend on larger ISPs for their upstream connectivity to International Internet Gateways. Therefore, these ISPs are expected to take unique private AS numbers from their upstream providers. However, the present status of NIXI and the number of ISPs joining over the years *(refer to Table 4.2)*, is not very encouraging. In view of the above, the Authority seeks the view of stakeholders on the following:

Q.45: Is the high cost of AS number allocation an impediment for small ISPs to connect to IX? If yes, what is the suggested way out?

Incentivizing establishment of more IXPs

4.61 Provision of incentives for encouraging investment to establish IXP can help in the growth of internet exchanges. Some of the incentivizing options for the growth of IXs in India are discussed in this section.

4.61.1 **Fiscal incentives**: To attract start-ups into the emerging domain of IXPs, various schemes can be introduced, including but not limited to tax exemptions, investment benefits, and credit facilities. As the IXPs are usually non-profit entities, financial aid can also assist market growth, especially in small cities. Easy accessibility to bank loans may be made possible at cheaper rates, i.e., with lesser interests

and collaterals. Promoting local investment opportunities via tax benefits, and reduced duties on the operational equipment needed to build IXPs will encourage the new entrants to get involved in the IXP business.

4.61.2 **Focus on priority regions:** As seen in Figure 4.5, IXPs are clustered in few Tier-1 cities where undersea cables and infrastructure is adequately available. The upcoming digital explosion and data localization will surely increase the traffic load in the IXs serving these areas, leading to inefficient traffic management. The priority areas need to be proactively identified considering various scalable factors for infrastructure creation and IXP establishment in such areas needs to be incentivized. The private IXPs would in turn necessitate the expansion of new peers such as Data Centres, CDNs, Content Providers in these areas heading to their overall digital ecosystem development. More incentives for such priority areas can be an option.

4.61.3 **Peering incentives:** Peering at multiple IXPs can increase reliability, help reduce latency and increase overall QoS. Direct peering can also be encouraged with content providers and hosting Data Centres. By giving incentives in terms of peering costs and port charges for interconnection to more than one IXPs, an ISP will be able to competitively expand its connections beyond a single exchange.

4.62 **Data Centre and IXPs coordination:** The synergy between Data Centres and IXPs can promote cost-effective strategies for an IXP establishment. Hosting an IXP in an existing Data Centre facility can substantially reduce the operating expenses associated with leasing space, purchasing power, and hiring staff, etc. Moreover, data hosting Centres already include the facilities that may be considered and used for an IXP establishment.

4.63 **The right ecosystem:** An Internet exchange in an emerging competitive telecommunications market requires technical skill,

participant trust, community engagement, and operational excellence to succeed. There needs to be a willingness to commit long-term budgeted funding, and plans need to be put in place to make the exchange self-sustaining and preferably self-governing. Finally, the Internet-aware subscriber base will attract local or international content companies. Achieving this relies on the availability of supportive aspects in the ecosystem, access to diverse infrastructure, a competitive service-provider market, and a capable workforce. As the majority of the initial IXP expenditure is on the training of staff to establish and maintain the facility, free, or subsidized skill development programs can help in this direction.

In view of the above discussions, stakeholders are requested to provide their response to the following questions:

Q.46: What other policy measures are suggested to encourage investment for establishing more number of IXPs? Any other issue relevant with IXP growth may be mentioned.

CHAPTER 5

DATA ETHICS – PRIVACY, OWNERSHIP, AND SECURITY

5.1 Data is shaping the future of humanity. The production, distribution, and consumption of digital data in the data economy are driving rapid advances in machine learning, artificial intelligence, and automation. Individuals and businesses are using data to reduce search and transaction costs and make informed choices. Rapid digitalization has helped India achieve inclusive growth with improved governance, and also poised it globally as a data-rich country. 'Digital India' is not only transforming India but also helping to achieve the United Nations Sustainable Development Goals Agenda 2030.

5.2 With the digital inclusion and proliferation of digital services, individuals are generating a significant quantum of personal data. Huge quantities of personal data are being handled by data fiduciaries today, which has raised the debate around data ethics. ***Data ethics*** are inter-personal, social, organisational, and national norms that govern how people/data users should conduct and behave in the digital world. It is a paradigm in which digital transformation is immune to the moral biases of those running the transformation. It also implicates not allowing the machines to discriminate and upturn the ethical values in our society. Data ethics work both ways from humans to machines and from machines to humans[88]. There is a possibility that the erstwhile human biases involved in the decision-making process may get transferred to the machines, which is one of the biggest concern areas in data ethics, today.

5.3 The presence of any ethical biases in the data model may lead to fear of risks emerging from reputational loss and operational risks. Data processing entities thus need to derive a robust framework for data ethics. They must ensure that current unbiased ethical practices and

[88] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-digital-ethics-noexp.pdf

policies are also applied to the data ethics framework, to ensure a holistic view of ethics governing their data processing initiatives.

5.4 Data ethics encompasses the moral obligations of gathering, protecting, and using personally identifiable information and how it affects individuals.[89] Appropriate handling of data, ensuring privacy and security are of equal importance. Fast emerging technologies such as 5G, IoT, and AI, etc., are poised to dramatically heighten both connectivity and the endless data wave along with the complexity of data security and privacy protection. Justice Sri Krishna Committee has made the first attempt to domestically legislate on the issue of data protection and laid the groundwork for a robust and responsible data-usage framework.

5.5 Since data is ubiquitous in the world today, the issue of the protection of the personal data of the users is a matter of deep concern for everyone. Collecting, generating, analysing, and disseminating data, both structured and unstructured, have the potential to adversely impact people and society. Therefore, the Authority felt it necessary to examine the issue of privacy and security of data in telecom networks. Since a sizeable portion of data flows through the telecom networks, the Authority has issued recommendations on 'Data Privacy, Security, and Ownership of the Telecom Data to the Government'. These recommendations on the telecom sector are still relevant to the present data economy of the country and would also address the complex issues of data protection and privacy with the 5G rollout in the future and the adoption of emerging technologies in India. The following sections deliberate on the NDCP-2018 provisions on data privacy, the Authority's recommendations on Data Privacy that are still pending with respect to the telecom sector, Draft Personal Data Protection (PDP) Bill 2019, and the Data Protection and Empowerment Framework for the telecom sector.

a. National Digital Communications Policy (NDCP)-2018

89 https://online.hbs.edu/blog/post/data-ethics

5.6 If India's economic, social, and political interests in the emerging data economy are to be effectively secured, its 'digital sovereignty' encompassing the data privacy, choice, and security of its citizens must be a prime consideration while participating in the global digital economy. Accordingly, the 'Secure India Mission' envisaged in the NDCP policy aims at ensuring sovereignty, safety, and security of digital communications with a focus on ensuring individual autonomy and choice, data ownership, privacy, and security, while recognizing data as a crucial economic resource. The following goal is laid down for 2022, under the 'Secure India Mission' – '*Establish a comprehensive data protection regime for digital communications that safeguards the privacy, autonomy, and choice of individuals and facilitates India's effective participation in the global digital economy'.* Further, the strategy emphasized to achieve this objective of 'Establish a strong, flexible and robust Data Protection Regime' has been spelled out as follows:

3.1(b)Addressing issues of data protection and security in the digital communications sector, by:

iv. Ensuring that core data protection and security principles are applied and enforced.

b. Recommendations on "Privacy, Security and Ownership of the Data in the Telecom Sector" dated 16th July 2018

5.7 In the backdrop of possible threats to the data privacy of the telecommunication consumers, the Authority held a consultation process in 2017 on the issue of **'Privacy, Security and ownership of the Data in the Telecom Sector'** and submitted its recommendations[90] to the Government on 16th July 2018.

