Regulating Cross Border Data Flows : An Assessment of India’s Data Localisation Framework

Nilay Pratap Singh

A dissertation submitted in partial fulfillment of the requirements for the Degree of Master’s in Public Policy (MPP)

National Law School of India University,
Bengaluru
2021

DECLARATION

I, Nilay Pratap Singh, hereby declare that this dissertation entitled ‘Regulating Cross Border Data Flows : An Assessment of India’s Data Localisation Framework’ is the outcome of my own study undertaken under the guidance of Prof. Srijoni Sen at the National Law School of India University, Bengaluru.

It has not previously formed the basis for the award of any degree, diploma or certificate of this University or any other institute or University. I have duly acknowledged all the sources used by me in the preparation of this dissertation.

29th May 2021 Nilay Pratap Singh

CERTIFICATE

This is to certify that the dissertation entitled ‘Regulating Cross Border Data Flows : An Assessment of India’s Data Localisation Framework’ is the original work done by Nilay Pratap Singh under my guidance and supervision. The results of the research presented in this dissertation have not previously formed the basis for the award of any degree, diploma or certificate of this University or any other institute or University.

29th May 2021

Professor Srijoni Sen
NLSIU, Bengaluru

Abstract

India finds itself at a key juncture in the development of a data governance framework for the data of Indian citizens. The Personal Data Protection Bill 2019 introduced data localisation requirements that mandate certain types of data to be stored and/or processed only within territorial boundaries of India and restricting the flow of data contingent on certain preconditions such as adequate level of protection being met. The framework proposed for India has sparked debates that are polarised and contentions exist on the alignment of data localisation with the objectives it is proposed to achieve. This research conducts an in depth and objective analysis of the complete Data Localisation framework for India. The research first expands the context of data localisation and unpacks the 'why' behind the introduction of the requirements. Next, given that existing studies do not take a comprehensive approach to assessing the framework proposed for India, this research analyses the stated objectives, the background of the issues and the efficacy of data localisation in resolving these. The study then conducts a cost benefit and case study based analysis of the proposed conditional data flow mechanisms that will play a key role in striking the balance between regulating data flows and participating in the global digital economy. The research finds that data localisation by itself is of limited utility in achieving the objectives and also raises security concerns and economic costs. Thus, the research proposes a set of multi dimensional policy recommendations to mitigate the costs arising and plug the gaps that are not addressed by the current framework.

Contents

List of Tables

List of Illustrations

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my academic supervisor, Professor Srijoni Sen for her continued guidance and support throughout the course of the project. The dissertation would not have been complete without her encouragement and expertise in shaping my ideas and thought processes at every stage. I would also like to thank Professor N Jayaram, Professor Sony Pellissery and Professor Rahul Choragudi for their invaluable teachings and feedback that helped me polish my research design and methodology. The Dissertation has also benefited immensely from the teachings of the distinguished faculty of the IPP during the course for which I extend my gratitude to all the professors. I extend my gratitude to the IPP staff for their valuable administration and logistical support.

I'm grateful to Mr Alok Vijayant, IAS and Mr Rahul Sharma, Founder, The Perspective for their valuable insights and continued guidance that have helped me immensely in refining my research.

I would like to make a special mention here of my Father. I fall short on words when I begin to describe the immeasurable role that my dear Father has played in holding my hand through thick and thin and being my guiding light on the darkest of days. He is my pillar of strength and inspiration, my mentor in life and I dedicate this dissertation to him, as I wouldn't have been able to complete it without his blessings. Papa, I am blessed to be your son, I am what I am today just because of you and I love you from the bottom of my heart. Glory with Guts!

1. Introduction

The genesis of the internet was grounded in it being an open network that is agnostic of national borders or physical territorial limits. The design of the internet architecture allowed for the seamless flow of information in a digital format and the creation of a digital footprint from online activities that we now refer to as data. A consequence of this, coupled with the rapid and simultaneous proliferation of globalisation and technology around the world, gave rise to societies and economies that were data driven and developed new means of business, trade, communications and other interdependent networks built on the free cross border data flows. The design of the networks on the internet and the way data traversed the global network also imparted an inherent international character to each data flow that sustained the intricate ecosystem described above.

While the years that followed the exponential growth of the internet and digital economies maintained the status quo of free cross border data flows driving growth, the last two decades of the 21st century have witnessed trends that challenge this status quo. The Internet, which was once a virtual space that existed free from the controls of any one government or any limitations posed on it by an entity, became subject to a tussle that was brewing to govern cyberspace. Different governments posited different objectives and priorities ranging from maintaining its sovereignty and control over its citizens in the virtual world, regulating the activities of the large technology corporations to catching up in the economic realm of benefits that accrued from the digital economy, started constructing data governance frameworks to regulate the extraction, collection, transfer and use of data that was generated by their citizens. (Chander and Le 2014) The governments also exhibited the trend of mandating localised storage of data on domestic servers within the territorial boundaries of the country as a means of regulating the data flows and pursuing their goals of security of data and unskewing the imbalances of the global digital economy amongst many others. These mandates of storing data on local servers of the country and prohibiting its transfer by entities outside the country (either completely or subject to certain conditions that vary across countries) is known as Data Localisation. Several countries have implemented Data Localisation in different formats and degrees. The EU allows for the transfer of personal data only subject to certain preconditions regarding the safety of data being met; Australia has mandated the localised storage of all health related data; China mandates for the localised storage of all data pertaining to its citizens on Chinese servers located within its boundaries and prohibited its transfer outside in the absence of consent and scrutiny from the competent authorities. (Chander and Le 2014; ITIF 2017)

India as a country took its first steps towards crafting a comprehensive data governance framework after the landmark Puttaswamy judgement that drew attention to the right to privacy online and stimulated debates on data protection and means to ensure user privacy of Indian citizens online. The introduction of the Personal Data Protection Bill in 2018 which was then revised and retabled in an updated form in 2019 (PDPB 19) lays down the framework for data protection in India. A key feature of this Bill, along with several policy documents that have been released in the last couple of years such as the RBI notification on local storage of all payment systems data in 2018 and the draft E-commerce policy, include provisions for Data localisation of different types of data pertaining to Indian citizens. While the RBI notification and E-commerce policy mandates are sectoral in nature and scope, the PDPB 19 is applicable to personal data of Indian citizens of two special categories - Sensitive Personal Data (such as financial and health records data) and Critical Personal Data (undefined in the PDPB and to be notified by the Central Government).

The introduction of Data Localisation in India has been subject to several contentious and polarised debates by stakeholders on a range of issues. The proponents of Data Localisation argue in favour of local storage of data for improving the security environment of the data; for enabling economic growth of Indian data driven businesses and the digital economy; for asserting some form of regulatory control over the Big Tech firms and solving the issue of cross border access to data by law enforcement agencies. The report by the Committee of Experts under the Chairmanship of Justice BN Srikrishna also posits its views in favour of data localisation in India. Firms like Phone Pe, Paytm and Reliance have been staunch supporters of the move and argue that the competitiveness of the domestic firms and innovation would increase on account of Indian data being stored within India. (Centre for Internet and Society 2019) On the other side of this debate, independent researchers, technology law and policy experts and industry bodies have raised concerns over the costs that accompany Data Localisation and how any purported benefits to the digital economy will be far outweighed by the costs and other negative consequences that will arise out of market exit of firms and reciprocal measures by other countries. Questions are also raised on the real intent behind mandating localisation, wherein some scholars argue that the move is dominated by the narrative of sovereign control over Indian data that poses a risk of fragmenting the internet architecture known as ‘Balkanisation of the internet’ that is a consequence of the countries walling off their digital economies from the global networks by regulating or cutting off data flows across borders. (Centre for Internet and Society 2019)

In light of these existing contentions and the fact that the PDPB 19 is still under consideration by the Joint Parliamentary Committee, this paper aims to first, expand the scope of the debates by exploring and analysing the larger context of regulating cross border data flows to understand ‘why’ India wants to introduce Data Localisation in the first place. The research then conducts a thematic, objective and in depth analysis of the Data Localisation framework proposed for India and the objectives to be pursued through it to assess the efficacy of the requirements to achieve the stated objectives. The study argues that Data Localisation, in spite of the opposition and lobbying by several stakeholders, is unlikely to be removed from the PDPB 19. Thus, the paper aims to add nuance and context to the existing debate over data localisation in India and provide a set of policy recommendations formulated on the basis of the gaps identified in the current framework which will serve as a reference for the policy makers in their considerations over data localisation for the Indian context.

2. Literature Review

2.1 The Duality of Cross Border Data Flows

The literature review suggests that the ecosystem characterised by cross border data flows, the status quo that is being affected and changed by data localisation exhibits advantages and disadvantages thereby according it a dual character. (GSMA 2018) identifies three key beneficiaries of free cross border data flows - citizens and individuals who get access to a wide range of goods and services and means to interact with people seamlessly; countries that benefit from participating in the global digital economy and markets that also attracts businesses to their local economies along with social and economic benefits of using data in the development sector; Businesses and organisations connect to new consumers and markets, are able to become efficient and deliver new innovative goods and services at lower overall costs. (US Chamber of Commerce 2014) in its report titled "Business without borders : The importance of cross border data transfers for global prosperity" outlines how data flows have enabled a new kind of digital trade of good and digitally delivered services that have overtaken the traditional trade of physical goods and contributed to economic growth and opportunities across the world. A report by McKinsey titled "Digital Globalisation : The new era of digital data flows" corroborates this and estimates that the global digital trade (referred to as global e-commerce marketplace) is valued at USD 8 trillion. (McKinsey 2016) Free cross border data flows don't only benefit data driven enterprises but close to 75% of the value from digitised services and tools also accrue to more traditional businesses. (US Chamber of Commerce 2014) In a report titled "A Roadmap for Cross Border Data Flows" , the World Economic Forum outlines the importance of free flow of data to the development of emerging technologies such as Blockchain, IoT, AI which are poised to revolutionize the economies of today. (World Economic Forum 2019) It is based on this evidence that data localisation requirements are termed protectionist and argued against. However, there are also some key disadvantages that come with free data flows and it is pertinent to note that the disadvantages are faced unequally in the ecosystem.

The report by the Committee of Experts under the chairmanship of Justice BN Srikrishna outlines that free cross border data flows has led to the dominance of select firms in data extraction and use which drives up their profits at the disadvantage of other businesses and economies. (Justice BN Srikrishna 2018) The firms also indulge in anti competitive behaviour in digital markets to consolidate their hold over data which is the key driver for deriving insights, innovating new products and services and growing their businesses. (Jain 2020) Also, the concentration of these firms in a few developed nations leads to benefits of the digital economy being reaped disproportionately at the cost of the others. There is a disconnect between the developing nations providing large markets for user data by virtue of their populations coming online and increased uptake in digitisation, and where the data is located, processed and eventually accrues profits and benefits. (Hicks 2019) The platform economies and apps that are the key markers of growth in digital products and services are also increasingly concentrated in developed nations that lobby in international trade forums to maintain the status quo so as to consolidate their growth. (UNCTAD 2019) Michael Kwet and Nick Couldry argue that the developed nations work in tandem with the Big Tech to perpetuate the structural dependencies and capitalise on the network effects especially in developing nations with large untapped user data potential such as India. (Kwet 2019) The Justice Srikrishna Committee also highlights the issues faced by law enforcement agencies in India in accessing data that flows freely across borders and the conflict of jurisdiction that arises from its seamless flow is an impediment to investigations. Thus, we see that the skewed disadvantages arising from free data flows across borders become a point of contention and are a driver of the agenda that seeks to regulate data flows by mandating data localisation.

2.2 The Sovereignty narrative

Free flow of data across borders has also given rise to the concept of cyber sovereignty which can be seen as the precursor to data sovereignty. With the rapid development and proliferation of the internet, more and more individuals started interacting in cyberspace that was unlike any forum that was available before. Citizens of different countries could connect at the click of a button and indulge in online activities in a space that was (at first) devoid of any laws or regulations. This started posing issues for governments in their exercise of sovereign power and extension of their laws over the citizens and their activities. (Lessig 1995) There have also been instances where the ubiquitous flow of data led to conflict between exercise of sovereign powers between two entities due to the lack of any rules for the resolution of the same. (Couldry and Mejias 2019) Thus, came about the concept of nation states attempting to exert influence over the internet with their laws and rules in order to hold the space and its actors accountable. The concept of data sovereignty originates from cyber sovereignty and is premised on the idea that having control over citizen’s data is integral to asserting sovereignty in cyberspace and becomes the lever for extension of power and pursuing sovereign objectives. In the Indian context, it has been argued that being a sovereign state essentially translates into the right to control the data of its citizens and to regulate the activities and actors that collect, process and use data for varied purposes. (Goenka et al 2019) The narrative accords the status of a national resource and a character of property to data that is supposed to have different dimensions of value that must first be available to the country where it originates. (Kovacs and Ranganathan 2019) This ideology asserts that control over data is necessary and sufficient for pursuing security and economic objectives and hence becomes the second key driver of the policy stance in favour of data localisation.

3. Research Design

3.1 Research Problem

India is at a key juncture in its journey towards crafting a data governance model. The data localisation requirements introduced through the PDPB 19 and a number of other policies signal towards the intent of the government to use data localisation in regulating cross border data flows and pursuing and it thus becomes imperative to assess the framework set up for data localisation in India.

This study aims to fill the existing gap in research by expanding the context of the Data Localisation in India along with conducting an objective and in depth assessment of the complete data localisation framework.

Problem Articulation

The research problem being addressed in the dissertation can further be articulated as follows-

1. The lack of understanding of '**why**' data localisation - There is a gap in the existing knowledge as studies have not explored why the regulations on cross border data flows (such as data localisation) emerge and what have been the key drivers behind the introduction of this policy in India. This is important to set the context before evaluating the data localisation framework.
2. **Limited study on the framework** - Studies on Data localisation have taken a limited view of the complete framework proposed. This can be understood as a two fold problem-
    a. **Conditional Data Flow Regime** -The Indian Localisation framework aims to strike a vital balance between international data flows of Indian data along with regulating them to pursue a set of objectives outlined. It does so by introducing three mechanisms - Standard Contractual Clauses, Binding Corporate Rules and Adequacy Decision Models[1]. There have been no studies on the costs and benefits and issues arising in the practical implementation of the conditional data flow mechanisms proposed.
    b. The studies are also limited due to the lack of uniformity in articulating the policy objectives to be pursued by the Indian framework. This study attempts to take a holistic view of the policy objectives set out by the

[1] Justice BN Srikrishna Committee Report 2019 - Chapter on Transfer of Personal Data outside India.

policy documents and organise them thematically before conducting an in depth assessment of the objectives and analysing the efficacy of data localisation to fulfil the same.

3.2 Research Objectives

Based on the research problem articulated above, the following are the main objectives of undertaking the study-

1. To expand the policy context of Data Localisation in India by gaining an in-depth understanding and insights on the key factors driving the policy stance on regulating cross border data flows by mandating localisation.
2. To define the localisation framework for India and undertake an objective and in depth analysis of the stated objectives and the background issues.
3. To assess the efficacy of Data Localisation in achieving the stated objectives and identify the potential issues arising from the practical implementation.
4. To recommend short to medium term policy measures to fill the gaps and augment the current localisation framework.

3.3 Research Questions

The research is guided by the objectives stated above, seeks to answer the following questions -

1. What are the factors responsible for the change in policy stance towards regulating cross border data flows and mandating data localisation in India?
    a. Research tool used to answer - Qualitative semi structured interviews and literature review.
2. Does localised storage of data reduce vulnerabilities from cyber threats and increase security of data?
    a. Research tool - Qualitative semi structured interviews.
3. Does data localisation enable better access to data for Indian Law Enforcement Agencies?
    a. Research tool - Qualitative semi structured interviews.
4. What are the economic implications of implementing data localisation in India?
    a. **Subsidiary question** - Does data localisation achieve the stated economic objectives of enhancing market competitiveness, innovation and growth in the Indian economy?

  b. Research tool - Qualitative data analysis of secondary sources of data and Qualitative semi structured interviews.

5. What are the costs and benefits of the proposed conditional flow regime?
   a. Research tool- Cost Benefit Analysis and Case Study Analysis.