5.8 Salient points from the Recommendations submitted by the Authority are as follows:

i. Elaborating on the need for and importance of data privacy in the telecom sector, the Recommendations analyzed the telecom

[90] https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

environment whether the existing data protection framework is sufficient or not.

ii. The Recommendations defined 'Personal data'; identified and assessed the adequacy, efficiency of existing data protection measures; and proposed resolutions for issues pertaining to data protection in relation to telecom services.

iii. The Recommendation emphasizes the Rights and Responsibilities of Data Controllers, Mechanism for regulating the Data Controllers as well as Accountability, Enforcement Models, and Enforcement Tools.

iv. The Authority proposed that the data controllers or the processors should be brought under a data protection framework, ensuring consumers' protection against misuse of their personal data.

v. Further, proposed measures to encourage new data-based business consent creation to protect telecom consumers against the misuse of their personal data by the data controllers.

vi. The Authority re-examined the encryption standards, stipulated in the license conditions for the TSPs to ensure data privacy and security of telecom networks. Also, the need to create a data sandbox that can be utilized by regulated companies for the development of newer services was emphasized.

vii. The Recommendations outlines issues related to Cross-Border Flow of Data, Jurisdictional Challenges, and Legitimate Exceptions to Data Protection Requirements.

viii. Several measures required were recommended for user empowerment in the telecom sector and to strengthen the safety and security of telecom infrastructure.

ix. Ensured parity between TSP's and other similar service providers through mechanisms to address the issues related to regulated and unregulated players.

x. Suggested consumer awareness programs be undertaken to spread awareness about data protection and privacy issues and setting up of redressal of telecommunication consumers' grievances relating to data ownership, protection, and privacy by the government.

c. The Personal Data Protection (PDP) Bill, 2019

5.9 Data privacy issues in India have been becoming more prominent over the past few years and are in the need of a strong data protection regime. In July 2017, the Government constituted a committee of experts under the chairmanship of the retired Supreme Court judge Justice B. N. Srikrishna. The committee was entrusted with the responsibility of identifying lapses in the present data protection regulations and for preparing more robust and comprehensive data protection laws.

5.10 This committee submitted its report on 27th July 2018, which also contained a draft data protection law, later codified as the draft Personal Data Protection Bill, 2018 (Draft Bill, 2018). The report has emphasized that the interests of the citizens and the responsibilities of the state have to be protected, but not at the cost of trade and industry. Later, the committee submitted a revised draft bill which is the current 'The Personal Data Protection Bill (PDP), 2019', introduced in Lok Sabha after further deliberations by the MeitY, on 11th December 2019. The Bill seeks to provide for the protection of the personal data of individuals and establishes a Data Protection Authority for the same. India's Personal Data Protection framework is modelled after European Union's (EU's) General Data Protection Regulation (GDPR) and the PDP Bill, 2019, incorporates many elements of the GDPR.

5.11 **Applicability:** The Bill governs the processing of personal data by (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with the personal data of individuals in India. Personal data is data that pertains to characteristics, traits, or attributes of identity, which can be used to identify an individual. The Bill categorizes certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator.

5.12 Below are the key provisions of the PDP, bill 2019:

- **Processing and Collection of Personal Data**: The draft bill has covered the processing of personal data by both public and private entities. The committee recommended that processing (collection, recording, analysis, disclosure, etc.) of personal data should be done only for "clear, specific and lawful" purposes. Only that data that is necessary for such processing is to be collected from anyone. The bill has jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected, or otherwise processed in India. The Bill has proposed that critical personal data of Indian citizens be processed in centres located within the country.
- **Individual Consent:** The committee proposed to make individual consent the Centerpiece of data sharing, awards rights to users, imposes obligations on data fiduciaries (all those entities, including the State, which determine purpose and means of data processing).
- **Data Localization:** Personal data will need to be stored on servers located within India, and transfers outside the country will need to be subject to safeguards. Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as 'critical personal data' by the Government can only be processed in India.

  Personal data collected, used, shared, disclosed, or otherwise processed by companies incorporated under Indian law will be covered in the Bill, irrespective of where it is processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals do not present in India.
- **Data Protection Authority:** The Bill sets up a Data Protection Authority (DPA) which is supposed to (i) protect the interests of data principals, (ii) prevent misuse of personal data, and (iii) ensure

compliance with the safeguards and obligations under the data protection framework by corporations, governments or anyone else processing personal data (known as "data fiduciaries"). The DPA shall perform the following primary functions:

B. monitoring and enforcement
C. legal affairs, policy, and standard-setting
D. research and awareness
E. inquiry, grievance handling, and adjudication

- **Right to be Forgotten:** The committee recommended giving "data principals" (persons whose personal data is being processed) the 'right to be forgotten'. This means they will be able to restrict or prevent any display of their personal data once the purpose of disclosing the data has ended, or when the data principal withdraws consent from the disclosure of their personal data.
- **Obligations of data fiduciary:** A data fiduciary is an entity or an individual who decides the means and purpose of processing personal data. Such processing will be subject to a certain purpose, collection, and storage limitations. For instance, personal data can be processed only for specific, clear, and lawful purposes. Additionally, all data fiduciaries must undertake certain transparency and accountability measures such as (i) implementing security safeguards (such as data encryption and preventing misuse of data), and (ii) instituting grievance redressal mechanisms to address complaints of individuals.
- **Rights of the individual:** The Bill sets out certain rights of the individual (or data principal). These include the right to:
  i. obtain confirmation from the fiduciary on whether their personal data has been processed,
  ii. seek correction of inaccurate, incomplete, or out-of-date personal data,
  iii. have personal data transferred to any other data fiduciary in certain circumstances, and

iv. restrict continuing disclosure of their personal data by a fiduciary if it is no longer necessary or consent is withdrawn.

- **Grounds for processing personal data:** The Bill allows the processing of data by fiduciaries only if consent is provided by the individual. However, in certain circumstances, personal data can be processed without consent. These include: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency.
- **Cross-border data transfer:** Cross-border transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee. Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross-border transfer for such data).
- **Social media intermediaries:** The Bill defines these to include intermediaries which enable online interaction between users and allow for sharing of information. All such intermediaries which have users above a notified threshold, and whose actions can impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.
- **Sharing of non-personal data with the Government:** The Central Government may direct data fiduciaries to provide it with any:
  a. non-personal data and
  b. anonymised personal data (where it is not possible to identify data principal) for better targeting of services.

Issues not explicitly covered in the Data Protection Bill

5.13 Draft Data Protection Bill applies to the processing of personal data by any individual or entity, and comprehensively covers most of the aspects of data ownership, security, and privacy. Whatever has not

been explicitly covered under the proposed Act, there is a possibility of covering that through the provisions of subordinate legislations that have been provided within the proposed Act. Memorandum regarding delegated legislation that has been attached with the draft bill details various powers under Clause 93 and 94 to make rules/regulations. Therefore, it is expected that certain other issues/details that have not been explicitly mentioned in the Data Protection Bill can be covered through subordinate legislation subsequently.

5.14 One such issue is regarding the use of metadata. The Authority in its' recommendations on data ownership, privacy, and security has recommended that

3.1 (d) All entities in the digital ecosystem, which control or process the data, should be restrained from using metadata to identify the individual users.

Metadata here is "data that provides information about other data" or "data about data", in certain cases, metadata can be used by the entities operating in the digital ecosystem itself to identify the individual users, such entities must be restrained from using metadata to identify the users/individuals.

5.15 Similarly, some of the issues on User Empowerment that have been covered for users of the telecom sector in the said recommendations can also be covered through subordinate legislation, like -

3.3 (b) To ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.

3.3 (e) Multilingual, easy to understand, unbiased, short templates of agreements/terms and conditions be made mandatory for all the entities in the digital ecosystem for the benefit of the consumers.

3.3 (f) Data Controllers should be prohibited from using "pre-ticked boxes" to gain users' consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.

3.3 (g) Devices should disclose the terms and conditions of use in advance, before the sale of the device.

3.3 (h) It should be made mandatory for the devices to incorporate provisions so that users can delete such pre-installed applications, which are not part of the basic functionality of the device if he/she so decides. Also, the user should be able to download the certified applications at his/her own will and the devices should in no manner restrict such actions by the users.

5.16 Further, with respect to the Data Privacy and Security of Telecom Networks, the Authority in its said recommendations mentioned that in case of breaches, data thefts, etc., timely sharing of information with the data consumer and various entities in the digital ecosystem is essential to mitigate the losses/breaches and prevent their future occurrences and suggested that a platform for sharing of such real-time information should be created, which would result in creating a safe and secure telecom network.