3.4 Methodology

The research primarily focuses on using qualitative research methods by employing interviews, literature review, content analysis of documents and secondary data analysis in order to derive valid conclusions and answer the research questions formulated.

The qualitative research methods are more suitable for the research since the study aims to gain in depth understanding of the ecosystem of regulating cross border data flows via data localisation along with analysing the opinions and thoughts of the key stakeholders on the emerging issues. This is important to contextualise the research problem and helps in identifying the key issue areas and map possible approaches for a policy that is yet to be implemented.

Data Collection

The research relied on two sources of data collection.

Primary data was collected by conducting qualitative in-depth semi structured interviews with key stakeholders identified. The interviews played a pivotal role in gaining an in-depth understanding of the issues and examination of the topic. Through the interviews, the author was able to benefit from the experiences, perceptions and opinions on the issues of such a large-scale intervention such as data localisation. The interviews were designed in a semi structured format. The key advantage of using this format is that it is flexible and allows for the freedom to explore other areas of interest with follow up questions during the interview. Due to the open-ended nature of the questions, the interviewees also had the flexibility of providing their insights on additional facets of the issue after responding to the pointed question placed before them. This approach led to more nuanced discussions of a wicked and intertwined topic such as data localisation. An interview guide[2] was prepared with a list of generic questions for each area of investigation which were then tailored according to the context and purpose of each interview and the expertise of the interviewee.

The **Secondary** sources of data were -

1. Government policy documents and draft discussion papers
2. Publications by industry bodies such as IAMAI, GSMA, BSA.

[2] Refer to the Appendix.

3. Papers by research organisations and think tanks.
4. Journal articles by independent researchers.
5. Market study reports by consulting firms such as PwC, McKinsey.
6. Reports published by multilateral organisations such as UNCTAD, World Bank, World Economic Forum, OECD and WTO.
7. Press releases on the policies, statements issued by the government and parliamentary debates on the issue of data localisation.
8. Short and long form commentary media articles.
9. Books -
    a. Data Sovereignty : The pursuit for Supremacy (Goenka et al 2019)
    b. Code 2.0 and the other laws of cyberspace - Lawrence Lessig
    c. The costs of connection- Nick Couldry and Ulises Meijas
10. Data and statistics reports by MoSPI, MEiTY (GoI), RBI, Economic Survey of India, Statista.

Analysis

The transcription of the interviews was carried out and then the contents were analysed to identify and categorise the themes and topics emerging from the interviews. The transcripts from different interviews on the same topic of investigation were also compared to bring out patterns and variations in the answers of the respondents which were particularly helpful for adding nuance to the issues that were found to be having contentious claims in the literature. The policy documents, publications and other secondary sources of data were analysed using content analysis to examine the perspectives on the problems under study. In the particular section examining the conditional data flow regime, a cost benefit analysis of the different mechanisms proposed was conducted along with a case study of the EU Adequacy decisions model for outlining the inefficiencies and practical difficulties in implementing these mechanisms. The outcome of these were then used to inform and formulate policy recommendations.

3.5 Scope and Limitations of the Study

The dissertation focuses on analysing the data localisation framework endemic to the Indian context that has been proposed by the Justice BN Srikrishna committee report and provisions made in the PDPB 19. The analysis of the objectives have been carried out keeping in mind the specific localisation requirements mandated in India as opposed to other studies that are based on studying different variations of localisation around the world. The study also does not get into a comparative analysis of localisation requirements of other jurisdictions as several studies have already focused on comparing and contrasting the localisation mandates across different countries. The study does not evaluate the alternatives to data localisation, this is done so being mindful of the trends developing through the recent policy proposals that indicate a definite policy stance on localising data within India and thus evaluating other policy measures will be of little utility in the Indian context. Additionally, the policy recommendations have focussed on short and medium term measures that will fill the gaps and augment the present proposed data localisation framework in India.

3.6 Organisation of the Dissertation

The following sections present the key findings and analysis based on the data collected through primary and secondary sources. The first two chapters expand the policy debate by tracing the key factors responsible for the shift to regulating cross border data flow and mandating data localisation with a focus lens on India. The chapter on ‘Unpacking the Cross Border Data Flows ecosystem’ dives deep into the concept of cross border data flows and the duality exhibited by the global ecosystem. The disadvantages identified therein are the first set of drivers. The second chapter on ‘Data Sovereignty’ explores the concept of being sovereign in cyberspace and outlines the second set of drivers behind data localisation. The third chapter then explains the Data Localisation framework proposed for India along with the core objectives that have been stated to be achieved via data localisation. The chapters that follow present the key findings and are centered on analysing these objectives, the background issues and the efficacy of data localisation in fulfilling the objectives. The chapter ‘An assessment of the conditional data flow regime’ then explores the costs and benefits and practical inefficiencies faced in the implementation of the conditional data flow mechanisms proposed, thus concluding a holistic analysis of all components of the Indian framework. The policy recommendations for each section were consolidated and presented in the last section.

4. Unpacking the Cross Border Data Flows ecosystem

The aim of this chapter is to holistically analyse the modern digital economy that is structured upon and driven by the seamless cross border flows. Doing so will help with an understanding of the ecosystem and the positioning of all stakeholders that will be key to understanding why the need for regulation of data flows was felt and policy measures have been engineered towards such regulation.

Today, economies that were earlier characterised by traditional activities such as manufacturing, production and trade in tangible goods and services have been transformed into digital economies. Although there are several ways of defining such digital economies, a widely accepted and holistic definition is- 'Digital economies are characterised by a broad range of economic activities that are based on digitized information and knowledge, that act as the key inputs and factors of production for the processes'. (Asian Development Bank 2018)

As the world became more digitized with the Internet and the Information Communication technologies, new models and ways of transacting business and commerce emerged. The space was no longer limited to physical interactions between producers, distributors and customers that involved the movement of tangible goods or services and involved a physical exchange of money. All 3 dimensions of transacting business underwent a fundamental transformation. The one that stands out most prominently here is a whole new ecosystem of digital products and services that now developed at breakneck speed- right from financial transactions becoming virtual to access to services such as video conferencing, emails, applications and digital platforms that cater to every need and demand of individuals and businesses. Additionally, the exchange of digital goods and services quickly scaled up to such levels that trade between countries was no longer limited to conventional exchange of goods. The services industry riding on the massive upsurge of digital services started occupying a prominent position in the GDP of countries and trade balance between countries that the world saw the development of 'digital trade'[3] , that would in the coming years outweigh the trade in tangible goods and services in volume in a fraction of the time. With this development and increased interactions online, the digital footprint that was being created, now referred to as data, became the key driver of the ecosystem. These new forms of production, commerce and trade are reliant on the

[3] Trade arising from exchange of goods and services across borders that are enabled by digital enabled transactions and increased digital connectivity. Here the goods and services referred to are not just the ones that are delivered in an online space but also includes the ones in the traditional supply chain that have witnessed a disruption in terms of the scale of transactions, stakeholders and opportunities that have come about with digital tools that shape these conventional chains. (OECD, WEF)

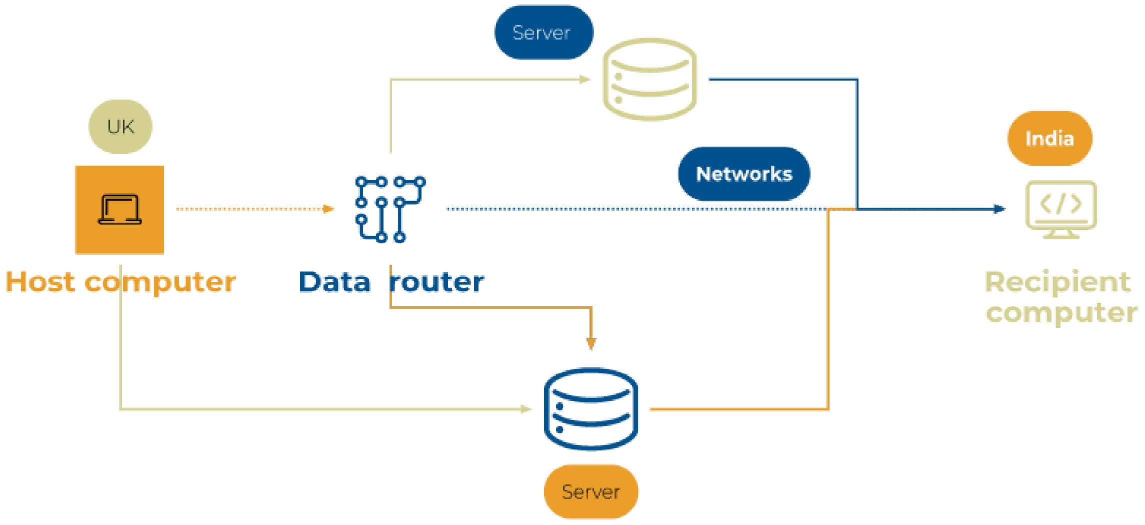
access to and processing and movement of data that is an asset in the value chains that enable growth of such digital services. (Casalini and Gonzalez 2019)

A range of new technologies such as cloud data services, data analytics, Big Data processes, digitised financial services (popularly referred to as fintech) along with improvements in computing power have led to the growth of "information industries" centered on the collection of mammoth amounts of data and creation of value from this information by processes of analysing, processing and deriving insights that aid a range of stakeholders in key decisions and driving growth and innovation. (OECD 2017)

4.1 Technology has invented a borderless flow of data

Another key dimension of this digitised transformation of the economies is the free flow of data across borders that was a consequence of the nature of the internet that was the base on which all digital activities and transformations were developing. Since its inception, the structure and organization of the internet has been elusive of limitations of the physical world such as national boundaries. It was envisioned to be a network and consequently a space that is not guided by the laws and the rules of any countries and facilitates a new dimension of self regulated interactions between people from all over the world just by virtue of them being able to access the network. In essence, the Internet is a "network of networks" made up of connected computers and servers across the globe and is sustained by the ability to transfer data across these networks. (Mandel 2014) Information on one computer is essentially broken down into different packets of data that then traverse through these innumerable networks across the internet on the way to the other computer that sought information.

Figure 1 : Process depicting how data traverses the internet

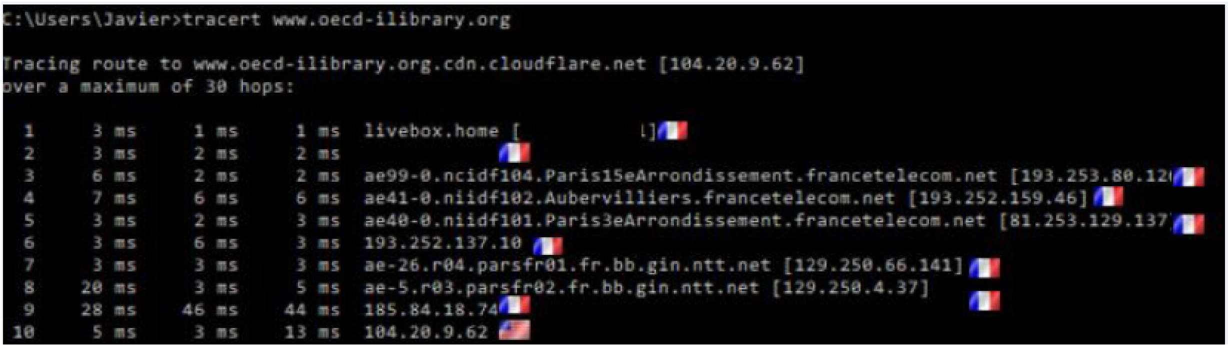


Source : By the author

When the data packets are ready to be sent from the host computer, there are millions of paths that can be taken. By the design of the Internet and using specialised functions of ‘routers’ - the data packets are sent through the least congested (in terms of data traffic by other similar data packets being transmitted) routes that optimises the time in which the whole operation is executed. This is also how the network latency is reduced online and information is available in microseconds at the click of a button, no matter where the data server hosting the relevant data is located. Firms have been found to be using servers located all across the globe to improve speed of access to data and hence the servers are located in across the globe and the data flows between two countries might also involve the data packets traversing a server in a third seemingly unrelated country as well using the principle of least congestion highlighted above. (Casalini and Lopez 2019)

The figures below illustrate the process practically. They outline the networks traversed by the data when a UK based newspaper is accessed from the French jurisdiction. On the face of it, this would appear as a simple cross border transfer between the two countries, but the ubiquitous nature of the data flows are outlined by the fact that Polish and American servers too are involved in this exchange. This again, can be attributed to the principle and design of least congestion.

Figure 2 : Schematic diagram of data path according to OSPF (1)



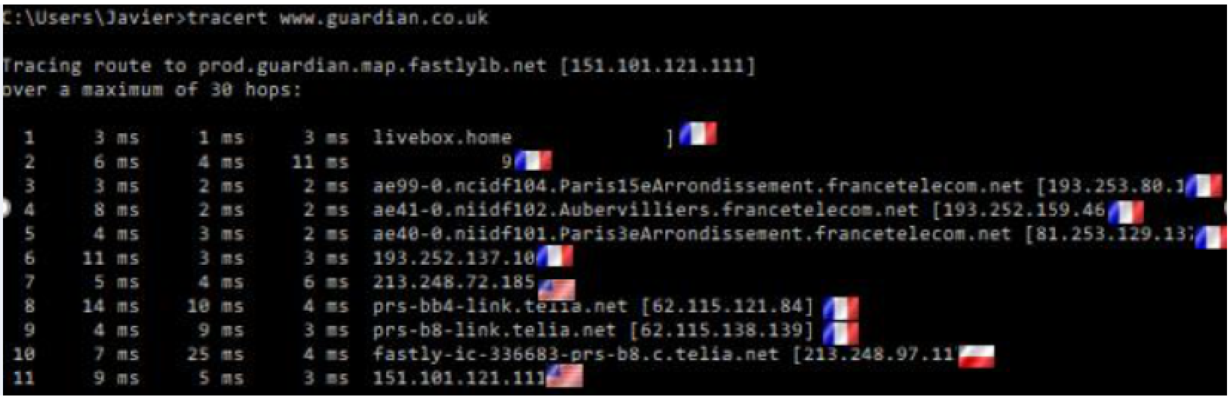
```
:\Users\Javier>tracert www.oecd-ilibrary.org

Tracing route to www.oecd-ilibrary.org.cdn.cloudflare.net [104.20.9.62]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  livebox.home [           l]🇫🇷
  2     3 ms     2 ms     2 ms               🇫🇷
  3     6 ms     2 ms     2 ms  ae99-0.ncidf104.Paris15eArrondissement.francetelecom.net [193.253.80.12🇫🇷
  4     7 ms     6 ms     6 ms  ae41-0.niidf102.Aubervilliers.francetelecom.net [193.252.159.46]🇫🇷
  5     3 ms     2 ms     3 ms  ae40-0.niidf101.Paris3eArrondissement.francetelecom.net [81.253.129.137🇫🇷
  6     3 ms     6 ms     3 ms  193.252.137.10 🇫🇷
  7     3 ms     3 ms     3 ms  ae-26.r04.parsfr01.fr.bb.gin.ntt.net [129.250.66.141]🇫🇷
  8    20 ms     3 ms     5 ms  ae-5.r03.parsfr02.fr.bb.gin.ntt.net [129.250.4.37]
  9    28 ms    46 ms    44 ms  185.84.18.74🇫🇷                            🇫🇷
 10     5 ms     3 ms    13 ms  104.20.9.62 🇺🇸
```

Source : OECD

Figure 3 : Schematic diagram of data path according to OSPF (2)



```
:\Users\Javier>tracert www.guardian.co.uk

racing route to prod.guardian.map.fastlylb.net [151.101.121.111]
ver a maximum of 30 hops:

  1     3 ms     1 ms     3 ms  livebox.home            ]
  2     6 ms     4 ms    11 ms                 9
  3     3 ms     2 ms     2 ms  ae99-0.ncidf104.Paris15eArrondissement.francetelecom.net [193.253.80.1
  4     8 ms     2 ms     2 ms  ae41-0.niidf102.Aubervilliers.francetelecom.net [193.252.159.46
  5     4 ms     3 ms     2 ms  ae40-0.niidf101.Paris3eArrondissement.francetelecom.net [81.253.129.13
  6    11 ms     3 ms     3 ms  193.252.137.10
  7     5 ms     4 ms     6 ms  213.248.72.185
  8    14 ms    10 ms     4 ms  prs-bb4-link.telia.net [62.115.121.84]
  9     4 ms     9 ms     3 ms  prs-b8-link.telia.net [62.115.138.139]
 10     7 ms    25 ms     4 ms  fastly-ic-336683-prs-b8.c.telia.net [213.248.97.11
 11     9 ms     5 ms     3 ms  151.101.121.111
```

Source : OECD

Thus, the movement of data- data flows- inherently gets an international character or what we today refer to as 'Cross Border Data Flows'. In simple terms, CBDF refers to the movement of information in the form of data between servers that are located in different countries/jurisdictions. (BSA Software Alliance 2018) Every activity online today makes use of these flows ranging from accessing a website, sending emails, reading online journals and making credit card payments to name a few.

Having understood the genesis of CBDF, we now pivot our attention to their role in the modern digital economies. The liberalised regime of CBDF has been found to lead to several advantages that accrue to various stakeholders in the ecosystem.

4.2 Benefits arising from free CBDFs

1. The nature of international trade has transformed with businesses and markets now linked digitally and a new mode of direct online interactions have increased opportunities and markets for sale of goods and services. (Meltzer and Lovelock 2018)

2. The growth of Digital trade and commerce, built on CBDFs have also added significantly to the global economy and GDP. Some quantitative studies on measuring the contributions have yielded the following data points :-
    a. A study by the McKinsey Global Institute titled "Digital Globalisation : New era of Data Flows" estimated that between 2005 and 2014 data flows increased by 45 times while traditional mode of trade and finances saw a flatlining decline. Additionally, it was found that global data flows increased the global GDP by 10%. [4]In 2014 alone, close to 2.8 Trillion USD were added to the global

[4] When compared to the increase that was projected in the absence of any data flows.

economy which outsripped the contribution of traditional goods flow in just under 2 decades. (McKinsey 2016)

b. According to a UNCTAD report titled "Digital Economy Report 2019", the digital economy fuelled by CBDFs and digital connectivity has been developing at 6 times the pace of many modern emerging economies. (UNCTAD 2019)

c. Digital services that are enabled by CBDFs have been estimated to add close to 3.2 Trillion USD to the trade in services worldwide. (McKinsey 2011)

d. The value of and contribution to GDP of trade in digital goods and services have increased significantly banking on CBDFs. A study by the All India Management Association found that the benefits of digitally enabled trade in goods and services accrue close to 35 Billion USD worth of benefits with its potential to reach upto 500 Billion USD by 2030, contingent on the stability of free cross border flows of data. (AIMA and Hinrich Foundation 2019)

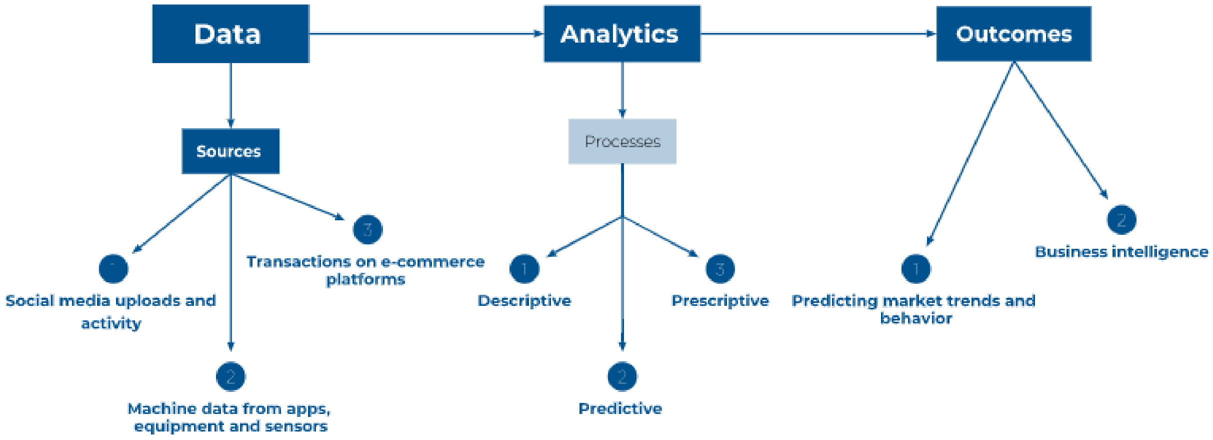
3. Organizations large and multinational in character along with smaller startups and SMEs have benefitted from the new modes of business that CBDFs have brought about.

   a. Several of the technology giants today are one of the most valuable companies in the world and their business models are based on the extraction, processing, analytics based operations on data and the ability to freely move data between locations. The result of which is offering a wide basket of tailor made goods, service and technological solutions to all levels and kinds of stakeholders across the globe.

   b. Organisations today benefit from the free CBDFs by leveraging it to optimise their supply chains operations, manage a global workforce, run analytics and derive insights from diverse sets of data that guides key business decisions in the international marketplace. (Rizvi et al 2019)

The following diagram illustrates the process of how businesses are converting data into actionable insights and intelligence that drives business decisions.

Figure 4 : Process of utilisation of data for insights by digital companies and economies


Data
Analytics
Outcomes
Sources
Processes
1
Social media uploads and activity
2
Machine data from apps, equipment and sensors
3
Transactions on e-commerce platforms
1
Descriptive
2
Predictive
3
Prescriptive
1
Predicting market trends and behavior
2
Business intelligence

Source : By the author

c. Smaller scale startups and SMEs have benefited from the unprecedented access to information and access to new services, research and technologies that have enabled them to establish their presence in global markets. The development of technologies riding on CBDFs have played a pivotal role in increasing the productivity and decreasing costs of operations and inefficiencies for such enterprises. The internet and common digital infrastructure such as cloud based data storage and analytics has also enabled these businesses to reach out to a wide base of customers worldwide directly, unconstrained by physical limitations and market entry barriers. (Meltzer and Lovelock 2018; GSMA 2018) New avenues of access to investments and FDI in digital technologies have opened up that have further acted in reducing market entry barriers.

d. A study by the Boston Consulting Group estimated that small and medium sized enterprises that leverage digital services and products in their business operations witnessed a revenue growth 22% higher than their non digital counterparts. (BCG 2012) In addition to this, the growth due experienced has been found to twice the scale witnessed by businesses operating offline. (US Chamber of Commerce 2014) Given that 90-95% of the businesses in developing and emerging economies such as India fall under the category of MSMEs, it can be seen that CBDFs and their benefits are a key component for the growth of these businesses in particular and the economy as a whole.

4. In addition to digital businesses with data driven business models, traditional businesses and sectors have benefited from cross border data flows as well. A study by the European Centre for International Political Economy highlighted that the ubiquitous

CBDFs affects several conventional sectors such as manufacturers, retailers, education services, financial services that operate offline. For example, a retailer today makes use of Point of Sale machines for card based transactions which make the use of digitised financial services and the free CBDFs that authenticate and facilitate that transaction. (US Chamber of Commerce 2014) Another example would be of UPI payments that have seen a major uptake in the recent years with several digital wallets and financial services being offered via apps and platforms to consumers.

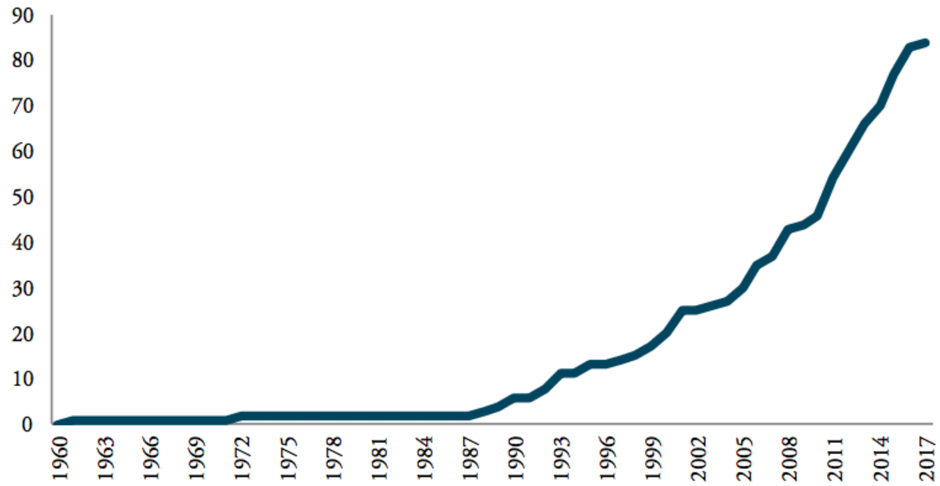
5. Traditional sectors have also made use of digitally enabled services such as softwares for account management, payrolls, keeping track of inventory and recording of sales even though their actual business operations are offline and they are not contributing to the digital economy in the conventional sense.
6. Individuals (as consumers in the digital world) too have access to a wide range of products and services that are delivered using digital platforms from businesses across the world. The services and products can be accessed instantly at the click of a button. This form of digital marketing has been found to increase the choice and satisfaction of the consumer's demands. (GSMA 2018) Data from individual activity is also used to understand the tastes and preferences of consumers which in turn is a valuable input in the product development cycle. Gaining new insights from analysing consumer data in the form of their activities such as (but not limited to) - browsing activity online, spending patterns and content preferences also helps the company in designing and modifying their products and services for the fast moving consumer space online.
7. New technologies, often referred to as technologies of the Fourth Industrial Revolution (Rizvi et al 2019, WEF 2020) have developed based on and adapted the model of the decentralized nature of the internet. These technologies such as Blockchain, Artificial Intelligence, Internet of Things (IoT) and Big Data analytics have been touted as the next big leap in transformation of the global economies and societies. All of them share a common link in the form of being driven by access to vast amounts of diverse sets of data from across different geographies - in other words, liberalised CBDFs. Their growth and the consequent development of knowledge and innovation industries around them has been an outcome of the status quo of free flow of data. These technologies have also carved out a prominent position in all sectors of the economy and industries today. Machine learning algorithms have revolutionized the healthcare and financial industries (amongst many others) by providing cross border collaboration and access to data that has enabled drug and vaccine development, medical diagnosis and the identification of fraudulent transactions and money laundering patterns and practices. (Institute of International Finance 2020)

Thus, we can see that the ecosystem of free Cross Border Data Flows has over the course of its development generated several benefits while driving growth and socio-economic development.

4.3 The curious case of regulating CBDFs

However, a peculiar parallel trend emerging across the globe warrants attention- that of an increase in the laws and regulations restricting free cross border flow of data.

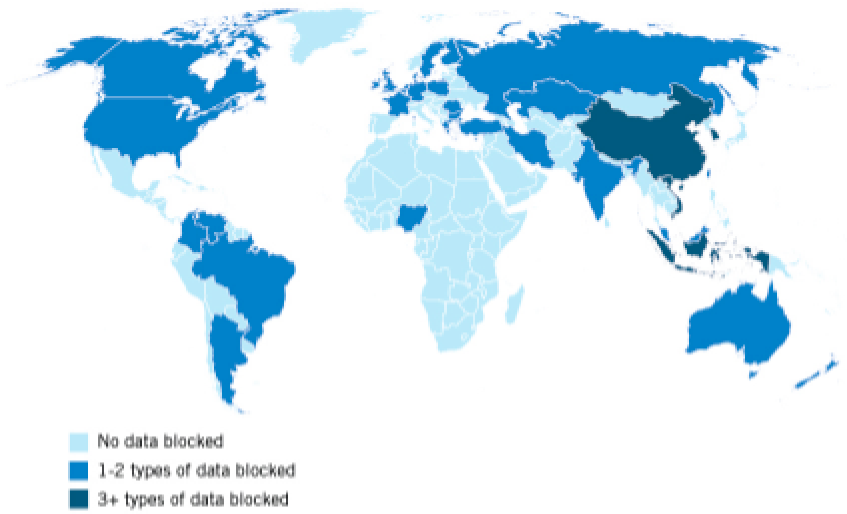
Figure 5 : The total number of restrictions imposed on cross border flow of data between 1960 and 2017 globally



Source : European Centre for International Political Economy

We can observe from the graph that the restrictions are not new in nature but have witnessed a sharp increase since the early 90's which was just when the Internet was taking its roots and the time period which can be attributed to the birth of the liberal CBDF regime that we observe today.

Figure 6 : Graphic representation of countries imposing data flow restrictions[5]



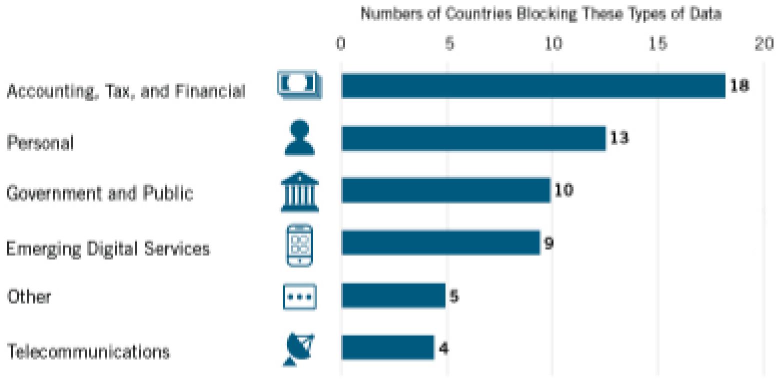
[5] As of 2017.

Source : Information Technology and Innovation Foundation

These restrictions on the free flow of data across borders takes many shapes depending on the type of data that it is applied to, nature of restrictions, degree of restrictiveness imposed, objectives pursued through such regulations. (Meltzer and Lovelock 2018) They can be in the form of conditional flow of data on the basis of some pre-decided criteria being met, local processing and/or local storage of data within the territorial boundaries of the country on its domestic servers. Local storage, processing and access conditions are commonly referred to as data localisation requirements.

In addition to country wide localisation mandates, it has also been applied sectorally (to certain sectors of the economy such as financial services data, health data) or to specific types of data - such as those considered sensitive by virtue of them pertaining of confidential personal information of individuals, Tax and accounting data, telecommunications, pertaining to sensitive government records etc. (ECIPE 2014, ITIF 2017)

Figure 7 : Types of data subjected to cross border data flow restrictions



Source : Information Technology and Innovation Foundation

In the case of India as well, Data localisation requirements have developed over the years through several policies and notifications but have taken a wide scope and definite shape in the form of a framework under the provisions of the Personal Data Protection Bill drafts of 2018 and 2019. And it is this framework that is the subject matter of this dissertation. A more detailed description and analysis of the Indian framework has been presented in the sections that follow.

4.4 Why are such Data Flow restrictive Policies emerging?

Noticing this trend in the rise of data flow restrictions and its evolution in several countries across the globe, it is pertinent to investigate the reasons and the intent that backs such moves and what pushes governments to regulate and restrict the free flow of data across borders and resort to data localisation policies. Through a combination of semi structured qualitative interviews and secondary research, this paper has identified six principle arguments that argue in favour of restricting data flows across borders.

Threats to Security of Data

With an increase in international flow of data, a key concern flagged by experts and policy makers has been the risk posed to the privacy of individuals online. Several incidents of data breach, leaks of personal information of citizens have exposed the vulnerabilities of the data in transit through the ecosystem of data flows. The Cambridge Analytica scandal amongst many other instances have triggered policy debates on the risks posed to and harms arising out of exploitation of personal data that is free to move online. The US PATRIOT Act and the uncovering of the Pegasus spying software snooping on personal communications and data of citizens of other nationalities have also heightened concerns over surveillance by foreign governments that also poses risks to national security of countries. It is argued that access to sensitive financial and government data can be manipulated to cause economic damages and disruption to public order in another country. (Sinha et al 2019)

Given that data privacy laws and frameworks with privacy safeguards are still taking their initial shape in several countries along with the fact that data flows pays no regard to which country's servers it traverses, concerns have been raised on the level of security and protection that citizen's data enjoys in other jurisdictions. For example- If a server in Morocco faces a cyber attack then there is no legal remedy available to citizens of another country whose data was compromised. Additionally, even if a data privacy and protection framework exists in the other country, it might be considered lower or less adequate in accordance with appropriate security safeguards to personal data. This assessment can be attributed to the fact that the notions of 'privacy' and what is considered an adequate level of protection for data are guided by different interpretations, contexts and normative factors such as the cultural definition and view on privacy in that country. (Mattoo and Meltzer 2018) The EU-US data sharing agreement referred to as the EU-US Privacy shield was invalidated by the CJEU[6] on the grounds that the data was susceptible to surveillance by the US government and hence the level of security that EU citizen's data was accorded in the US was lower than what it enjoyed in the jurisdiction of the EU and hence was considered adequate to allow data flows on accounts of preserving privacy of the personal data.