3.4 (f) A common platform should be created for sharing of information relating to data security breach incidences by all entities in the digital ecosystem, including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem, including all such service providers to be a part of this platform.

5.17 The Data Protection Bill has provided that 'every data fiduciary shall notify the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal', but there is no recommendation regarding the creation of any data breach platform for sharing of information by the entities in the data ecosystem.

5.18 The Authority in its recommendations on data privacy has realized that the notification of general data protection law will take some time and accordingly, it has recommended -

"The existing framework for the protection of the personal information/data of telecom consumers is not sufficient. To protect telecom consumers against the misuse of their personal data by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem,

which control or process their personal data should be brought under a data protection framework.

Till such time a general data protection law is notified by the Government, the existing Rules/License conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem. For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers and Applications."

Data Sharing and Consent Management Framework

5.19 Freedom and fairness should be the two main guiding principles while sharing the personal data of the individuals in a digital ecosystem. Here, freedom refers to enhancing the autonomy of the individuals with regard to their personal data in deciding its processing, which would lead to an ease of flow of personal data. Fairness pertains to developing a regulatory framework where the rights of the individuals with respect to their personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated. In such a framework, the individual must be the "data owner" since he/she is the focal actor in the digital economy. The relationship between the individual and entities with whom the individuals share their personal data is one that is based on a fundamental expectation of trust. Individuals expect that their personal data will be used in a fairly and transparently.

5.20 A workshop was conducted in TRAI on 28th August 2020 to discuss the issue of Telecom Subscriber Empowerment with the stakeholders, including TSPs and ISPs. During the discussion it emerged that while empowering the telecom subscribers to use their data for establishing their creditworthiness or financial standings, it is important to preserve the privacy, security, and ownership of this data. It was felt that the process of data sharing and consent management by TSPs would require comprehensive discussion and the Authority decided to hold a consultation in this matter with the stakeholders.

Policy and Regulatory Initiatives towards data sharing and consent management

- **Government Initiatives**

5.21 The issue of consent has been addressed by the Government to some extent in the past where in the guiding principles for sharing of user data across services after obtaining user consent have been outlined in a key policy document on "Electronic Consent Framework[91]" developed by MeitY.

5.22 Subsequently, RBI on behalf of all the financial sector regulators has issued the master direction known as the "Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016[92]" for all the financial sector participants. It incorporates the concept of the Account aggregator, which after obtaining the consent of the customers electronically, collects the information from providers of information based on the standardized consent artefact and securely transmits the same to users of the information. This direction is for the benefit of financial sector consumers, as it empowers them to use their personal data, in the form of financial transactions history, for availing new services from any other competing service provider.

5.23 The statement of objects and reasons for the PDP bill 2019, inter alia, mentions:

4. The salient features of the Data Protection Bill, 2019, inter alia, are as under— (i) to promote the concepts such as consent framework, purpose limitation, storage limitation and the data minimisation;

Accordingly, the provision for right to data portability has been included in the draft bill.

5.24 Recently, NITI Aayog has come out with a discussion paper on Data Empowerment and Protection Architecture (DEPA) for a secure consent-based data sharing framework to accelerate financial inclusion. DEPA empowers every Indian with control over their data.

91 http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

92 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD46859213614C3046C1BF9B7CF563FF1346.PDF

It democratises access and enables secure portability of trusted data between service providers. It involves the creation of a standardized technology architecture implemented within the right institutional constructs. DEPA's technology architecture is an interoperable, secure, and privacy-preserving framework for data sharing through:

a. A technology standard for a machine-readable Consent Artefact;
b. Open APIs for data sharing; and
c. A standard for Financial information.

d. TRAI's Recommendation on "Privacy, Security and Ownership of the Data in the Telecom Sector"

5.25 The Recommendations proposed consent mechanisms with varying levels of granularity in choices to be provided to the users by the service providers. Such choices are to be explicitly presented to the user before any data is collected. It is also recommended that the users be provided with appropriate notices detailing the practises regarding personal information being collected. Examples of such practises include purpose of collection and its intended use, and whether the personal data which is collected will be shared with a third party. Individual consent may be obtained only after providing the notice.

5.26 It was emphasized that Notice, Choice, and Consent are the most important rights that should be given to the data consumers. Such notices should include disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc. Similarly, Choice and Consent implies that a data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information and take individual consent only after providing notice of its information practices. Consent may be considered to be a powerful means of protecting an individual's information. An individual is best placed to decide the sensitivity of his/her information rather than the Government or any other agency deciding it on his behalf.

5.27 Regarding issues related to consent management and Account Aggregators, the Authority recommended that

I. *"The Right to Choose, Notice, Consent, Data Portability, and Right to be Forgotten should be conferred upon the telecommunication consumers.*

II. *In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.*

III. *For the benefit of telecommunication users', a framework, on the basis of the Electronic Consent Framework developed by MeitY and on lines of the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users.*

The issue of Account Aggregator and Electronic Consent Framework was also deliberated upon in the recommendations as follows:

"Subsequent to the development of the Electronic Consent Framework by MeitY, RBI, on behalf of all the Financial Sector Regulators, has issued the master direction known as the "Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016" for all the Financial Sector participants. It has the concept of the data fiduciary (Account aggregator) that, after obtaining the consent of the customers electronically, collects the information from providers of information based on the standardized consent artifact and securely transmits the same to users of the information. This direction is for the benefit of financial sector consumers, as it empowers them to use their personal data, in the form of financial transactions history, for availing new services from any other competing service provider."

In the same recommendation, the Authority has said that there is a need to develop a consent framework for telecom sector. Once the framework for data privacy and security is approved by the Government, the Authority may work on such framework. Though the Government has not yet approved any framework for data privacy, however the Data Protection

Bill, seeks to provide for data portability and consent framework as mentioned above.

e. Challenges in sharing telecom subscriber data

5.28 In telecom sector, telecom service providers control an individual's data as custodians or fiduciaries. Going to each TSP individually to access or share data becomes a lengthy and tedious exercise. Collecting individual's data directly from TSPs, for instance, is also a cumbersome task – typically involving physical visits to their premises or call Centre engagements, sharing physical documents using browser uploads or USB sticks, or sharing of confidential username and password data with a third party. Moreover, data is stored in different formats and porting specific data as per the requirement from one database to another service provider is not a standardised process. These issues, described here in the context of personal data, also apply to other forms of data such as derived data (e.g., credit scores). Finally, there is a lack of harmonisation around the regulations for data sharing within and across sectors.

5.29 Creating a simple and secure mechanism to share this data with the individuals' consent would empower them to use data to improve their well-being themselves through ease of access to new financial products and services. However, this is only possible if action is taken to ensure ease of data flows between siloed data custodians housing information (e.g., different banks, NBFCs, Government departments, telecom service providers, etc.) with user consent.

5.30 The end user may more often than not be fully aware as well as have lower bargaining powers when compared to the custodians of their data in the digital ecosystem. This asymmetry is exploited on many occasions by the custodians to their advantage. They may use personal data of individuals to improve their services; they may even monetize this data by sharing it with third parties. Users often get plagued with bursts of targeted marketing, social media engineering strategies, etc., not knowing that it was their own data submitted in the past which

has enabled such campaigns. In the absence of necessary data protection framework, the end-user does not have any recourse to deal with the exploitation by the entities in the digital ecosystem. Many times, the user is forced to part with its personal data with very little information about how the data is going to be utilized. He has no facilities to access, view, amend, or delete his submitted data. In case of any data breach, he may not even be informed about it till it gets reported.

Data Empowerment and Protection Architecture (DEPA)

5.31 In August 2020, NITI Aayog released a discussion paper[93] on Data Empowerment and Protection Architecture (DEPA). Based on the consent philosophy codified by the PDP Bill, 2019, the aim is to provide individuals with the practical means to access, share, and use datasets containing their personal information in an accessible and easily understandable manner. This includes purchase data, traffic data, telecommunications data, medical records, financial information, and data derived from various online services.

5.32 The main objective of DEPA is to give users control over how their data is used and to enable seamless accumulation and consumption of personal data while ensuring privacy and security. DEPA offer users access to better financial services. Its main features include:

a. Designing an evolvable and agile framework for good data governance.
b. Empowering people to access their data and share it with third-party institutions seamlessly and securely.
c. Giving free, informed, specific, clear, and revocable consent to users.

5.33 The basic building blocks of the proposed DEPA technology framework consists of:

i. An Electronic Consent Framework[94], with a specification for a consent artefact managed by MeitY.

[93] https://niti.gov.in/node/1299

[94] http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

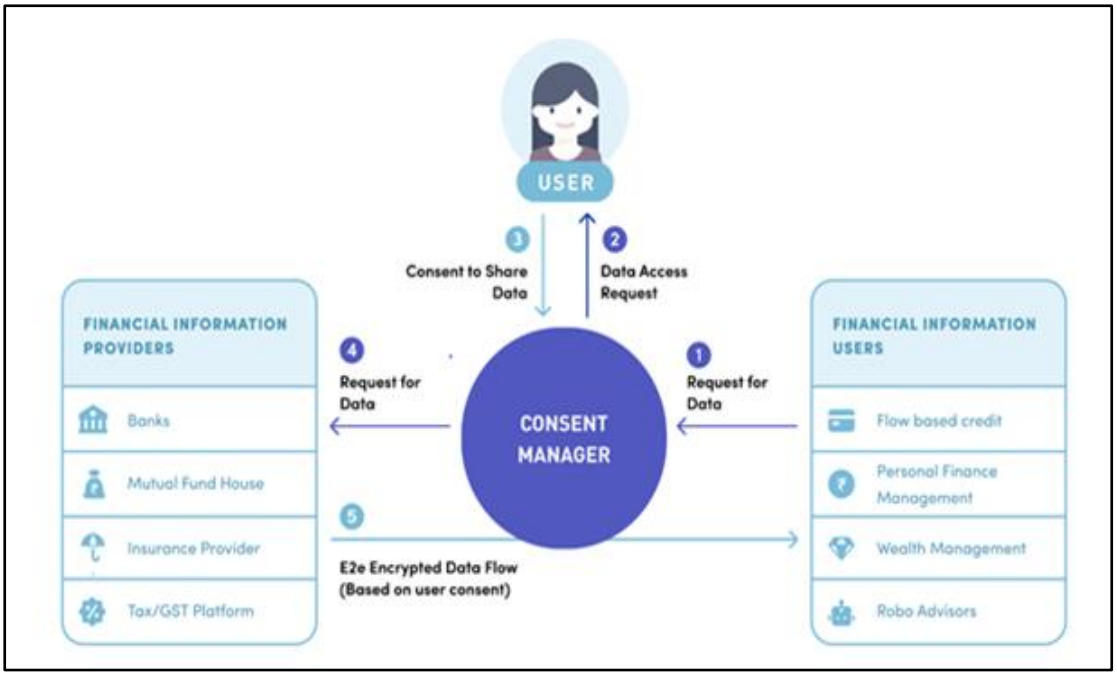
ii. Data Sharing API Standards to enable an encrypted flow of data between data providers and users.

iii. Sector specific Data Information Standard. For the financial sector, this is the Financial Information Standard, which explains the required shared elements of a bank statement across institutions for instance.

5.34 DEPA's Institutional Architecture will involve the creation of new market players known as User Consent Managers. These will ensure that individuals can provide consent as per an innovative digital standard for every data shared. These Consent Managers will also work to protect data rights like the Account Aggregators (AAs) in financial sector as conceptualised in RBI Master Directive, discussed in the previous section. The core principle of AA platforms built on DEPA is to give users complete authority over how their data will be used.

5.35 Under DEPA, the interaction between an individual, a potential data user, and the data fiduciary holding users' information will be mediated through consent managers—organisations maintaining the 'electronic consent dashboard' for users. Consent Managers will be having the responsibility of making sure that individual data is not shared without user consent. Figure 5.1 gives an idea about the flow of consented data in the proposed DEPA institutional architecture.

Figure 5.1: DEPA Architecture



(Source: DEPA discussion paper)

DEPA-based Consent Management Framework for telecom sector

5.36 Telecom data is often the first digital footprint generated by a low-income household, and a steady history of on-time recharges could contribute to building a credit history. Collecting and sharing user data in digital form is a key requirement for ensuring that the interaction between a user and the service provider can be consummated seamlessly in a paperless, fully electronic, and high trust way. Efforts to share digital data about users must overcome the challenge of easy access across various systems in a secure and traceable manner. It is imperative that all user data sharing is fully consented to, in electronic form, by the user(s) whose data is shared. Collecting, managing, auditing, and tracing paper-based consents is costly, inefficient, and also risky. Thus, it is necessary to create a user-friendly technology framework for electronic consent. The guiding principles of such a user-friendly framework are:

1) **User** Centricity: Users should be at the centre of any data sharing and should be given adequate control and decision-making power on how data associated with them is shared.

2) **Trustable and Compliant**: Use of digital signatures to guarantee integrity of access permissions given by users in consent flows. This avoids security issues faced by existing approaches, and also makes the framework fully legal under the DEPA and IT Act.
3) **Universal Identity**: The technical framework should leverage universal, authenticable, non-repudiable, and digital identities to *allow interoperability and usability* across telecom service providers.
4) **Granular Control**: The framework should allow users to set permissions and rights for data access at a granular level.
5) **Open Standards Based**: The framework should use open technology and legal standards available in the country. It should be agnostic to applications, programming languages, and platforms.

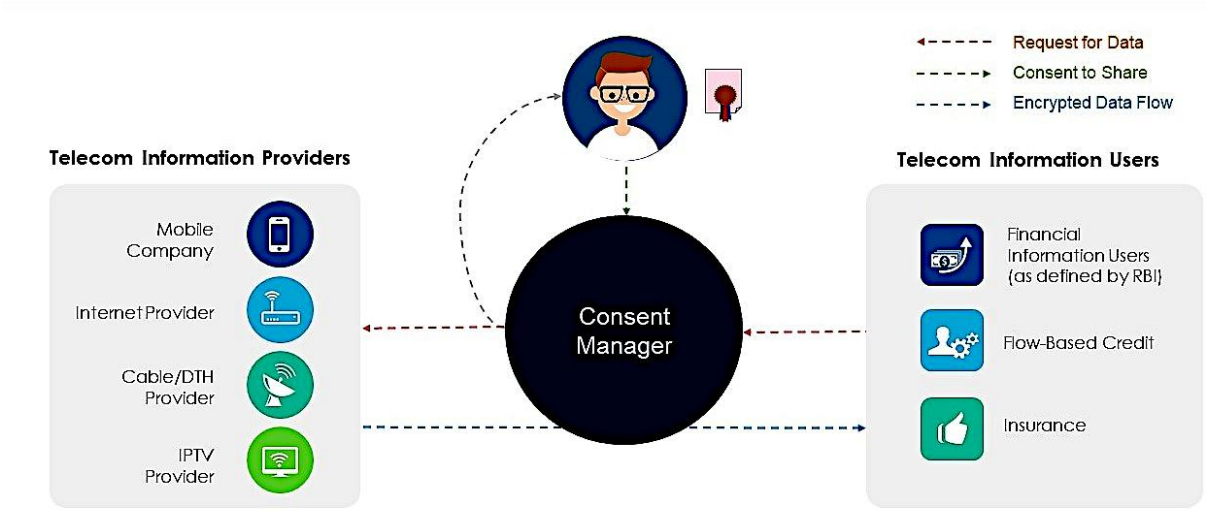
5.37 Consent capture and use process is comprised of two flows - *consent flow* wherein consent is created, and the consent parameters are shared with the relevant entities, and a *data flow*, where the actual data access, based on user consent, happens. In the data flow, the consent artifact is utilized to enable the data consumer to access the data held by the data provider. In consent flow, where the user grants permission for a certain kind of data access between a data consumer and a data provider. The consent flow must necessarily involve an interaction between the consent manager and the user, at the end of which, a consent artifact—an electronic representation of the consent given by the user is generated and shared by the consent manager with either the data consumer or the data provider, depending upon who initiates the data share. This consent artifact is used in the second flow, the dataflow, for the actual data share to happen, sometimes repeatedly. In the case of data shares initiated by the data

consumer, the data provider must verify the signature in the consent artifact before granting access to data. In the case of data shares initiated by the data provider, the data consumer must verify the signature before accepting data. The consent and data flows operate asynchronously in an API-driven manner, which ensures efficiency and resilience. Events at various stages of the consent and data flows are logged and digital signatures are used to ensure security in each of the flows. The separation of the consent and data flows is a key feature of the consent framework. It is important for data flows to be executable asynchronously without the engagement of the user.