[6] Court of Justice of the European Union - the chief judicial authority of the EU.

Access to data by Law Enforcement Agencies

The nature of crime has also evolved with the increased digitisation of activities. Hackers and cyber criminals now target the personal information of individuals or make use of the internet to carry out their criminal activities. As a result of which Law Enforcement Agencies (LEAs) around the world have been requiring access to data for investigations and prosecution purposes. Often data like emails exchanges between 2 criminals or whatsapp messages blackmailing another person become key pieces of evidence in the investigation of cyber crimes. However, due to the ubiquitous flow of the data across borders, LEAs of one country face an issue in accessing the data. The companies that store this data make use of the global cloud storage which is distributed amongst servers in many jurisdictions and often refuse requests of LEAs citing that the data is stored outside their jurisdiction. LEAs then have to turn to formal legal bilateral or multilateral agreements such as Mutual Legal Assistance Treaties to facilitate their requests. This has been found to be an extremely cumbersome and time taking process. The US-India MLAT process for access to data has been found to be taking an average of 10 months before the data is made available to the LEAs. Such issues of non compliance and extended timelines prove to be detrimental in the investigation of cyber crimes and impairs the functioning of the LEAs.

Conflict of jurisdiction

Further, an issue of assertion of data protection rights and enforcement of data protection laws outside of the country from where data is exported arises with the free cross border flow of data. (OECD 2019) There is a conflict of law question that is centered on “Who’s data protection laws will govern the flow of data and accord its safety principles' '. This question is complex as its determination is guided by several factors such as the origin of the data, residence of the data subject, where the data is currently stored, Where is the company handling the data’s storage incorporated amongst others that have been found to arise in different cases. Thus, even if data protection laws exist, their enforcement faces an issue in the ecosystem of free CBDFs and we observe that a number of regulations that restrict CBDFs are also incorporating clauses extending extraterritoriality to the application of the legislation as an attempt to assert the jurisdiction of the local data protection laws and courts.

Imbalance in the ecosystem

Even though increased digitisation and data value chain have been accruing benefits as has been highlighted earlier, these benefits are shared unequally and are found to be highly skewed towards a few countries and businesses - Large technology companies or the ‘Big Tech’ and a few developed nations. A study by the UN argued that at the most enterprising ends of the value chain - be it collection and processing of market data to derive intelligent business opportunities and insights or RnD has been concentrated in the hands of a few. (UNCTAD 2019) Capitalising on the first mover advantage these technology companies that have originated from and incorporated in a few developed nations were able to rapidly scale their resources and abilities to amass massive amounts of data from other countries which made their data driven business models thrive. A group of Big tech companies - Google, Amazon, Facebook, Alibaba and Microsoft (GAFAM) have been estimated to have a market cap of 3 trillion USD just between them. (Kwet 2019) However, the first mover advantage was soon argued to be developing into 'data monopolies' where practices such as mergers and acquisitions and hostile takeovers of other players in the ecosystem were employed to consolidate and entrench their position more favourable in the ecosystem so as to keep a steadily increasing access to vast amounts of data. This can be visualised as a cycle that access to more data leads to new market opportunities and expanding a wide range of products and services to customers and these offerings in turn increase the scope and reach of data collection from all individuals by pervading all aspects of their lives and interactions online. Data is collected from fitness bands, social media activity, emails and other business suite functionings offered to name a few amongst an innumerable number of sources of data collection for these companies. The extensive proliferation of digital platforms by these companies has benefitted from network effects, economies of scale and infrastructure resources that have added to market domination. (Kwet 2019) These companies have frequently been called out for anti competitive practices and accused of distorting market competition and dynamics that stifle consumer choice while also impairing the domestic markets from scaling innovation and expanding. (IT For Change 2020) Further, it must be noted that by making use of the digital architecture such tech firms are able to expand to new markets without necessarily establishing a significant or any physical presence and hence have been operating from outside the ambit of taxation laws of the domestic economies. This has been seen as a major point of contention as data that is increasingly being viewed as a resource of economic value is extracted and exported by companies without incurring much costs.

Access to data has also enabled a few select companies to rope in investments to scale up their offerings and over time they have become 'critical infrastructure providers' to many in the digital space. Today, economies in Africa or India amongst the developing nations are heavily dependent on key digital services that are provided just by a handful of companies. Software, Hardware and connectivity are provided by large technology companies and where one hand they benefit the local economy in digitising, the companies themselves have been argued to be deriving benefits that are disproportionate when compared to what they offer. Control over the technical ecosystem helps the companies in earning revenue and profits by monetising on the data or by way of charging a rent for using the infrastructure and the intellectual property. (Kwet 2019, Kilic and Avila 2020) For instance Google's proprietary software, corporate cloud infrastructure and centralised internet services have dominated the landscape and made many nations 'structurally dependent on these services for all their digital needs in the public and private spheres'. As a second example, monetisation of data can be understood in terms of the selling of data by these large corporations to producers and other businesses that are then used for targeted advertising and influencing consumer behaviour in other markets. Amazon India has been under scrutiny by the Competition Commission of India for favouring certain brands and retailers and pushing their adverts more prominently to influence consumers on the platform. It has also been argued that the developing economies of the Global south have been providing an enormous market of new users often referred to as the 'Next billion users opportunity' who's data is being extracted and exported without checks and balances. Hence the local economies and societies are suffering economically and in terms of user privacy and rights while acting as a source of raw material (data) for the data value chains.

In addition to data, the 'knowledge capital' such as IP and technologies that develop from the RnD based on data collected from the developing countries has been exported abroad and has been used to earn profits in other countries while downgrading local capabilities and resources to develop technical capacity. (IT For Change 2020)

It is not just the companies but the countries that have gained disproportionately from the ecosystem of free CBDFs. Even though the amount of digitally enabled services and digital trade has been increasing, it has been found that close to just ten countries have been benefiting by having dominance in 90% of the global patents on technology, 70% of the digital services and goods exports and having a sound technical base for key emerging technologies such as AI, Blockchain that are in turn powering their economies forward by developing on data sets extracted from other countries. (UNCTAD 2019) Tying together the points on how a few select firms establish market dominance and how the concentration of these firms in select developed nations today leads to disproportionate benefits for these economies, we look at a few examples in data points.

The dominant firms use their algorithms and access to vast amounts of data by virtue of network effects and infrastructure capabilities to develop the new products and services that majorly manifest in the forms of new apps and platforms which can be seen as both products and channels to offer products and services by these companies. Thus, it can be argued that the market of apps and digital platforms represent the truly global market in digital products and services. Caribou Digital in its 2016 report titled 'Winners and Losers in the Global App Economy' highlights that close to 95% of the value generated by the app economy is captured by just 10 countries. Even if the number of developers in countries like India are comparable to the dominant players, the revenue capture is disproportionately skewed in favour of the top players thus leading to a bolstering of their market dominance and the countries benefiting from the digital markets. (Caribou Digital 2016)

Table 1 : Size of national app markets by total number of downloads

Rank	Google Play Store	Apple App Store
1	United States	United States
2	Brazil	China
3	India	Japan
4	Russia	United kingdom
5	South Korea	Russia
6	Mexico	France
7	Turkey	Canada
8	Indonesia	Germany
9	Germany	Australia
10	Thailand	Italy

Source : Compiled by the author

Table 2 : Top 10 countries by app developer[7] concentration

Rank	Country	Developers
1	United States	1567
2	China	776
3	United Kingdom	456
4	South Korea	395
5	Japan	351
6	Russia	321
7	Germany	307
8	India	289
9	Taiwan	256
10	Spain	239

[7] App Developer here refers to firms engaged in the activity of app development.

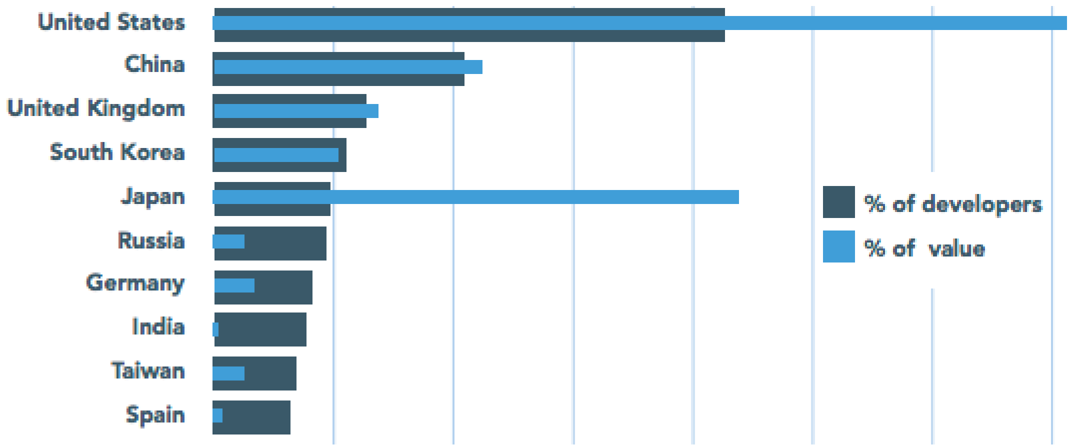
Source : Compiled by the author.

Table 3 : Top 10 countries by market share of revenue from app stores

Rank	Google Play Store	Apple App Store
1	Japan	United States
2	United States	Japan
3	South Korea	China
4	Germany	United Kingdom
5	Taiwan	Australia
6	United Kingdom	Canada
7	France	Germany
8	Hong Kong	France
9	Australia	Russia
10	Russia	Italy

Source : Compiled by the author

Figure 8 : Top 10 countries in the global app economy by developers and share in revenue



Source : Caribou Digital 2016

The digital economy is also driven by the development and proliferation of digital platforms. These digital platforms are the channel to deliver digital products and services and have gained prominence given the fact that the top 7 companies in the world by market cap have data driven and platform oriented business models. (UNCTAD 2019) Within this platform economy, two thirds of the market value and share is dominated by a handful of platforms by the Big Tech dominated by firms from the US and China. This has also led to a geographical concentration with the US accounting for close to 72% of the market capitalization of platforms followed by China at 25% even when going by the number of platforms, these countries fall behind other territories. The US based platform companies also accounted for 80% of the profits generated globally by digital platforms. This highlights the market concentration which is further exacerbated by the fact that these companies have been found to consolidate their market position by anti competitive behaviour, hostile takeovers and expanding their data extraction infrastructure. (UNCTAD 2019)

These trends reflect in the politics that follow economic globalisation as developed countries and these large technology corporations lobby and influence the rules and agreements at the international level that govern data flows. GATS and TRIPS negotiations centered on rights and the governance of data flows at the WTO have been increasingly driven by the narrative of promoting a free and liberal flow of data across borders. The Osaka Track of the G20 along with negotiations of the RCEP and TPP negotiations have exhibited similar skewed trends and advocacy for maintaining liberal flows by deeming restrictive regulations as ‘unnecessarily protectionist’ in nature. This can be seen as an attempt to preserve the status quo so as to secure the economic dominance and geopolitical benefits in the global digital economy.

1.4.5 Safeguarding and boosting the local digital economy

Taking note of the economic imbalances in the ecosystem of free CBDFs, developing countries such as India have posited the idea of data localisation laws as a means to correct these disadvantages faced by the domestic digital economy. A form of digital industrial policy that is premised on the idea that keeping data stored on local servers will enable the domestic firms and economy to capitalise on it and hence drive growth is also driving the agenda of regulating data flows. (Komaitis 2017) In the opinion of the Indian policymakers, localised storage of data will help the digital economy of India by-

1. Attracting FDI in technology.
2. Development of data infrastructure spurred by the demand on account of data being stored with Indian service providers rather than global cloud networks.
3. Creation of employment and a skilled IT workforce that is argued to be a direct consequence of the expanding businesses and technological industries in India.
4. Providing better access to valuable sources of data that will boost productivity of the firms and boost innovation in the country. This is also envisioned to play a pivotal role in providing the domestic businesses with a competitive edge with respect to the global corporations and work towards leveling the playing field with competition.

Thus we see that the concerns discussed above have been a major driving force behind the rise of restrictions on the flow of data across borders in general and of data localisation laws in particular. The Committee of experts headed by Justice BN Srikrishna have also cited these policy red flags while arguing in favour of a data localisation framework and policy for India which manifested in the form of localisation requirements in the Personal Data Protection Bill 2019 of India.

5. Data Sovereignty

There is however another driver of restrictions on cross border data flows such as data localisation laws- that of the emerging concept of Data Sovereignty - an idea that nation states in the modern cyber world should be able to assert sovereign control over what data is collected from their citizens. Who collects and how much of it along with the reasoning that the benefits from data must flow equitably to the source (citizens and countries where they reside) of this data. In this section, we take a finer look at the concept of Data Sovereignty and its evolution in the Indian context which will help holistically establish the intent and the reasons behind the emergence of data localisation in India.

Data Sovereignty is an emerging concept that has come to occupy a prominent position in guiding data governance frameworks, especially in the context of regulating the free cross border flows of data. The concept has many definitions in literature, however the most widely used interpretation can be stated as follows -

Data Sovereignty is the idea that data that ‘originates’ , i.e, is created by the digital activities of citizens of the country should be subject to jurisdiction of the national laws, regulations and privacy safeguards and standards of that country. The state has the right to assert sovereign control over the data, its movement and regulate the activities of and hold accountability over entities involved in the process of data collection, processing and storage.

A striking feature of Data Sovereignty is its geographical/territorial approach that manifests in its assertion that data must be kept within the territorial boundaries of the country for better regulatory oversight and enforcement of domestic laws and safeguards. Essentially, the state has sovereign property rights over the data that is created within its boundaries and has the right to decide and mandate where the data is stored and processed.

5.1 What is Sovereign in cyberspace?

The notion of State sovereignty first originated with the rise of nation states and a new political order with governments elected by the citizens and entrusted with a charter of responsibilities they hold towards the state and its citizens. Sovereignty in its foundational sense refers to the power of the state to control and regulate behaviour- an absolute and independent authority of a state to exercise its control and jurisdiction over subjects and communities within its territory.

In a larger international context the concept of sovereignty has governed the relations between states and found utility in deciding the limits on the exercise and extent of power. (Rizvi 2020) This has been a key factor in maintaining global order and stability over the better part of 2 centuries. However, with the advent of the internet, this very notion of sovereignty was beginning to be challenged. The very architectural construct of the internet as we have noted earlier was opening up new means of communication and interactions between individuals and groups. The foundations of the internet were centered on being a ubiquitous network that is an alternate space free of national boundaries and extending that logic, a space that operates outside of the constraints of the laws and regulations of different sovereigns. It is interesting to note that it was journalists, dissent groups and activists for a range of causes that first capitalised on this freedom of the internet space and thus advocated for its freedom from laws and regulations of the offline world. Such groups could connect with one another without disclosing their identities and free from the fear of surveillance as it was difficult to retrace communication back to specific locations in the early days. Even if it was traced back, only the approximate location or the computer (which could be of a public nature) were identified. The independence of the internet or cyberspace (a larger term referring to the software, physical hardware such as the computers, servers making up the network and the codes that run the network) was echoed by John Perry Barlow as early as in 1996. An excerpt from the declaration is as below, which helps elucidate the elusive nature of the internet and hints towards the issues that sovereign states started confronting in trying to preserve its control and authority over such a ubiquitous new space.