5.38 Adopting DEPA in telecom sector and allowing TSPs to become one of the financial information providers may enable subscribers to access their data and share it with third-party institutions. A new type of private consent manager institution can ensure that subscribers can provide consent as per an innovative digital standard for every granular piece of data shared securely. DEPA roll-out has already begun in the financial sector, with a closed user group (CUG) launched by major banks in July 2019, further may be followed by launches in other sectors also. Figure 5.2 depicts the Account Aggregator model[95] which has been in forefront of developing DEPA Consent Framework, that could be implemented for telecom data sharing and consent management framework.

Figure 5.2: Implementation of Consented Sharing of Telecom Data

[95] https://pn.ispirt.in/tag/account-aggregator/



(Source: iSPIRIT developers)

5.39 Connectivity of TSPs as information providers with the data sharing and consent management framework proposed in DEPA via open APIs can provide telecom subscribers with the practical means to access, control, and selectively share their personal data. This sharing of data can be helpful for individual empowerment, while minimising privacy risks and data misuse. By giving people the power to decide how their data can be used, this framework can enable telecom subscribers to control the flow of and benefit from the value of their personal data. Devising an interoperable, secure and privacy preserving framework for consented data sharing of telecom subscribers may empower them with greater control over their data. It is important that such an electronic framework is created for better management of user consent in a paperless system.

Q.47: How can the TSPs empower their subscribers with enhanced control over their data and ensure secure portability of trusted data between TSPs and other institutions? Provide comments along with detailed justification.

Q.48: What is the degree of feasibility of implementing DEPA based consent framework structure amongst TSPs for sharing of KYC data between TSPs based on subscriber's consent?

Q.49: Are there any other issues related to data ethics that require policy/regulatory intervention apart from the issues that have already been dealt with in TRAI's recommendations on the issue of 'Privacy, Security and ownership of the Data in the Telecom Sector' dated 16th July 2018 and the draft PDP Bill ? Provide full details.

Q.50: Stakeholders may also provide comments with detailed justifications on other relevant issues, if any.

CHAPTER 6

ISSUES FOR CONSULTATION

Q.1: What are the growth prospects for Data Centres in India? What are the economic/financial/infrastructure/other challenges being faced for setting up a Data Centre business in the country?

Q.2: What measures are required for accelerating growth of Data Centres in India?

Q.3: How Data Centre operators and global players can be incentivized for attracting potential investments in India?

Q.4: What initiatives, as compared to that of other Asia Pacific countries, are required to be undertaken in India for facilitating ease of doing business (EoDB) and promoting Data Centres?

Q.5: What specific incentive measures should be implemented by the Central and/or the State Governments to expand the Data Centre market to meet the growth demand of Tier-2 and Tier-3 cities and least focused regions? Is there a need of special incentives for establishment of Data Centres and disaster recovery sites in Tier-2 and Tier-3 cities in India? Do justify your answer with detailed comments.

Q.6: Will creation of Data Centre Parks/Data Centre Special Economic Zones provide the necessary ecosystem for promoting setting up of more Data Centres in India? What challenges are anticipated/observed in setting up of new Data Parks/zones? What facilities/additional incentives should be provided at these parks/zones? Do give justification.

Q.7: What should be the draft broad guidelines to be issued for Data Centre buildings, so as to facilitate specialized construction and safety approvals?

Q.8: Is there a need to develop India-specific building standards for construction of Data Centres operating in India? If yes, which body should be entrusted with the task? Do provide detailed justification in this regard.

Q.9: Till India-specific standards are announced, what standards should be followed as an interim measure?

Q.10: Should there be a standard-based certification framework for the Data Centres? If yes, what body should be entrusted with the task?

Q.11: Should incentives to Data Centres be linked to the certification framework?

Q.12: Are there any specific aspects of the disaster recovery standard in respect of Data Centres that needs to be addressed? If so, then provide complete details with justification.

Q.13: Whether trusted source procurement should be mandated for Data Centre equipment? Whether Data Centres should be mandated to have security certifications based on third-party Audits? Which body should be entrusted with the task? Should security certifications be linked to incentives? If so, please give details with justifications.

Q.14: What regulatory or other limitations are the Data Centre companies facing with regards to the availability of captive fiber optic cable connectivity, and how is it impacting the Data Centre deployment in the hinterland? How can the rolling out of captive high-quality fiber networks be incentivized, specifically for providing connectivity to the upcoming Data Centres/data parks? Do justify.

Q.15: What are the necessary measures required for providing alternative fiber access (like dark fiber) to the Data Centre operators? Whether captive use of dark fiber for DCs should be allowed? If so, please justify.

Q.16: What are the challenges faced while accessing international connectivity through cable landing stations? What measures, including incentive provisions, be taken for improving the reliable connectivity to CLS?

Q.17: Is the extant situation of power supply sufficient to meet the present and futuristic requirements for Data Centres in India? What are the major challenges faced by Data Centre Industry in establishment of Data Centres in naturally cooled regions of India? What are the impediments in and suggested non-conventional measures for ensuring continuous availability of power to companies interested in establishing Data Centres in the country? What incentivization policy measures can be offered to meet electricity requirements for Data Centres?

Q.18: Should certification for green Data Centres be introduced in India? What should be the requirement, and which body may look after the work of deciding norms and issuing certificates?

Q.19: Are there any challenges/restrictions imposed by the States/DISCOMs to buy renewable energy? Please elaborate. Please suggest measures to incentivize green Data Centres in India?

Q.20: What supportive mechanisms can be provided to Data Centre backup power generators?

Q.21: Availability of Water is essential for cooling of Data Centres, how the requirement can be met for continuous availability of water to the Data Centres? Are there any alternate solutions? Please elaborate.

Q.22: Whether the existing capacity building framework for vocational or other forms of training sufficient to upskill the young and skilled workforce in India for sustenance of Data Centre operations? What dovetailing measures for academia and industry are suggested to improve the existing capacity building framework, and align it with the emerging technologies to upskill the workforce in India?

Q.23: Is non-uniformity in state policies affecting the pan-India growth and promotion of Data Centre industry? Is there a need for promulgation of a unified Data Centre policy in India, which acts as an overarching framework for setting Data Centres across India? What institutional mechanisms can be put in place to ensure smooth coordination between Centre and States for facilitating DC business? Do support your answers with detailed justification.

Q.24: What practical issues merit consideration under Centre-State coordination to implement measures for pan-India single-window clearance for Data Centres?

Q.25: Is there a need for Data Centre Infrastructure Management System (DCIM) for Data Centres in India? What policy measures can be put in place to incentivize Data Centre players to adopt the futuristic technologies? Elaborate with justification.

Q.26: What institutional mechanism needs to be put in place to ensure digitization of hard document within a defined timeframe?

Q.27: Would there be any security/privacy issues associated with data monetization? What further measures can be taken to boost data monetization in the country?

Q.28: What long term policy measures are required to facilitate growth of CDN industry in India?

Q.29: Whether the absence of regulatory framework for CDNs is affecting the growth of CDN in India and creating a non-level-playing field between CDN players and telecom service providers?

Q.30: If answer to either of the above question is yes, is there a need to regulate the CDN industry? What type of Governance structure should be prescribed? Do elucidate your views with justification.

Q.31: In case a registration/licensing framework is to be prescribed, what should be the terms and conditions for such framework?

Q.32: What are the challenges in terms of cost for growth of CDN? What are the suggestions for offsetting such costs to CDN providers?

Q.33: Do you think CDN growth is impacted due to location constraints? What are the relevant measures required to be taken to mitigate these constraints and facilitate expansion of ecosystem of Digital communication infrastructure and services comprising various stakeholders, including CDN service providers, Data Centre operators, and Interconnect Exchange providers expansion in various Tier-2 cities?

Q.34: What measures can be taken for improving infrastructure for connectivity between CDNs and ISPs, especially those operating on a regional basis?

Q.35: Is there a need to incentivize the CDN industry to redirect private investments into the sector? What incentives are suggested to promote the development of the CDN industry in India?

Q.36: How can TSPs/ISPs be incentivized to provide CDN services? Please elucidate your views.

Q.37: Are there any other issues that are hampering the development of CDN Industry in India? If there are suggestions for the growth of CDNs in India, the same may be brought out with complete details.

Q.38: Do you think that presently there is lack of clear regulatory framework/guidelines for establishing/operating Interconnect Exchanges in India?

Q.39: What policy measures are required to promote setting up of more Internet Exchange Points (IXPs) in India? What measures are suggested to encourage competition in the IXP market?

Q.40: Whether there is a need for separate light-touch licensing framework for operating IXPs in India? If yes, what should be the terms and conditions of suggested framework? Do justify your answer.

Q.41: What business models are suitable for IXPs in India? Please elaborate and provide detailed justifications for your answer.

Q.42: Whether TSPs/ISPs should be mandated to interconnect at IXPs that exist in an LSA? Do justify your response.

Q.43: Is there a need for setting up IXP in every state in India? What support Govt. can provide to encourage setting up new IXPs in the states/Tier-2 locations where no IXPs exist presently?

Q.44: Whether leased line costs to connect an existing or new IXP is a barrier for ISPs? If yes, what is the suggested way out? What are other limitations for ISPs to connect to IXPs? What are the suggestions to overcome them?

Q.45: Is the high cost of AS number allocation an impediment for small ISPs to connect to IX? If yes, what is the suggested way out?

Q.46: What other policy measures are suggested to encourage investment for establishing more number of IXPs? Any other issue relevant with IXP growth may be mentioned.

Q.47: How can the TSPs empower their subscribers with enhanced control over their data and ensure secure portability of trusted data between TSPs and other institutions? Provide comments along with detailed justification.

Q.48: What is the degree of feasibility of implementing DEPA based consent framework structure amongst TSPs for sharing of KYC data between TSPs based on subscriber's consent?

Q.49: Are there any other issues related to data ethics that require policy/regulatory intervention apart from the issues that have already been dealt with, in TRAI's recommendations on the issue of 'Privacy, Security and ownership of the Data in the Telecom Sector' dated 16th July 2018 and the draft PDP Bill? Provide full details.

Q.50: Stakeholders may also provide comments with detailed justifications on other relevant issues, if any.

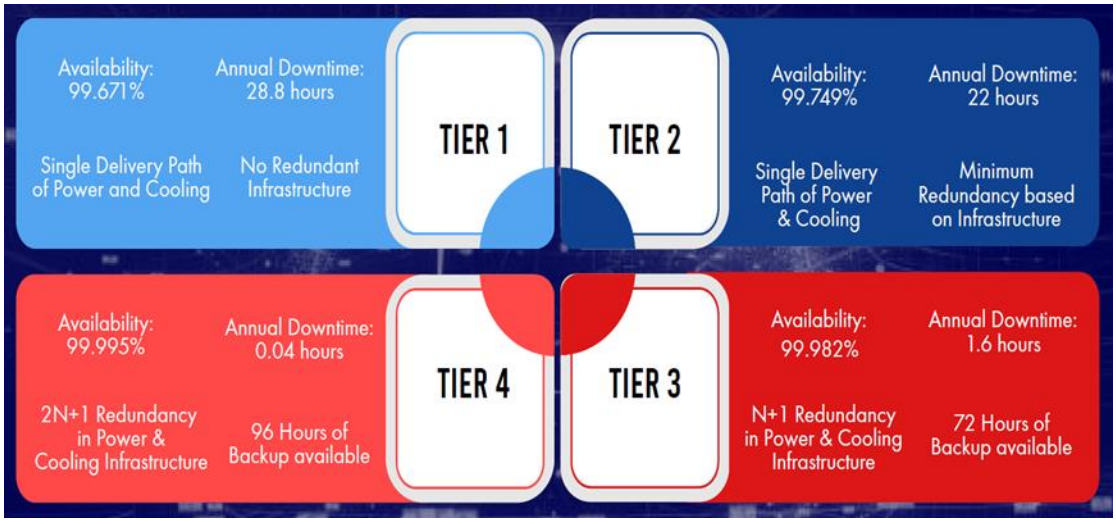
ANNEXURE I (Chapter no. 2/Para no. 2.39)

DATA CENTRE STANDARDS AND CERTIFICATIONS

TIA-942 Tier Classification: The Telecommunications Industry Association (TIA) created the first set of standards for Data Centres in 2005. TIA-942 has been amended twice since then based on the change in technological ecosystem. The Uptime Institute standard was formed separately and differed from the TIA standard because of its specialty in Data Centres, whereas TIA standards could apply to many aspects of the IT industry. To provide uninterrupted services, Data Centres entail redundant IT equipment, electrical power, and cooling equipment. In this regard, Uptime Institute proposed design classification with respect to multi-tier topology to make Data Centres more reliable and fault tolerant.

Data Centre tiers are an indication of the type of Data Centre infrastructure to be considered for a given application. It is a standardized methodology used to define uptime of a Data Centre. A Data Centre tier, or level, in other words, is used for differentiating key Data Centre requirements, the focus being redundant components, cooling, load distribution paths, and other specifications. It is a measure of Data Centre performance, investment, and return on investment. The tier classes (I to IV) characterize the prospects, showing to what extent a system will be functional.

Figure 1: Data Centre tiers



Moreover, the tier classification sets the foundations needed to compare the functionality, capability, and relative cost of the designed topology of a particular Data Centre. The overall evaluation can be performed by determining the least value of the distinct elements, such as power supply, communication, cooling, and monitoring. The table below summarizes configurations of the four-tiered system.

Tier Requirements	TIER I Basic Capacity	TIER II Redundant Capacity	TIER III Concurrently Maintainable	TIER IV Fault Tolerance
Distribution paths (power and cooling)	1	1	1 active/ 1 alternate	2 active
Redundancy active components	N	N	N+1	2(N+1)
Redundancy backbone	×	×	✓	✓
Redundancy horizontal cabling	×	×	×	Optional
Raised floors	12”	18”	30-36”	30-36”
UPS/Generator	Optional	✓	✓	✓
Concurrent maintenance	×	×	✓	✓
Fault tolerant	×	×	×	✓
Annual downtime	28.8 hours	22.0 hours	1.6 hours	0.4 hours
Availability	99.671%	99.749%	99.982%	99.995%

Uptime Institute Tier Certification: The Uptime Institute last revised its certification process in July 2015. The Tier Certification process typically starts with a company deploying new Data Centre capacity. The Data Centre owner decides to achieve a specific Tier level to match a business demand. Data Centre owners turn to Uptime Institute for an unbiased, vendor neutral benchmarking system, to ensure that Data Centre designers, contractors, and service providers are delivering against their requirements and expectations.

Other Standards: Besides the Up Time standard, there are others like EPI-based on TIA-942 (where "tiers 1-4" are replaced by the terms "rated 1-4"), BICSI based standards followed in the USA, whereas countries like Europe, China, and Singapore, etc., have their own standards. The below table shows few international Data Centre standards followed in various countries.

Standard → ↓ Guideline	Up Time [USA]	EPI based on TIA-942 [USA]	BICSI based on TIA-942 [USA]	SS-507 [Singapore]	EN-50600 [Europe]
Conformity	Tier: I - IV	Rated: 1 - 4	Class: 0 - 4	Pass / Fail	Class: 1 - 4
Availability of Standard	Yes	Yes (Paid)	Yes	Yes	Yes
Certification	Available	Available	Not Available	Available	Available
Scope of Topology	Tier Standard Electrical Mechanical Distribution OS Standard Other Element	Electrical Mechanical Distribution Architectural Telecom Site Location Safety- Security Efficiency	Electrical Mechanical Distribution Architectural Telecom Site Location Safety- Security	Electrical Mechanical Distribution Architectural Telecom Site Location Safety- Security	Electrical Mechanical Distribution Architectural Telecom Site Location Safety- Security Efficiency

Incorporation	Commercial	Non-Profit	Non-Profit	Non-Profit	Non-Profit
Accreditation	No	ANSI	ANSI	Spring	EN-CENELEC
Training Event	Yes	Yes	Yes	No	No
Auditor	Up Time Only	Multiple ORG	N/A	Multiple ORG	N/A

ANNEXURE II (Chapter no. 2/Para no. 2.47)

ILLUSTRATIVE LIST OF APPROVAL/CLEARANCES REQUIRED BEFORE COMMENCEMENT OF A DATA CENTRE OPERATION

The approvals required to establish a Data Centre facility may have some variations indifferent states. As an illustration, the clearances required to build a Data Centre in Chennai is provided in the below table.