> ‘I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders.’[8]

Adding to this the fact that the internet has lent a duality to the identity of citizens. Besides being a citizen of a country and abiding by the laws stipulated by that sovereign, individuals have been forming a digital identity for themselves through their actions, interactions and transactions online. For instance, a person X might be operating in online chat forums under a vague username beyond which the internet asks for no proof or validation of identity. The internet has also made it harder for sovereigns to enforce their rules and laws on actions and regulate behaviour on the internet. Lawrence Lessig has been one of the foremost authors to delve into the concept of the changing meaning of sovereignty in the digital space. In his book

[8] John Perry Barlow - A Declaration of Independence in Cyberspace https://www.eff.org/cyberspace-independence

"Code 2.0" has elucidated this concept further by giving examples on the ubiquitous nature of activities that the internet enables and what problems it creates for sovereign functioning. Consider a person staying in a state, say State A, where all forms of gambling and betting activities are banned by law. There is another state, State B however where there are no such regulations and businesses based out of the second jurisdiction have started online gambling platforms. The individual from state A uses his computer to access the website for online gambling activities. Now , the issue that the sovereign authority faces here is that of enforcing its laws over the activity. The individual from state A is liable to comply with the anti gambling mandate but only within the territorial boundaries of State A till where the sovereign authority extends. In this case however, though the individual is still within the state limits of State A, the individualis gambling on the platform as part of an online community that is devoid of territorial considerations. The business offering the platform cannot be held liable either since they are incorporated in State B and not in violation of the latter's laws. Thus, the activity in the online space has posed a challenge in determining whether the jurisdiction of the offline space also extends to activities online which are way tougher to place in one particular jurisdiction. (Lessig 1995) Lessig further posits the idea that individuals exist as part of an offline and an online community simultaneously, both with their own sets of norms and rules.

The influence of the online communities are viewed as a direct threat to the sovereign authority of a state as these command an influence on the individuals beyond the online space as well. An example here can be that if an individual is exposed to online discussion forums that are anti-establishment in nature then the person carries these ideas back to the offline world and hence such a phenomenon poses a challenge to the sovereign authority that controls the information and behaviour of the individual in the real world. (Lessig 1995) This also highlights that the notion of the internet was challenging the propensity for governance over citizens by the nation states. (Kovacs and Ranganathan 2019)

5.2 Competing Sovereigns

The problem of sovereign exercise of power is not only limited to state and citizen interactions but also permeates into a competition of sovereign powers between states in the digital world. Individuals today are able to access a wide range of information, literature and expose themselves to different cultures and ideologies by way of the internet. This however has propped up certain issues for the sovereign in cyberspace. A case in point is a sovereign trying to extend its rules over global platforms. Lessig cites the example of the tussle between the French and the American Governments in trying to assert their laws over an internet company Yahoo Inc. The subject matter of the conflict was Yahoo enabling the sales of Nazi paraphernalia on its platform. French law prohibited the sale of any such material while the

American law did not. When French citizens were able to access the platform and the materials, the French government raised objections and argued for Yahoo to remove the ads since they were in contravention of the French Law. The counter argument made by Yahoo Inc (a company incorporated in the US) was that France was overreaching with the assertion of their laws in this instance and were stifling freedom of speech while also being in contravention with American Law and principles. There have been several such examples of different sovereign states finding the global flow of information as being in contravention of their domestic laws and principles while also exposing their citizens to foreign cultural influences that the sovereign would protect their citizens from for ensuring stability and order in the country. The response has thus been a rise in the sentiment for countries to attempt to extend their jurisdiction and sovereign authority over the activities of their citizens on the internet and to assert for their values to be placed on digital activity that permeates their country's borders.

5.3 From Digital Sovereignty to Data Sovereignty

The intent to assert sovereign authority is not limited to just the citizen's activities however, the by-product of their activities - data is also under the ambit of this ideology which then takes the form of 'Data Sovereignty'. As more and more individuals get connected online and participate in the interactions and transactions of the digital world, they are creating valuable sources of data which has a commercial, social and strategic significance as it has the power to influence individuals, communities and entire societies today and thus governments today see control over this data as an enabler to a stronger position for their sovereign authority in the cyberspace which is why we can say that data sovereignty flows from mitigating risks faced by sovereigns in the cyberspace. Elaborating on this further, as exhibited by the previous sections, there are key security concerns that arise from the lack of control of sovereigns over user activity online and the kind of information and services that they access. In addition, as was seen in the competing sovereign sections, the lack of boundaries on the internet has placed uncertainty over the exercise of jurisdiction by the sovereign which also impacts security interests as conflict of laws and lack of access to data for law enforcement purposes are issues that are rooted in the competition between sovereign authorities. Thus the fundamental principle here is that by asserting data sovereignty leading to more control over data, how it is collected, who is allowed to collect it, where it is processed and stored will essentially lead to mitigating the aforementioned risks faced by the sovereign in cyberspace. The sovereign response posits the idea that the terms of data flows cannot be dictated and that the interests of the countries that are providing access to data must be factored in.

In the Indian context in particular, the following factors have added to the development of the narrative on data sovereignty.

Responsibility of the Government to safeguard citizen's data

With the birth of the Indian democracy and the creation of the Indian state, the citizens of the country were uplifted to be the source of sovereignty. A part of the sovereignty was acceded to the government under the premise that the former will be responsible for safeguarding the interests of the citizens and the state as a whole. In the digital world, this has translated into protecting user privacy and there has been a renewed focus on the government's role in ensuring right to data privacy in India after the Puttaswamy Judgement of 2017 which held the right to protection of data as a fundamental right. This was followed by a number of regulations and bills such as the RBI notification and the Personal Data Protection Bill in 2018 and a renewed draft in 201, draft E-commerce policy along with the draft policy on cloud computing. A common link between all these policies is that they are centered on ensuring data privacy of Indian users by mandating localised storage of data on servers within the Indian territory. Thus, the role of the government in protecting user privacy is seen to be fulfilled by asserting control over the data by keeping it inside the territorial boundaries of India.

Changing perceptions and priorities on data

At the core of the ideology and phenomenon of data sovereignty is the change in thinking over the value of data. Earlier data was seen as a natural byproduct of activities conducted online and as something that just exists in cyberspace without much utility. However, as business processes have evolved, data has become a valuable resource for firms and developing new technologies, products and services. Data can be analysed in different ways using tools of analytics which then generates insights that guide business decisions and help in understanding market dynamics. In essence, it is argued that these companies collect data from a huge user base in countries like India without paying any taxes for their activities conducted within India and centered on Indian citizens or incurring costs of investing in local data infrastructure. The firms have been accused of justifying their data collection on the grounds of data being a public good which can be accessed and availed by anyone but then treating it as their private property and deriving disproportionate benefits from it. (Kovacs and Ranganathan 2019)

Thus, governments have argued that it is necessary for them to have sovereign control over data in order to check the data processing activities of foreign firms and derive some monetary benefits from taxing such data collection and processing activities. Data is now being viewed as a national resource and the sovereign control over data is also warranted by the governments to ensure that data is not monopolised in the hands of a few and is available to all stakeholders equitably. (IT for Change 2019) This policy stance has been reflected in India over the last few years in the form of antitrust hearings against the big technology corporations who are accused of data monopolisation, introduction of digital taxes on entities and their activities of data collection from India and most prominently data localisation laws that seek to exert sovereign control over the data and its commercial value while also rebalancing the digital markets and empowering domestic businesses to access data and become more competitive and create value.

(Goenka et al 2019) sheds light on the strategic value that data has attained. As highlighted earlier, data of citizens from one nationality is often targeted through foreign surveillance and is susceptible to data breaches and attacks. This holds serious implications for the national security of a country as exploitation of data can facilitate the manipulation of the citizens, promotion of enmity between religious groups that can lead to communal violence and disruption of public order. In particular, the data generated by government departments, military research and development is of interest to foreign actors and is targeted through cyber attacks on critical infrastructure. Thus, the governments have started a strategic status to different kinds of sensitive data.

Susan Aaranson in her paper, ‘Data is a development issue’ posits that data has the potential to be used to innovate new solutions in the development sector. The increased digitisation of government services and delivery channels has placed data at the centre of the value chain. Modern governments are increasingly shifting to data driven decision making to make more proactive public policies. (Aaranson 2020) A key argument mandating sovereign control over data is to localise the storage of data being extracted and processed by firms and make these data sets available at the request of the government for use in development programs and social good. (IT for Change 2019)

National response to the inefficacy of existing frameworks

Global multilateral frameworks governing digital flows have originated mostly in the form of debates on digital trade and have been found inadequate in addressing the concerns raised or rectifying the imbalances. The deadlock in negotiations, with a select group of developed nations arguing in favour of free and liberal flow of data across borders and others advocating for regulation and restrictions on data flows has degraded the efficiency of such arrangements. A series of competing interests are operating with each country wanting to exert its own notions on how the digital economy must be arranged and how the rules must be formulated in a more consultative, equitable and accountable manner that levels the playing field of data governance. Traditional laws and frameworks too have failed to keep pace with the rapid advancement of technology and business structures with competition policy, taxation and IP policy at the national and international levels no longer finding utility in an ecosystem characterised by stakeholders and practices that were not existing at the time such laws were formulated. Thus, a combination of the concerns flagged by policymakers and inefficiency of existing mechanisms around free flow of data across borders has prompted regional and national level legislations and regulations that by mandating localised storage and restrictions on cross border data flows seek to address the pertinent issues of the ecosystem that has developed. Michael J Morton, the VP of Data Strategy at Dell technologies notes that

> Through the prism of data sovereignty, we can see the wider power of data—and the motivations behind certain geopolitical maneuvers to maintain sovereignty. A nation that controls the data within its borders gains advantages over those that don't (or do so ineffectively). As data becomes ever more valuable, we will see more countries jostle over data sovereignty. (Morton 2020)

The idea of sovereign control over data has been gaining traction in the development of data governance frameworks around the world and a manifestation of this ideology of Data Sovereignty is seen as the introduction of data localisation requirements and laws. Localised storage of data is seen as key to further the data sovereignty agenda as similar to how citizens within the territorial boundaries of India are subject to Indian laws, the localisation move is envisioned to be using the same principle in extending sovereign authority and control over data. Thus, data localisation laws (being a geography based approach to regulating data flows) are observed to follow as a natural consequence of the development of Data Sovereignty.

6. India’s Data Localisation framework

Having analysed the factors behind the rise of restrictions on cross border data flows, we now turn our attention to how these restrictions are manifesting in the Indian context. The restrictions on the free flow of data across borders takes many shapes depending on the type of data that it is applied to, nature of restrictions, degree of restrictiveness imposed, objectives pursued through such regulations. (Meltzer and Lovelock 2018) Listed below are the broad categories under which each of these restrictions can be placed going from the least to the most restrictive.

Table 4 : Types of restrictions on CBDFs

Conditional flow regimes	Based on Accountability on data exporter/ organisations	Consent based	The transfer of data across borders is contingent on obtaining explicit consent from the data subject to whom the data belongs.
		Ad Hoc authorisation	The transfer of data here is reviewed by a designated authority (usually the Data Protection Authority/Regulator) on a case by case basis.
		Standards based	The companies are allowed to transfer data across borders given that they satisfy certain preconditions and standards[9] that have been mandated by the host country. They are often facilitated via Standard Contractual Clauses and Corporate Rules.
Localised storage requirements	Based on geography	Localised storage	This condition requires at least one copy of the data to be stored on a local server within the territory of the implementing country.
		Localised storage + processing	Adding another layer of strictness, in this regime the data must be stored as a copy and ‘main processing’[10] must be done using local digital infrastructure (local data centres) In this case though the local infrastructure has to be used, the data can still be transferred abroad.
		Complete Ban on data exports from the	In this most strict form of data localisation, the data is stored, processed on and accessed only within the territory of the country using the local data infrastructure.

[9] These pre conditions and standards are pertaining to the level and standard of security that is accorded to the data that is being exported and often includes the obligations of the exporting and importing entities in protecting the data from unauthorised access by third entities. These restrictions also impose penalties in case there are data breaches that expose the data or are used for purposes other than what the entities were initially allowed for.

[10] Processing is a blanket term used for all kinds of analytics that are run on data and data sets to derive insights which eventually become the information. It also refers to the management of data such as retrieval, updation, systematisation. (ECIPE 2014)

		implementing territory	

Source :Compiled by the author

Different data governance frameworks and Data Protection laws around the world have used different permutations and combinations of the restrictions mentioned above. The specific types of restrictions and the types of data it is applicable to (listed in the provisions of the PDPB 19) characterise the Data Localisation Framework of India.

However, data localisation requirements are not new in India, several policies and notifications over the years have included local storage requirements for different categories of data applied selectively in different sectors.

Table 5 : Indian data localisation regulations before the PDPB 19

Legislation/Policy	**Data Localisation Requirement**
Public Records Act 1993	Restricts transfer of Public records outside India
IT Act 2000 and IT Rules 2011	Body corporates are not allowed to transfer Sensitive Personal Data if the other entity cannot provide the same level of protection as outlined in the rules.
Unified Access Licenses for the Telecom Service Providers	Subscriber information must be stored and processed locally. Accounting and user information cannot be transferred outside India.
National Data Sharing and Accessibility Policy (NDSAP)	All government data to be stored locally and transfer of data is allowed only for non sensitive data for limited and approved uses.
Companies Act 2013	Books and records of Indian companies in the electronic format must be stored in India.
Guidelines on the Contractual Terms related to Cloud Services for Government Departments and Authorities	Cloud Service Providers empanelled by Government departments must store the data and software shared with them locally.
National Telecom Roadmap	Gateways and Servers servicing customers in India must be physically located in the country.
IRDAI (Outsourcing activities by Indian Insurers) Regulations, 2017	All insurers must ensure the localised storage of original policyholder records.
FDI Policy 2017	Subscriber data must be stored locally and prohibited from transfers outside India. Applicable to all companies receiving FDI.

Draft E-Pharmacy Regulations	E-pharmacies must locally store the data generated or mirrored through their digital portals.
RBI Notification on ‘Storage of Payment Systems Data’ 2018	Payments data of Indians to be stored within India, processing may happen abroad.
Draft Personal Data Protection Bill 2018 (provisions revised in the 2019 draft of the bill)	At least one live copy of all personal data to which the bill applies must be stored locally. Categories of Data notified by the Central Government must be stored and processed in India with no transfers outside allowed.
Draft E-Commerce Policy	Restricts the cross border data flow of data originating from IoT devices in public spaces and data generated by Indian users on e-commerce platforms.

Source : Compiled by the author

The Personal Data Protection Bill 2019 (PDPB 19) on the other hand is the first legislation under consideration that introduces a sector agnostic and unified framework for localising Indian personal data. The types of data that are subjected to the localisation requirements also makes the new proposed framework the most widely applicable data localisation restrictions in India.

6.1 Structure of the Indian Framework

The Indian data localisation framework is made up of three principal components -

A. The provisions in the Personal Data Protection Bill 2019 for **localised storage requirements**

   a. The PDPB 19 relaxes the restrictions of the 2018 draft by reducing the scope of application of the localised storage requirements to 2 categories of data - Sensitive Personal Data and Critical Personal Data.

   b. Sensitive Personal Data - Financial, health, biometric, sexual orientation data of individuals.

   c. Critical Personal Data - Categories designated by the Central Government as such.

   d. Localisation requirements - At least one copy of the Sensitive personal data must be stored on Indian data centres. Critical personal data shall only be stored and processed within India.

B. The **conditional data flow mechanisms** that have been prescribed in the PDPB 19

The bill provides for the conditional transfer of data outside Indian in the following ways.

For the transfer of Sensitive Personal Data

1. The data may be transferred outside India where the explicit consent is given by the data principal for such a transfer and where,
2. The transfer is in accordance with a contractual agreement or intra-group scheme that has been pre-approved and certified by the proposed Data Protection Authority. Further the approval of the contractual agreement and intra group scheme shall be contingent upon them including provisions such as -
    a. Ensuring the effective protection of rights of the data principals that have been outlined in the relevant sections of the PDPB19.
    b. That the data fiduciary involved in the transfer of data to another entity will bear the liability for any non compliance with a provision/ safeguard under the contract/scheme.
3. The third approach is that of adequacy assessments and certifications for other jurisdictions. According to the text of the PDPB19, 'the Central Government after consulting the DPA may allow the free flow of data to another jurisdiction that has been approved' on the basis of its finding that -
    a. The data transferred will be subject to an adequate level of protection, with due regard to the applicable laws and international agreements.
    b. The transfer will not affect the enforceability of relevant laws by the authority with the appropriate jurisdiction.
4. Under section 34, subsection (1) clause (c) - the authority may approve the transfer of sensitive personal data for 'any specific purpose'.