S.no.	Clearance	Authority	Under single window
Statutory Approvals: Pre-Construction Stage			
1	Environment Clearance	Ministry of Environment, Forest and Climate Change (MoEFCC)	No
2	Consent to Establishment	Metropolitan Development Authority and Central Pollution Control Board (CPCB)	Yes
3	Provisional Fire No Objection Certificate (NOC)	State Fire and Rescue Services/ National Fire Protection Association (NFPA)	Yes
4	Storm Water Permits	State Pollution Control Board	Yes
5	Sewage Discharge Approval		Yes
6	Tree Cutting NOC	Central Pollution Control Board (CPCB): Forest Department	No
7	Drainage/Garden NOC	Metro Water Supply and Sewage Board	Yes

8	Building Permit/ Approvals	Metropolitan Development Authority	Yes
9	Commencement Certificate		Yes
10	Telecom	Service provider/Controller of Communication Accounts of State	No
11	Water Supply	Metro Water Supply and Sewage Board	Yes
12	Power Connection Feasibility, Design and Sanction	State Electricity Board	Yes
13	Traffic Approval NOC	Commissioner of Traffic	No
14	NOC for High-Rise Structure	Airport Authority of India (AAI)	No
Pre-Construction Stage Compliance			
15	Registration with DIC	Director of Industry (DIC)	No
16	Registration IEM	Ministry of Commerce	No
Statutory Approvals: During Construction Stage			
17	220kVPower connection cable laying from substation to project premises	State Electricity Board	Yes
18	220kVPower Connection	State Electricity Board	Yes

	Substation Testing and Charging		
19	Form V Approval - Labour	Labour Department: State Government	Yes
20	Plinth Checking Certificate	Metropolitan Development Authority	Yes
21	Electricity Safety License	Central Electricity Authority (CEA) / Chief Electrical Inspector to Government (CEIG)/ Public Works Department (PWD): Electrical Inspector	No
22	Elevator Permits and Certification: Safety License	Central Electricity Authority (CEA)/Public Works Department (PWD) Electrical Inspector	No
23	Diesel Generator System approval	CEIG/State PCB/PWD-Electrical Inspector	No
24	High Speed Diesel License	Petroleum and Explosives Safety Organization (PESO)/Chief Controller of Explosives Department (CCOE)/PWD: Electrical Inspector	No
Statutory Approvals: Post-Construction Stage			
25	Lift Operating Licenses	Public Welfare Department: State Government: Lift Inspector	Yes
26	Occupancy Certificate	Metropolitan Development Authority: Fire Department	Yes

27	Completion Certificate	Metropolitan Development Authority	Yes
28	Consent to Operate Certification	Central Pollution Control Board (CPCB)	No
Statutory Approvals: Fire and Explosive			
29	Preliminary Explosive License for HSD	Petroleum and Explosives Safety Organization (PESO)/ Chief Controller of Explosives Department (CCOE)	No
30	Final Explosive License for HSD		No

ANNEXURE III (Chapter no. 4/Para no. 4.30)

IXPs: GLOBAL EXPERIENCE

Country	IX Name	Whether license is required to become IXP	Public or Private	Governing Structure	Profit/Not for Profit	Whether allows Bilateral/ Multilateral peering	Whether Peering amongst IXP mandated	What are fees charged? (One time/ Per port/ Traffic dependent etc.)	Whether the tariffs are regulated	Allows peering to what all entities (Only licensed or non-licensed)
Kenya	Kenya Internet Exchange Point (KIXP)	Yes, Kenya is the **first and the only** country in the world to adopt an IXP licence requirement.	Private	KIXP is operated by Telecommunication Service Providers Association of Kenya (TESPOK), a non-profit organization representing the interests of ISPs and other TSPs in Kenya. KIXP is a member of the European IXP association, EURO-IX.	Non-profit	Multilateral peering	No, in 2009 restrictions are removed on peering relationships between participating networks.	Members connecting to the KIXP will be registered as TESPOK members of a special category with a joining fee of Ksh 30,000/- and monthly subscription as per level of traffic as agreed upon by members.	No	Licensed ISPs can connect to KIXP. Also allows peering to international content companies like Google.

South Africa	Johannesburg Internet Exchange (JINX)	No	Private	JINX is operated by Internet Service Providers' Association (ISPA), a non-profit Internet industry body.	Non-profit	Open to any peering. Each organization is free to establish its own policy for interconnection.	No, but each JINX user must negotiate interconnection agreements with the other JINX users.	One-time membership fees exist. There are five categories of ISPA membership, by which access to ports is allowed. Each organization / JINX user is free to establish its own policy for interconnection.	No	Content-server hosting is not available at the JINX exchange.
Hong Kong	Hong Kong Internet Exchange (HKIX)	No	Private	HKIX is owned and operated by the Hong Kong Internet exchange Limited, in collaboration with The Chinese University of Hong Kong.	Non-profit	Each HKIX participant must have its own global internet connectivity through other Internet access provider(s) that are independent of HKIX facilities.	No	There is currently no plan that impose any charges for membership or connection. No port charges, instead the participants provide their own equipment, provided with university's	No	It is an open exchange serving more than just the research and education networks.

								budget. Growth is funded from participants through per-port charges.		
London, United Kingdom	London Internet Exchange (LINX)	No	Private	LINX is a mutually owned membership association for Internet operators.	Neutral, Non-profit	Multilateral peering	No	A LINX member pays the carrier for the transport service and LINX for its standard fees although some carriers may bundle LINX fees.	No	A wide variety of networks peer at LINX and LONAP exchanges, including large content providers such as the Google, Yahoo, and the BBC. The diversity of service providers peering includes gaming and gambling specialists, media streaming providers, DDoS mitigation specialists,
	London Network Access Point (LONAP)	No	Private	As a membership organization, the LONAP exchange is owned by the networks that participate in it.	Neutral, Non-profit	Multilateral peering	No	Membership of the organization is UK GBP2000 per year; this fee provides for two 1Gbit/s connections to the exchange at no further charge. 10Gbit/s Ethernet	No	

								ports are charged at UK GBP2500 per year.		software-as-a-service providers, and advertising networks.
United States	Equinix Internet Exchange (Equinix IX)	No	Private	Equinix is one of the world's largest operators of carrier-neutral Data Centres and Internet Exchanges, the company's IX service allows ISPs and enterprises to exchange Internet traffic through a global peering tool.	Commercial, for profit	Both	No	Not known	No	Equinix IX enables networks, content providers and large enterprises to exchange internet traffic through the largest global peering solution
Singapore	Singapore Internet Exchange (SGIX)	No	Public	SGIX is launched in 2010 as an initiative under the Singapore Government's Intelligent Nation 2015 (iN2015) master plan. Funded by the regulator IMDA (Infocomm Media Development Authority).	Neutral, Non-profit	Not known	Yes	Per port charges are levied.	Yes	SGIX enjoys participation from a full range of brand-name peers, including operators from global and domestic network providers, social

										media, and video streaming companies, as well as cloud infrastructure providers, CDNs, online gaming companies, educational institutions, and research organizations.
Japan	Japan Network Access Point (JPNAP)	No	Private	JPNAP is an open, carrier-owned, for profit, neutral IXP. Nippon Telegraph and Telephone Corporation (NTT) established JPNAP, in partnership with IIJ (the Internet Initiative Japan).	Commercial, for profit	Both, Open Multilateral peering is allowed but also has bilateral connections with selected peers.	No	Per port charges: For 10GbE Port: Initial fee: 100,000 yen. Basic monthly fee: 2,400,000 yen	No	Allows peering to all entities (ISPs, domestic and foreign content providers, CDNs)

Brazil	Internet Exchange Brazil (IX.br)	No	Public	Brazil's IX.br is operated by the CGI.br (Brazilian Internet Steering Committee).	Not-for-profit and almost fully funded by Committee.	Not known	No	No per-port costs for all but the heaviest of users. Peering is free at all the other locations unless your traffic goes above 1 Tbps.	Yes	Allows peering to licensed ISPs.
Republic of South Korea	Korea Internet Neutral Exchange (KINX)	No	Private	KINX was launched in a commercial Data Centre by 13 members of the Korean Internet Association.	Not-for-profit	Bilateral peering	No	Per port charges, "Sending Party Network Pays" regime of interconnect settlements. The Government sets a price ceiling and is reviewed annually.	Yes	Allows peering to licensed ISPs. KINX now has product offerings in transit, cloud, Data Centre colocation, content delivery, and security.