While for **critical personal data** that has been mandated to be processed exclusively within Indian territory, there are certain provisions that allow for its cross border transfer. They are as the followings-

1. The critical personal data may be transferred to any person or entity that is engaged in the provision of health or emergency services.
2. Where such a transfer[11] is necessary for action to fulfill conditions listed under Section 12[12] under chapter 3 that deals with the 'Processing of Personal Data without Consent'.

[11] Any transfer under this clause shall be notified to the DPA within a period specified by the subsequent regulations.

[12] The provisions that allow for non consensual processing under Section 12 have been included in the Appendix.

3. Where the transfer of such data is in accordance with the adequacy determination by the Central government as highlighted above and where such a transfer (in the opinion of the Central Government) does not affect the security and strategic interests of the country .

C. The **objectives to be achieved through the introduction of data localisation in India.**

An analysis of the recommendations of the Justice BN Srikrishna Committee report, White Paper on Cross Border Flows of Data by the MEiTY along with several government documents posit a set of objectives to be achieved through the introduction of data localisation in India. This paper identified and categorised the objectives articulated in 2 broad categories

Table 6 : Thematic categories of data localisation objectives for India

Security and Law Enforcement	● Enhancing National Security by preventing Foreign Surveillance and reliance on fibre optic and physical data infrastructure. ● Better enforcement of local data protection laws ● Ensure faster and better access to data for Indian Law Enforcement Agencies
Economic	● Promoting National Economic growth by enhancing access to data by domestic firms ● Improving competition and rebalancing the digital markets ● Promoting innovation and the creation of an AI ecosystem

Source : Compiled by the author

The sections that follow conduct an in depth analysis of the objectives, the background issues and the utility and efficacy of data localisation in achieving the stated objectives.

7. The Security Paradigm

In the modern cross border data flows ecosystem, the seamless flow of data brings with it concerns of the security of the data along all points of the data value chain right from collection (often termed as extraction), processing, transit and storage. Given the mammoth volume of data pertaining to various aspects of citizens that is exported to other jurisdictions every second, the security of such data is a key concern of both governments and the businesses revolving around both the intellectual property of the information that the data contains and more prominently the overall security of the proprietary data. (World Economic Forum 2020)

With the rapid growth and incorporation of technology in our societies, both the governments and its function as well as many aspects of our daily lives got digitised. Following this digitisation is the footprint that our activities with such technologies generate, the footprint being data. From government land records, financial information, health records, many kinds of personal data became available and with this, the threat to such data from hackers and other governments became more prominent. With the growth in dependence on platforms and apps that track our data, the "attack surface" for cyber attacks has widened greatly. (Nanda 2021) The potential to misappropriate and exploit such data carriers with its grave consequences not only for the citizens it pertains to but also for society, the economy, political systems and the national security of a nation. (Goenka 2019, Cory 2017)

The nature of modern warfare too has evolved to become digital as the damage that can be caused remains high without the opportunity cost of human life and resources that would otherwise go into a physical conflict. Defence and national security officials and organisations too have become dependent on data driven services and platforms for supporting their work and communications. Specialised data sets are created by analysing the performance of drones and weapons, of satellite data and surveillance that informs key decisions in the planning of operations and deployment of manpower. Although in most cases these are intra-organisational networks, the threat of cyber espionage and leakages of confidential data cannot be ruled out. (Aaranson 2020) Nation states today are unanimous in echoing the view that data carrier strategic value to it and since it has the potential to be misused and in some cases weaponised to harm a country's stability and security, the protection or security accorded to such data features prominently in modern doctrines on national security. Additionally, cyber security related concerns in data localisation policies flag threats such as network attacks on domain name systems, attacks on a country's critical infrastructure. In the context of India as well, data breaches and cyber attacks on critical infrastructure such as nuclear power plants (most recently the Kudankulam power plant attack), energy infrastructure, informatics centres and government departments corroborates the strategic value of data since all of such attacks are centered on access to data which can then be used to cause harm across the spectrum of stakeholders. (World Economic Forum 2020) The points till now have shown how direct attacks to access and exploit data undermine the national security objectives of a country. However, there are indirect ways, more gradual in manifesting, that can harm national security in the digital age. An example here would be that of firms such as Facebook that aggregate huge volumes of personal data of individuals but have little to no restrictions or regulation of third party access to it. Further, companies closely linked to foreign governments and having a multinational presence can misuse and take advantage of inadequate data protection or data flow restrictions to further the objectives of their host government against other countries. (Aaranson 2020) The most prominent example here would be that of China and its Tech Giants such as Xiaomi, Tik Tok and Tencent. Which are massive data gathering platforms and apps that monitor user data and can be potentially (or are as they have been accused of) forced to share user data with the Chinese government or security agencies, which can then be used to jeopardize the governments and citizens of other countries. The US has come under fire as well for compelling the Tech giants incorporated in its territory to share user data of individuals from all over the world for security purposes, a move that has been perceived to amass more data of strategic value belonging to other countries and citizens to gain the upper hand in the cyber war domain. Lastly, an interviewee highlighted that not just the singular organisations under attack that face threats, but due to the rapid movement of sensitive information intra and inter businesses the systems and data moving through multiple stakeholders exposes the data supply chain and all connected in this network to a cyber attack.

As part of the narrative of sovereignty in the digital world as well, securing the data of Indians is seen as a pillar of asserting data and hence cyber sovereignty in the global digital economy. This is so as a key tenet of data sovereignty is to assert domestic control over data appropriation and data flows. Several reasons such as protecting the individual’s data from breach and exploitation, safeguarding the consumer’s interests from manipulation in the digital business space, maintaining public order are cited as reasons to regulate the cross border flows of data and also to mandate the localised storage to further the national data sovereignty agenda. (Mitchell 2019)

Thus, one of the key arguments in favour of data localisation has been that the localised storage of data leads to better security being accorded to it. The notion is premised on the belief that storing data on servers within the national boundaries upgrades the security of the data making it less susceptible to attacks and misappropriation. A closer look at data protection legislations around the world and the data localisation frameworks put forth in them, outline the integral role that data localisation has been envisioned to play in ensuring the cybersecurity backing to the safety of data. (Duggal 2019) The Srikrishna Committee report too argues that the localised storage of data is necessary for better security to data by reducing cyber vulnerabilities. The report quotes evidence of surveillance on citizen data by foreign governments and threats arising from the potential sabotaging of the fibre cable infrastructure that are employed extensively to transport data across the globe in its arguments for localised storage, that would play a role towards mitigating such threats. (Justice B.N SriKrishna 2019)

While the threats to the security of data and the evolving nature and intensity of cyber attacks are valid concerns for policymakers and merit attention, the role of data localisation as a policy to mitigate such threats and enhance the security of data has been highly contested. Where on one hand centralised storage via data localisation is argued in favour of keeping the reasons cited above in mind, on the other hand, several experts have flagged the misunderstanding in the position of localisation in achieving the stated objectives of security of data.

Thus, this research focussed on taking a closer and more nuanced look at the utility of data localisation in mitigating security risks to data. **The key research question for this chapter was - "***Does localised storage of data reduce vulnerabilities and improve security provided to data?***"**

The research tool employed was qualitative semi structured interviews with cyber security experts, privacy professionals and technology policy researchers.

7.1 Key findings

One of the primary takeaways from the interviews was that the debate on data localisation and improving security outcomes for data must be viewed from 2 separate perspectives- the first one being the utility of data localisation in national security concerns revolving around data and the second one being protecting the security of data itself.

7.2 National security and Data Localisation

The primary areas where cross border data flows and national security are closely linked is the networks of fibre optics that are the physical assets enabling data flows and exchanges between countries.

Threat from disruptions of cable networks

Another key issue of national security in the context of data is centered on the physical disruptions of the data transmission channels that have the potential to harm the security and economic interests of the country. Underwater sea cables that transmit data have been a particular cause of concern as there's enough evidence of the vulnerabilities of data travelling through such cables ranging from submarine based spying to sabotage of cables that disrupt data flows. The Srikrishna Committee has echoed these concerns and advocated for localised storage of data to reduce the dependence on the physical transmission networks highlighting that the potential costs of disruption can manifest in the form of economic downturn (as stock exchanges can get targeted by such a disruption) and destabilization of public order. (Justice BN Srikrishna Committee 2019) Corroborating this concern an interviewee pointed out that should a trade war or a cyber war erupt between two countries which leads to the other country disrupting the network of data flow with India thereby cutting off our access to Indian data, in this situation having a local copy on servers will add to the resilience against such an event, here data localisation is of significant importance. However, it must be noted that the current data localisation requirements proposed for India do not reduce dependence on the undersea cable networks as copies of Sensitive Personal Data can still be transferred abroad which will inadvertently make use of such cables and the threat would persist.

7.3 Cybersecurity and Data Localisation

Another stated objective of data localisation has been to improve the cybersecurity of Indian data by keeping it on Indian servers and restricting its free flow on servers across the globe. One of the key findings from key informant interviews has been that the geographical location of data storage, by itself, is not a determinant of the security provided to that data. Several experts have highlighted their concern on the territorial approach that is advocated by the localisation framework in India as this represents a myopic view of data security, not taking into account several factors of the cyber security architecture that in reality is the determining factor of security of data. In a report titled "A Roadmap for Cross Border Data Flows" the World Economic Forum has argued that so as long that a country's data infrastructure remains connected to the global internet network, it will be susceptible to cyber attacks and limiting its processing or storage to a particular geography does not necessarily shield the data from such attacks.

But since data localisation (a territorial approach by nature) has been touted to enhance the security of data by storing it on local servers within India, it was pertinent to further investigate the role of the geographical location of data storage and its security. An analysis of the stakeholder responses provided the insight that **the role of geographical location of data in**

determining security boils down to the question of the data being stored in a distributed manner on data centres in a decentralised network or in data centres that are restricted to a particular territory.

The responses reflected that by limiting the storage of data in a centralised format in one jurisdiction as opposed to the distributed storage across several data centres and cloud networks spanning various countries, the data accumulated would represent a “honey pot of data”- which by virtue of its physical concentration in one location can then be easily targeted by cyber attacks and disrupted/destroyed. Further, if data is concentrated in a handful of locations (relative to the large number of server locations that the data is stored on cloud networks), these data centres can be easily identified and it would be easier for hackers to narrow down on the physical location of the servers where the data is stored and these can be targeted through attacks that focus on disrupting the physical infrastructure of the data centre. The cooling stations, power supply grids, fibre optic cables relaying data and the network put in place inside the data facility can then be directly targeted and hence this carries a massive destructive potential for data loss without a chance for recovery. Quoting an interviewee here,

“*Post localisation is enforced, if a hacker wants to target financial data of Indians in the form of credit card and transaction details, they will be easily able to identify the data centres that are contracted out by say Mastercard, Visa or any of these giant payment processors. They will know exactly where to hit and depending on their degree of sophistication they will ascertain the vulnerabilities with that data centre which may be physical or technical in nature*”

Localised storage of data on Indian servers also burdens the government to provide the requisite physical security of the installations. (Sinha et al 2019)

Therefore, data localisation by mandating the centralised and concentrated storage of data on Indian servers ends up making the data more vulnerable to security threats.

A majority of the stakeholders interviewed argued against data localisation as the cloud service providers (who are handling close to 70% of the internet traffic data today) using decentralized networks of the internet spread across the globe provide a higher quality of security to data when compared to local data centre service providers in India. This can be attributed to the fact that Cloud Service Providers have built data security processes and systems that use the free cross border data flows by design and have proven to be more robust than local data centres that store data in a concentrated form on site.

Global processes built on free CBDFs that Cloud Service Providers use to provide robust data security

In the distributed and decentralized storage on a cloud network, it is relatively more difficult for the hackers to identify where the data is stored exactly as it traverses the ubiquitous data networks around the world. The status quo is that data is collected by some app or a platform used by customers and this data is then broken down into smaller packets of information[13] and transmitted across the globe bouncing off several nodes and being stored in a decentralized network of data centres and cloud networks and often many copies of the data are stored in different locations for security concerns. Tying this to the example quoted above, at present Mastercard might be making use of the data storage facilities of global cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud or even a combination of them. Per this arrangement, the financial data relating to the credit card transactions of Indians will be managed using a network of data centres spread all across the world under the control of these service providers and they will be employing sharding to distribute the data on this decentralised network. Thus maintaining multiple copies in multiple locations that makes it tougher to ascertain where the data is at a particular instance to attack.

Maintaining a copy also ensures that in case the data is compromised in one location, it is not destroyed/lost completely and can be recovered from another location. 'Data stored in multiple locations allows safe contingency operations and recovery from malware and malfunctioning while ensuring the availability of secured backups not compromised by one catastrophic event.' (Goenka et al 2019) This plays a pivotal role in augmenting data resilience and backup capabilities. Hence, even though a copy of the data stored on an Indian server via data localisation will add another level of assurance against permanent data loss, data localisation does not directly play a role here given that a robust backup mechanism already exists. Additionally, in a security network that is decentralized and follows compartmentalized management of data, even if the hacking entity accesses a portion of data, it is only a partial piece of information and cannot infiltrate beyond that or derive much utility from such fragmented data. (Drolet 2019)

Global cloud service providers and multinationals have a better understanding of the cross border data flows ecosystem and are experienced players with the necessary resources and capital invested in cyber security standards and architecture. It has been highlighted during the interviews that even though the cloud service providers follow a decentralised practice for the

[13] The practice of breaking the data packet into smaller chunks of information is referred to as 'sharding' and is a common practice that companies make use of leveraging the network architecture of the internet.

storage and processing of data, the control and management of data and its security is handled centrally. The model makes use of the pooling of the best most sophisticated data security measures and have been found to be better positioned to respond to and eliminate a data breach attempt since the counter measures will not have to be applied to each individual system and instead the solution can be applied to all components (user machines) of the cloud network from a single point of intervention.

An efficient response to cyber threats to security of data warrants a quick and efficient sharing of information regarding such attacks and threats amongst stakeholders. This draws from the fact that digital criminal activity has been found to exhibit similar behaviour the world over and a pre-emptive identification and effective response to such threats gains majorly from information from other geographies relating to fraud detection and suspicious online activity and transactions. (Yazbeck 2018) Thus, today a global database of such fraudulent activities and behaviour (that has developed as a result of collaboration between stakeholders and free flow of data) helps the cyber security professionals understand the threat landscape and prepare more robust security responses thereby protecting the integrity of data. This is of particular relevance in the financial data and services landscape. An example to further elucidate the point will be that when a fraudulent transaction is detected in one jurisdiction say in Singapore by HSBC, then this analysis helps in narrowing down on any similar transactions that might take place by the hacker anywhere in the world and the chain of actions can then be stopped by flagging and declining all activity exhibiting a similar pattern. Mastercard too has echoed concerns that arise from restricting cross border data flows and hampering fraud detection in financial services. The company argues that

> “If Indian data is disconnected from the world’s global database because of data localisation restrictions, then the fraud detection systems will be built on local trends and will fail to benefit from learning from global patterns and trends in online hacking activity. This will bring about a qualitative degradation in the financial services landscape in India since the quality of security being accorded to data will be inferior by virtue of a limited threat perception and understanding of cyber threats to such data.” (Alawadhi 2019)

Finally, it was found that from the perspective of global MNCs and cloud service providers - they will have to invest in the local data infrastructure and with different sets to regulations to comply with in each jurisdiction, the situation can lead to a variance of local security measures and standards being applied to the security of data. Such a fragmented approach has been found to be a regulatory and compliance burden for firms without doing much towards enhancing security of data and only contributes towards the lack of interoperability of cyber security regimes which further weakens the response of the ecosystem to cyber attacks. (World Economic Forum 2020)

In the context of data centres in particular, no regulations are stipulated for the kind of data security measures that must be employed as a baseline. This issue has been missing from the recent draft Data Centre Policy as well further raising concerns on the quality of security provided by Indian data centre service providers.

Protection from Foreign Surveillance

The proponents of data localisation are of the view that when data is stored on local servers within the territory of the country, it is less susceptible to surveillance by foreign governments and unauthorised hacking by other entities that malign privacy of the individual and expose them to exploitative practices on the internet. The Srikrishna Committee highlights incidents such as the Cambridge Analytica Scandal and legislations like the US PATRIOT Act and the US Foreign Intelligence Surveillance (FISA) Act that have been used to carry out surveillance activities on citizens of other nationalities using data. Speculations are also raised on the close links between Chinese tech giants and the government which can potentially expose huge amounts of data and information on citizens of other nationalities. The underlying logic of the argument made in favour of data localisation mitigating surveillance concerns is that storing data within the territory will cut off its access to foreign governments and entities which are benefitting from the free flow of data. However, a closer inspection of the issue at hand revealed that the location of data is redundant when it comes to preventing foreign surveillance activities. By their very nature, surveillance activities of governments are concentrated on systems and citizens abroad, therefore, their surveillance is not contingent fully on data of other nation’s citizens being stored within their territories as has been projected particularly in the case of the US, where most of the major data intermediaries are located and store data. Surveillance has become increasingly sophisticated over the years and does not need physical access to data or the deployment of any physical resources in another country, instead, malware and other tools are deployed remotely that enable access to the systems and the data needed for surveillance. (Chander and Le 2014) In the particular case of the US, many legal means such as the CLOUD Act provides the government with legal access to all data that is held by US based firms irrespective of the location of storage. Hence, if the US government wants access to data on Indians held by Microsoft or Google, then it has a legal way to do this for surveillance. Data localisation is a redundant measure in such cases. On the other hand, experts argued that by mandating localisation, the country may become more susceptible to foreign surveillance since the concentration of data will be on select servers within the country and this will ease the logistics and the efforts to narrow down on specific Indian data that would otherwise be a relatively lengthier and more complicated procedure when the data is stored in a distributed manner over cloud networks. (Burman 2021) Additionally, the Indian PDP Bill allows for Sensitive Personal Data to still be transferred abroad while maintaining a copy on Indian servers, which keeps such data susceptible to surveillance. Therefore, Data Localisation does not mitigate risks of foreign surveillance.

Therefore, we see that the policy of data localisation has limited utility in achieving its stated objectives for national security and also exposes the Indian data to more cyber threats on account of concentration of data and inefficiencies in data security measures by localised data centre service providers in the country.

8. Law enforcement access to data via Data Localisation

One of the principal arguments in favour of mandating data localisation and restricting cross border data flows is that it leads to a better access to data for law enforcement agencies (hereafter referred to as LEAs). The SriKrishna Committee report has listed this as one of the benefits accruing from localised storage and processing of data within Indian territory. The committee takes cognisance of the fact that in today's digital world, cyber crime and cyber threats to nations and citizens have evolved and have the potential to cause severe harm without the need for any physical interaction or movement of resources. Transborder cyber crimes such as money laundering, terror financing, financial phishing and fraud, trafficking and smuggling have been found to be increasingly making use of technology products and services. In the particular context of India, terrorists in the Pathankot Air Force base terror attacks were found to be using whatsapp calls for communicating with handlers. Similarly, the Mumbai terror attacks were coordinated using blackberry devices and messaging. Online scams and phishing make use of emails and fraudulent whatsapp messages to target the user's computer with a virus and to breach the system to access data that is then used to run elaborate scams. Cases of money laundering and tax evasion by business tycoons that have fled the Indian jurisdiction have also warranted the need for LEAs to access their financial statements and communications that are stored in the form of data with the global companies providing access to such networks and platforms. Online harassment and abuse has also seen The use of whatsapp and facebook channels to spread fake news and information resulted in a spate of mob killings in several parts of the country leading to the targeting of individuals and communities and also disrupting public order and security. The police investigating these crimes needed access to the content of these chats and posts.

Thus, more and more investigations (of ordinary crime as well since digital tools are often employed in crime in one way or another) require that the intelligence and LEAs have access to data held by data fiduciaries[14] for the detection as well as gathering of evidence for prosecution. (Sargsyan 2016 and Justice BN SriKrishna Committee Report 2019 The digital evidence required - content of the chats; emails; access to a user's device or profile is essentially held in the form of data by the global technology corporations and we have seen how they make use of the network architecture of the global internet to store data in multiple servers under the cloud model. This leads to a situation where the data that the LEAs need access to are most often stored in other countries, beyond the limits of their jurisdiction that is limited territorially. Thus the aim of this chapter is to explore the issues faced by the Indian

[14] In this particular context, data fiduciaries are often foreign entities such as multinational companies that operate in the domestic country and store data elsewhere using the cloud architecture of the internet.

LEAs in accessing data that is stored outside India for investigations and analyse the role of data localisation as a solution. **The research question for this chapter is** - “Does Data Localisation lead to better access to data stored abroad for Indian Law Enforcement Agencies?”

In the particular case of India, It is important to take note of the fact that platforms and websites that interact the most with consumers and citizens in India are provided by foreign companies and entities by virtue of their first mover and scaling up advantage - 8 out of the 10 most popular websites that Indians use are provided and owned by US based companies. (Justice BN SriKrishna Committee Report 2019) As a result of which, LEAs when wanting access to data for investigations, have to request these foreign firms or foreign governments for access to the required information. On the surface, the LEA of a particular country requiring data access for legitimate criminal investigative purposes looks straightforward and the entity should comply with the request, this however is a more complex issue.

Even though the number of requests for access to data has seen a sharp rise, the compliance in the form of granting access to data has been sluggish. Several studies have highlighted that the LEAs face a range of challenges in accessing data stored in foreign jurisdictions which leads to delays and often a denial of data access. This inturn has a negative impact on the functioning of the LEAs and hampers the course of the investigation.

This paper identifies **2 key issues that restricts the access of LEAs to data stored by foreign firms-**

1. The denial of requests on the basis of lack of jurisdiction or citing a conflict of jurisdiction between countries over the data.
2. Inefficiencies that exist in the current mechanisms used by LEAs for accessing data stored in other countries.

Both of these key issues have been explored and analysed in depth in the sections that follow.

8.1 Conflict of jurisdictions

The point of tension arises when the LEAs and the courts of the country lack the necessary means and tools to compel the data fiduciary to produce the data that is stored in a foreign jurisdiction and hence hamper the course of the investigation. (Gaillard and Molinuevo 2018) In addition the difficulty in enforcement of local data protection laws on entities in the online space and in other jurisdictions have propelled policy makers to argue in favour of data localisation. Several instances of LEA requesting access to data from companies have highlighted the competing territorial jurisdictions governing the case. It is important to note here that the access to data by LEAs is governed not only by the domestic legislations but also by the laws of the other countries involved by virtue of the stakeholders involved in the exchange being spread over multiple jurisdictions. A few prominent examples help understand this complex interplay between competing jurisdictions and the issues faced by LEAs in accessing data.

Microsoft Ireland vs The United States

In this case the US Government under the Stored Communications Act issued a warrant to Microsoft Inc to hand over the contents of an email for a narcotics investigation being conducted by a US LEA. Microsoft provided the metadata or the non content data such as subscriber information of the email that was stored on US based servers to the LEA but refused to hand over the content data citing that it is stored on a server in Ireland and hence outside the jurisdiction of the warrant which is limited to US territory. It appealed against the warrant stating that in asking Microsoft to provide data stored outside the US territory, the US government is unilaterally extending the extraterritorial reach of the SCA and instead asked the US to formally request the Irish Government through the proper legal/diplomatic channel for access to the data. The Irish government too asserted its jurisdiction over the data stored within its territory and argued against the US's attempt to access data without its consultation or cooperation. On the other hand, the US government argued that since the data is stored on a server that is under the full control of Microsoft, a company that is incorporated in the US, it must provide access to such data under its control regardless of where it stores it.

Belgian Government vs Yahoo! Inc

The case involved a crime that was committed using a Yahoo email account. A directive was issued to Yahoo Inc under the Belgian Code for Criminal Procedure to provide the data on the accounts requested to identify the individuals. However, Yahoo refused to comply with the order stating that it is incorporated in the US and under the blocking statute of the US ECPA and hence the request must be channeled to the US who would then be eligible to issue a directive to Yahoo. Yahoo also argued on the basis of it not having a commercial establishment in Belgium at the time and hence not under the enforcement jurisdiction of the country. The Belgian government however posited that by virtue of offering services to citizens within Belgian borders, Yahoo has a commercial presence and hence under the jurisdiction of the Belgian courts.

Brazil Government vs Orkut

In 2006, a federal judge issued a directive to the social media networking site Orkut (a platform controlled by Google) to provide the Brazilian LEAs access to data pertaining to accounts of Brazilian individuals who were alleged to be using the platform for spreading child pornography and narcotics. Orkut refused to comply with the order on the grounds that the data regarding the individuals was stored on US servers subject to US blocking statutes such as the ECPA and hence the Brazilian authorities cannot be given access to. The Brazilian government then resorted to heavy fines and even jailed an Orkut employee for non compliance which eventually pressured the company to produce the required data.

Taking a cue from the examples above we can see the a typical case involving an LEA to access data the following considerations add to the complexity of determining the laws of which country will be applicable over and guide the access to the data-

1. The location of the data ascertained by the location of the data server/centre under a controller.
2. The country where the Foreign firm is incorporated and hence what domestic laws will they be subject to. Here the foreign firm refers to the entity that is involved in the provision of services and collection of data (data fiduciary) but does not necessarily store the data on its servers. The data storage services may be contracted out to a third party cloud service provider as is the norm today.
3. The country of incorporation of the service provider themself. This is due to the fact that modern cloud service providers have a wide network of data centres spread across the world. The country of incorporation of the service provider will thus be distinct from the location of the data centre (which is under its control)
4. The nationality of the individuals to whom the data pertains. The investigation may warrant access to data that pertains to individuals of different nationalities who were involved in the cybercrime. This also sheds light on the issue of the cyber criminals making use of the internet and conducting transnational crime without any presence or assets in the country where the crime takes place. This poses a significant issue of determining the applicability of domestic laws.
5. The extraterritorial reach of the domestic laws of a country.

Additionally, the determination of jurisdiction has been developing on the different standards used by countries and on the basis of what factor and the location of which stakeholder the courts decide to stress on in deciding the claims. Additionally, in the absence of international agreements that set the boundaries on exercise of jurisdiction by different states, the question on the applicability of laws of sovereigns becomes further complex. (UNCTAD 2019)

Does Data Localisation resolve the conflict?

It has been posited by the Justice BN Srikrishna committee along with the proponents of data localisation that mandating localised storage of data on Indian servers will help resolve the questions on conflict on law favourably arguing for India's right to exercise jurisdiction over the data in question. However, we must differentiate between asserting jurisdiction and being able to assert exclusive jurisdiction that helps the LEAs compel the companies to share access to the data stored by them. The contention on exclusive jurisdiction was also brought out by multiple stakeholders during the interviews conducted. The stakeholders unanimously agreed that even after data will be stored of Indian servers, it will be subject to at least the laws of the country where the company handling the data is incorporated along with Indian jurisdiction. Further, if the country where the company is incorporated has blocking statutes, such as those in the US, that prevent the companies from sharing data with foreign governments (in this case India will be considered the foreign government) then the issue of competing jurisdictions will still continue to pose issues for access for LEAs. A report by the Centre for Internet and Society echoes this contention and states that

> 'Even if Facebook stores data on Indian servers, it is still Facebook's data and is subject to the statutes of the US such as the ECPA and SCA that prohibit the US incorporated companies from sharing certain types of data with other governments and mandates that the foreign governments make official requests to the US government directly to access the data that is held by such US firms'. (Sinha et al 2019)

Secondly, it is argued that data localisation may help in extending jurisdiction over such foreign entities that offer services and collect data from Indian citizens but do not have a presence in the country by virtue of being registered or having personnel or physical property in the country. [15] The idea is that localised storage requirements would compel the companies to establish through a subsidiary in India and invest in physical infrastructure for data storage needs thereby enabling the extension of jurisdiction over them using the establishment principle. However, we must note that in the Indian context, the PDP Bill of 2019 already has provisions for mandating entities that qualify as 'significant data fiduciaries' [16] to register in India, thus the basis for enforcement of laws will be their legal registration already provided for instead of the data localisation stipulations. (Burman 2021)

Further, it was found that the extension of the jurisdiction of local data protection laws will be a function of the scope of applications as laid down in the provisions of the Act that is a clearer and less restrictive approach than mandating data localisation, that brings with it several costs

[15] This is a common way of operating by modern firms that use the internet architecture and services to reach the consumer without establishing a presence in the country.

[16] On the basis of the volume of data that they collect and process, the number of users that they are in the business of data with.

and consequences. A number of data protection laws have started incorporating extraterritorial effects incorporated by design. Article 3 of the GDPR titled ‘territorial scope’ states that-

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.[17]
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.[18]
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.[19]

Similarly, the Personal Data Protection Bill of India, under Section 2 clause (c) outlines its scope of application as below.

The provisions of this Act shall apply to-
(c) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is—
(i) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India;
(ii) in connection with any activity which involves profiling of data principals within the territory of India.

Thus, looking at these provisions we can see that the laws in development have made provisions that will ensure the effective enforcement of data protection safeguards to Indian Personal Data. The underlying intent draws from the ‘targeting principle approach’ (Hoglund 2018) to jurisdiction in International Public Law and is to extend the reach of the data protection laws beyond the territory of India and over entities that are conducting business and interacting with citizens by way of offering services (and hence collecting and processing data), even if they are not physically present within the jurisdiction. This acts towards mitigating the concerns that foreign service providers that are not physically present operate outside the ambit

[17] EU General Data Protection Regulation- Official Legal Text (https://gdpr-info.eu/)
[18] Ibid
[19] Ibid.

of the local laws and also establishes a more stable link between the online activity of the companies and the effects on the state and its citizens. Therefore the argument that data localisation is necessary for the enforcement of domestic data protection laws on foreign entities is not justified.

While the PDP Bill of India does well on the front of expanding the reach of the data protection safeguards that will be able to Indian personal data per the principles and provisions of the bill, there is still an element of territoriality that is attached to enforcing these safeguards which can be interpreted from the wordings of the clauses - 'within the territory of India'. There is wide consensus of the fact that in order to keep pace with the technological developments, the data governance frameworks must shift away from territory based determinations of jurisdiction. Given how data management and storage processes are evolving, data is getting fragmented and stored around servers and only being identifiable when assembled remotely, which thus makes it difficult to ascertain which particular territory the data at a particular point is located in and consequently adding to the conflict of laws. (Gimelstein 2018) Several companies have also highlighted that if the territory based jurisdiction determinations continue, then legal requirements rather than technical considerations will guide their data storage choices and practices which will undermine the productivity and efficiency in providing services to consumers. (Westmoreland 2014) In order to further strengthen the position of Indian data protection law in providing security to Indian personal data and taking a holistic view of the fact that Indians' data must be protected regardless of its location the PDP Bill must be amended with additional provisions regarding its scope of application. Several interviewees were of the opinion that territorial principles must not continue to occupy a central position in jurisdictional applications of the laws. They instead argued in favour of an approach centered on a data principal's nationality. In essence, this approach relies on the principle that the reach of the Indian PDP and its safeguards extends to the data of all Indian citizens whether or not it is collected or processed within the territory of India. To demonstrate the working of the additional safeguard we consider an example. An individual who is a citizen of India might be residing abroad temporarily for educational or business purposes. Their online activity in the other country will produce data that will be subject to the laws of the country by virtue of the location and time of collection. Hence, should this data be required for an investigation by Indian LEAs, it can be denied on the grounds that the provisions of the PDP Bill do not extend to it. On the other hand, if the jurisdiction is extended by provisions based on Indian nationality, then India can make a stronger claim on the data in question in the above example.