List of Acronyms

S. No.	Acronym	Description
1	5G	5th generation cellular wireless system
2	AA	Account Aggregator
3	AFIX	African Internet Exchange
4	AI	Artificial intelligence
5	AICPASOC	American Institute of Certified Public Accountants, System and Organization Controls
6	AMS-IX	Amsterdam Internet Exchange
7	ANSI	American National Standards Institute
8	APAC	Asia-Pacific
9	APIX	Asia Pacific Internet Exchange
10	APNIC	Asia Pacific Network Information Centre
11	AR	Augmented Reality
12	AS	Autonomous Systems
13	ASN	Autonomous System Numbers
14	AUD	Australian Dollar
15	AWS	Amazon Web Services
16	BBC	British Broadcasting Corporation
17	BEREC	Body of European Regulators for Electronic Communications
18	BFSI	Banking, Financial Services and Insurance
19	BGP	Border Gateway Protocol
20	BICSI	Building Industry Consulting Service International
21	CAGR	Compound Annual Growth Rate
22	CapEx	Capital expenditure
23	CAPs	Content Application Providers
24	CBRE	CB Richard Ellis (real-estate company)
25	CDN	Content Delivery Networks
26	C-DoT	Centre for Development of Telematics
27	CII	Confederation of Indian Industry
28	CLS	Cable Landing Station
29	CP	Consultation Paper
30	CPs	Content Providers
31	CST	Central Sales Tax
32	DC	Data Centres
33	DCIM	Data Centre Infrastructure Management System
34	DCSI	Data Centre Security Index

35	DDoS	Distributed Denial of Service attack
36	DE-CIX	Deutscher Commercial Internet Exchange
37	DEI	Development and Expansion Incentive
38	DEPA	Data Empowerment and Protection Architecture
39	DIP	Digitize India Platform
40	DISCOM	Distribution Company
41	DIT	Dehradun Institute of Technology
42	DLC	Domestic Leased Circuits
43	DoT	Department of Telecommunications
44	DPA	Data Protection Authority
45	DPIIT	Department for promotion of Industry and Internal Trade
46	DR	Disaster Recovery
47	EC	Edge Computing
48	eMBB	Enhanced Mobile Broad-Band
49	EoDB	Ease of Doing Business
50	EPI	Enterprise Products Integration Pte Ltd
51	ESCAP	Economic and Social Commission for Asia and Pacific
52	EUR	Euro
53	FDI	Foreign direct investment
54	FY	Financial year
55	GB	Gigabyte
56	Gbps	Gigabyte per second
57	GDP	Gross Domestic Product
58	GDPR	General Data Protection Regulation
59	GIS	Geographic Information System
60	GPS	Global Positioning System
61	GST	Goods and Services Tax
62	HD	High Definition
63	HIPAA	Health Insurance Portability and Accountability Act
64	HTML	Hypertext Markup Language
65	HTTP	Hypertext Transfer Protocol
66	IaaS	Infrastructure as a Service
67	IANA	Internet Assigned Numbers Authority
68	IBM	International Business Machines Corporation
69	ICP	Internet Content Provider
70	ICT	Information and Communication Technology
71	IDC	Internet Data Centre
72	IEC	International Electronic Commission
73	IEEE	Institute of Electrical and Electronics Engineers
74	IEM	Industrial Entrepreneurs Memorandum

75	IGBC	Indian Green Building Council
76	IIB	International Internet bandwidth
77	IIM	Indian Institutes of Management
78	IIT	Indian Institutes of Technology
79	IMT	International Mobile Telecommunications
80	INR	Indian rupee
81	IoT	Internet of Things
82	IP	Internet Protocol
83	IP-I	Infrastructure Provider Category-I
84	IPR	Intellectual Property Rights
85	IPTV	Internet protocol Television
86	ISMS	Information Security Management System
87	ISO	International Standards Organization
88	ISP	Internet Service Provider
89	ISPAI	Internet Service Providers Association of India
90	IT	Information Technology
91	ITES	Information Technology Enabled Services
92	ITU	International Telecommunication Union
93	IX	Internet Exchange
94	IXP	Internet Exchange Point
95	IXPA	Internet Exchange Point Association
96	IXPN	Internet Exchange Point of Nigeria
97	JINX	Johannesburg Internet Exchange
98	Kbps	Kilobits per second
99	KIXP	Kenya Internet Exchange Point
100	KPMG	Klynveld Peat Marwick Goerdeler
101	kW	Kilowatts
102	LAC-IX	Latin American and Caribbean Internet Exchange
103	LAN	Local Area Network
104	LBT	Local Body Tax
105	LEED	Leadership in Energy and Environmental Design
106	LINX	London Internet Exchange
107	M&E	Media and Entertainment
108	M2M	Machine-to-machine
109	Mbps	Megabytes per Second
110	MeitY	Ministry of Electronics and Information Technology
111	MERC	Maharashtra Electricity Regulatory Commission
112	MIIT	Ministry of Industry and Information Technology
113	mMTC	massive Machine Type Communications
114	MSME	Micro, Small & Medium Enterprises

115	MU	Mega Units
116	MW	Megawatts
117	NCR	National Capital Region
118	NCSC	National Cyber Security Coordinator
119	NDCP	National Digital Communications Policy
120	NFV	Network functions virtualization
121	NGBN	Next Generation Broadband Network
122	NIXI	National Internet Exchange of India
123	NLD	National Long Distance
124	NOC	No Objection Certificate
125	NSWS	National Single Window System
126	OECD	Organisation for Economic Co-operation and Development
127	OFC	Optical Fibre Cable
128	OHSAS	Occupational Health and Safety Assessment Series
129	OpEx	Operating expenditure
130	OTT	Over-the-top
131	P2P	Peer-to-Peer
132	PAIX	Palo Alto Internet exchange
133	PB	Petabytes
134	PCI	Pioneer Certificate Incentive
135	PCI DSS	Payment Card Industry Data Security Standard
136	PoP	Point of Presence
137	QoE	Quality of Experience
138	QoS	Quality of service
139	R&D	Research and Development
140	RAM	Random Access Memory
141	RAN	Radio Access Network
142	RECs	Renewable Energy Certificates
143	RIR	Regional Internet Registries
144	ROI	Return on investment
145	RoW	Right of Way
146	SaaS	Software as a Service
147	SDN	Software-defined networking
148	SEZ	Special Economic Zones
149	SGIX	Singapore Internet Exchange
150	SGSI	Information Security Management System
151	SGST	State Goods and Services Tax
152	SIX	Seattle Internet Exchange
153	SMAC	Social, Mobile, Analytics and Cloud
154	SME	Small and Medium Enterprise

155	TEC	Telecommunication Engineering Centre
156	TIA	Telecommunications Industry Association
157	TRAI	Telecom Regulatory Authority of India
158	TSP	Telecommunications service provider
159	TV	Television
160	UIXP	Uganda Internet Exchange Point
161	URCA	Utilities Regulation and Competition Authority
162	URLLC	Ultra-Reliable Low Latency Communications
163	USD	United States Dollar
164	VAT	Value-added tax
165	VCA	Video Content Analysis
166	vCDN	Virtual Content Delivery Network
167	VNI	Visual Networking Index
168	VoD	Video-on-demand
169	VoIP	Voice over Internet Protocol
170	VR	Virtual reality
171	W	Watt