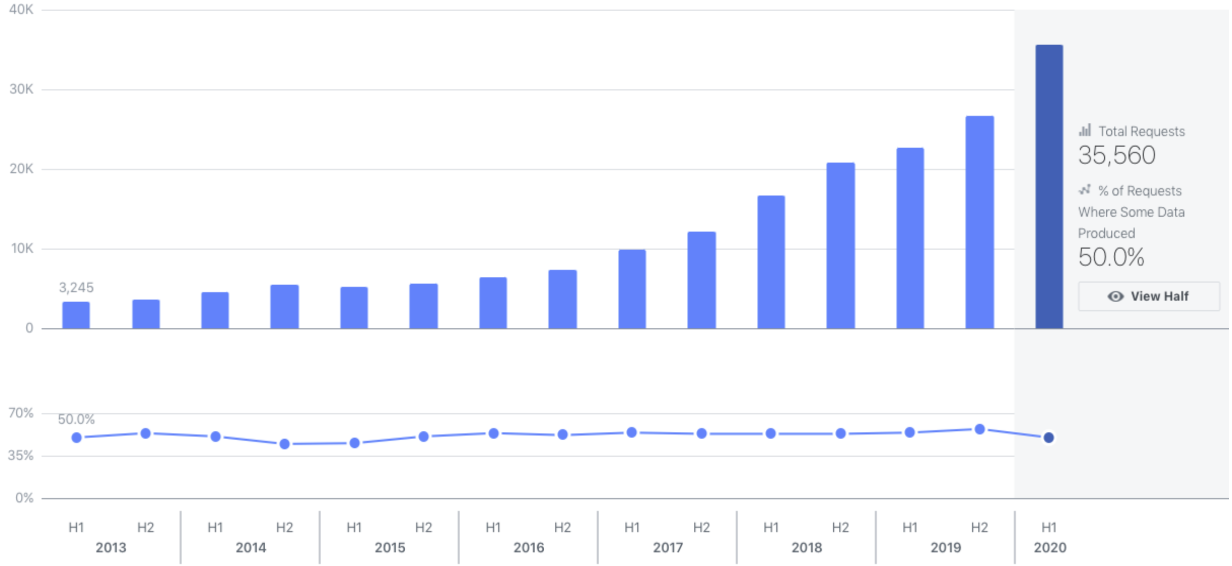
8.2 Inefficiencies in the existing mechanisms

The following sections analyses three predominant methods- Direct Data Requests to Service Providers; Mutual Legal Assistance Treaty (MLATs) and Letters Rogatory (LRs)- used by the Indian LEAs to access data that is stored by fiduciaries in other jurisdictions

Direct Data requests to Service Providers

Direct data requests are a form of an informal mechanism that has been devised by the LEAs to seek data access outside of the formal legal and diplomatic channels due to their structural inefficiencies that cause prolonged delays in investigations that involve access to data across borders. In this method the governments make the requests for access to user data directly to the firm concerned. For instance, an investigation agency in India while investigating a case of extortion may require data/ information on the whatsapp chats between the criminal and the victim or access to emails exchanged between criminals. In such a scenario, the government or the LEA will make a direct request to Facebook or Google for providing them with the necessary data. In making direct requests for access to data to these firms, the LEAs face an issue of non compliance with requests which translates into non disclosure of data that is sought. Tech giants such as Google and Facebook publish half yearly "Transparency Reports" that include details about the number of requests made by governments for access to user data, how many were complied with along with other details. These reports can be attributed to the fact that these firms have in recent years come under intense scrutiny and fire all across the globe under allegations of partnering with governments and providing access to user data that leads to the invasion of privacy of individuals and gives power to the state for domestic surveillance and censorship amongst others. Below are some data points from the latest transparency reports by Facebook and Google. (Jan -June 2020)

Figure 9 : Graph depicting total number of requests received and % of requests complied with by Facebook for India.



Source - Facebook Transparency Report 2020

We observe here that the number of requests[20] (both emergency and legal) made by the Indian government for access to data to Facebook have increased exponentially over the years- rising from 3245 in the first half of 2013 to a staggering 35,560 requests in the first half of 2020 itself. However, the metric that stands out here is the compliance rate of 50% which indicates that of all the requests made by the Indian government (on behalf of the LEAs for investigation) just about half of the requests were complied with and data that was sought was provided.

To see whether such low rates for data disclosure and compliance are uniformly applicable to other countries making such requests, a comparative table was compiled with metrics displaying the requests made and % of compliance. The countries were selected on the basis of the volume of data requests made by them which were found to be comparable to the Indian requests.

Table 7 - Comparison of data requests[21] made by different countries in the first half of 2020 to FB and their compliance %

[20] There are broadly 2 kinds of requests that are made to such firms by government- Legal requests and emergency requests. Legal requests known as "legal process" are the ones that are accompanied by a search warrant or a legal instrument. The data is then disclosed on the basis of the terms of service of FB and the law applicable in the particular case. Emergency requests are the ones that are made without a legal instrument, citing the urgent need for access to data for the investigation. FB has declared that in some instances it voluntarily discloses data in the absence of legal instruments based on their own assessment of the situation involving a serious physical or imminent risk.

[21] The total number of requests made also includes the requests made under the formal MLAT route that are categorised under the Legal process. A distinction could not be made since the court orders do not always indicate that they are a product of the MLAT process. (Facebook transparency report 2020)

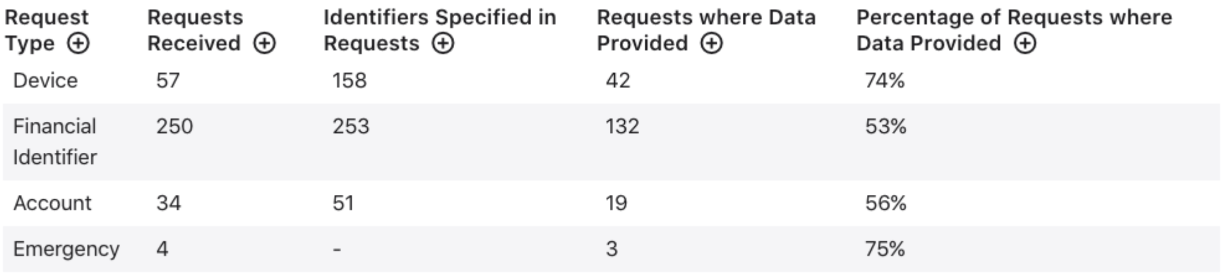
Country making the request	Number of requests made (Legal process + emergency)	% of requests where the data was produced by FB
UK	9,185	88
US	61,528	88
France	11,086	85
Brazil	7,517	71
Germany	11,211	62
Global	1,73,592	72.8

Source : Compiled by the author

The data in the table above reflects that there is a significant gap between the compliance rates for other countries with a comparable number of requests when compared to the Indian figures. Particularly in the case of the US, where the number of requests for data access are close to twice the number of requests by India, a staggering 88% of the requests were honored by FB. The global trend of a 72.8% compliance too reflects the disadvantage that India faces in accessing data stored by foreign companies and the lack of efficiency of direct data requests.

In its transparency report for the same period, Apple reported the following figures for government requests to customer data.

Figure 10 : Indian requests and breakdown of compliance status by Apple Inc.



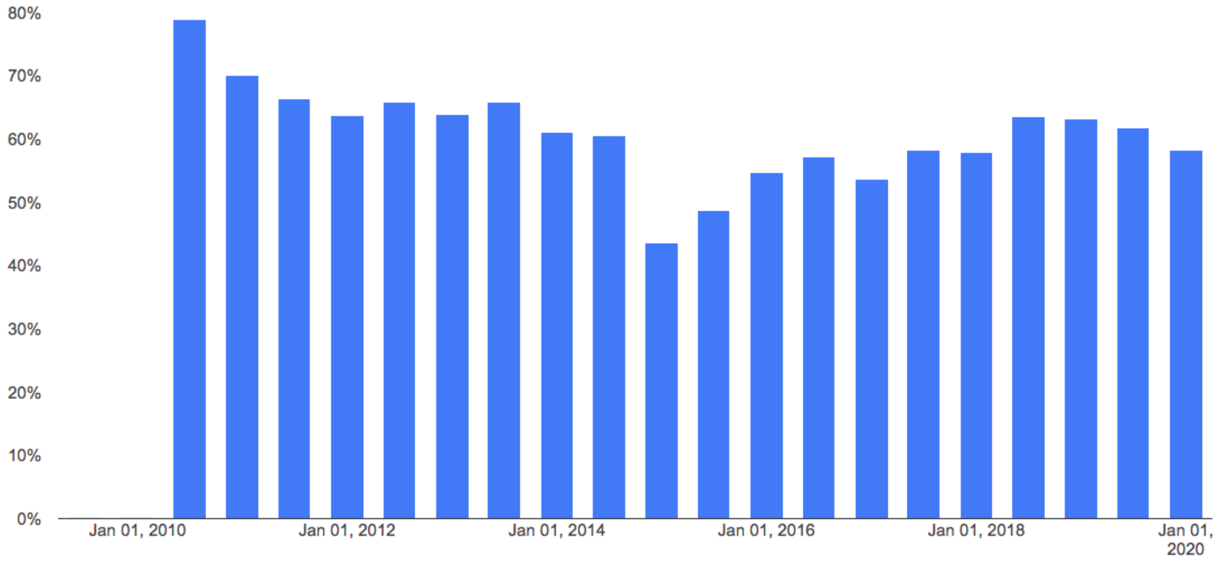
Request Type ⊕	Requests Received ⊕	Identifiers Specified in Requests ⊕	Requests where Data Provided ⊕	Percentage of Requests where Data Provided ⊕
Device	57	158	42	74%
Financial Identifier	250	253	132	53%
Account	34	51	19	56%
Emergency	4	-	3	75%

Source : Apple Transparency report (Jan -June 2020)

Here, the requests for ‘Device’ are those regarding access to customer data such as the IMEI number to identify the devices. ‘Financial identifiers’ would typically be credit card details of the customer and ‘Account’ would be customer information in the form of the Apple ID used on various devices, email ID and access to contents of email. (Apple Transparency Report H1 2020) However, we see a low compliance rate of close to 56% for Account and financial identifiers, which can be argued to be the most prominent pieces of data required in online and criminal investigations.

Taking a look at data reflected in the Google Transparency Report.

Figure 11 : Graph depicting compliance % by Google for Indian requests.



Source : Google Transparency Report 2020

A total of 11,218 requests under different categorisations of legal and emergency requests were made to Google in the Jan-June 2020 period. The data in the figure above is in sync with the trend observed with Facebook, with Indian requests for access to user data for accounts held under various google platforms and apps have seen an average compliance rate of 58-60% in the last 6 years. Thus, we see that Indian LEAs are denied access to evidence more often when compared to other countries. A study by the Observer Research Foundation titled "India US Data Sharing for Law Enforcement" drew similar conclusions about the US service providers and their response to Indian LEAs user data requests. It was further found that Indian LEAs wait much longer to receive the data per the request when compared to other countries' LEA requests.

Issues identified

While trying to ascertain the reason for such compliance rates, the most explicit declaration by Facebook and a sentiment that has been echoed by other data fiduciaries as well has been that - the companies carry out their own analysis of whether the request is in conformity with the laws applicable to that particular context[22] in addition to whether the request is consistent with principles of rule of law, human rights, privacy and free expression. (Sonderby 2020) This in turn gives the companies a wide spectrum of discretion in deciding to comply with the requests by governments. The compliance with requests through this method is purely based on voluntary cooperation by the firm since the channel of the request does not have a legal

[22] The applicability of laws and determining whose law governs the data has already been shown to be a complex process in the previous section on jurisdiction in cross border data flows.

backing and hence not binding on the company. The non compliance here has been the source of friction between governments and tech companies (in the role of data fiduciaries) in many instances and has elevated the concerns and prompted the policy makers in India to look for other solutions that remedy the quagmire that is caused by lack of access to data crucial to investigation by LEAs.

Further, insights from key informant interviews brought to light some additional concerns. Firstly, foreign service providers are mostly requested for -

1. Subscriber data (such as username, email id, billing address in the case of financial services online)
2. Traffic data which relates to the movement and duration of data. It will typically include the origin and destination of the communication.
3. Content data - This would include the actual substance or content of the data. Eg - The contents of the email exchanges between the individuals under investigation.

The one with the most utility in online and even ordinary criminal investigations is that of content data since it forms the basis for evidence in prosecution. However, the foreign service providers (and this is most applicable to those based out of the US) are allowed to only share non-content types of data on a voluntary basis with other countries. This is because laws such as the ECPA[23] prohibit the sharing of content of data with other countries except where a US court of law has scrutinised the request on the basis of the request meeting "probable cause" and has passed an order to the same effect. Thus a major limitation of the direct data requests mechanism is that its scope is limited to access to basic subscriber information or metadata (Parsheera and Jha 2020) Access to the actual content still needs to go through more formal routes with more steps of legal scrutiny as will be described in the following sections. Further, a number of studies by the CSIS, RAND Corporation and Brookings to name a few have brought out the contentions from both the LEAs and the service providers have been highlighted that adds to the lag in the system of access to digital evidence in the form of data stored in remote servers abroad. The key insights have been distilled in the tables below-

[23] The Electronics Communications Privacy Act is a federal law of the US. It governs the access to stored data and interceptions of live communication data for law enforcement purposes.

Table 8 : Mapping of arguments by Service Providers for direct data requests.

Arguments made by the Service Providers for rejecting the data access requests	
1	Personal emails being used to send the requests instead of official emails and documents with the appropriate official letterhead of the department making the request - A requirement that has been explicitly specified by the service providers.
2	Multiple agencies involved and often multiple officers from within the same organisation sending requests for access to the same accounts and data. Which in the opinion of the service providers only adds to the build up of the paperwork.
3	The service providers also flag concerns on the articulation of the data access requests. On the websites that endorse how the service providers handles government and LEA data requests, they specify that the requests must indicate as precisely as possible, the data or the account that the access is sought to, the law under which such a request is being made and the specific provisions that are being triggered in the particular case. However it has been found that often the requests lack the details mentioned above that leads to rejections.
4	The service providers have also been found to be turning down requests on the basis of the location of data. Arguing that the Indian subsidiary of the service provider does not hold the data the access is sought to and hence the service provider cannot provide the data as it is held in another jurisdiction.

Source : Compiled by the author

On the other hand, the LEAs have their own set of contentions with the current ecosystem.

Table 9 : Mapping of arguments by LEAs in direct data requests.

Arguments made by the LEA	
1	The LEAs argue that the service providers make the process more complicated by adding criteria that are open to interpretation. The grounds for not being 'clear in articulation' do not hold water according to them since the LEAs cannot be expected to know the exact ways in which the service provider refers to and categorises their data and accounts.
2	The lack of a real time interaction between the two also adds to the inefficiencies of the system since much of the communication is limited to paper trails that are time consuming and also do not provide a space for addressing and understanding each other's concerns with the process.

3	The data that is handed over to the LEAs in an unstructured format and making effective use would require significant investment in data analytics tools and human resources that are currently lacking in Indian agencies.

Source : Compiled by the author.

In addition to the above, different companies have been found to be following different templates and methods for evaluating such direct data requests. Where Google has mentioned in Terms of Service that the requests will be evaluated and complied with on the basis of it satisfying ‘global standards, internal privacy regulations of the company and laws of the US and the requesting country’. Apple and Facebook’s Terms of Service reflect their evaluations are based on the legal basis of the domestic laws of the requesting country. (Srikumar et al 2019) This can be viewed as an ambiguity that on one hand gives a wide scope of discretion to the service providers since the meaning of the words can have broad interpretations- a discretion that exhibits trends of non compliance and turning down requests more often. On the other hand it adds administrative burden for the Indian LEAs to keep tailoring their requests to the specific firms given the rising number of investigations that seek data access. A general insight on the dynamic between global data fiduciaries and governments has been that a reason for the reluctance in cooperating with LEA requests has been to counter the direct overreach of governments on the firms outside of the set legal and diplomatic channels. The firms posit that by complying with direct requests, a ‘dangerous precedent’ is being set which can have serious repercussions for the autonomy of the firms in operating and also for the privacy rights of the users. Thus, in order to project themselves as a proverbial defender of digital rights online, the firms are seen taking a skeptical and sluggish approach to direct requests for access to data. Thus it can be seen from the data and its analysis presented above that the route of direct access requests to service providers has been inefficient in meeting the requirements of access to data critical to investigations for the law enforcement and intelligence agencies.

Mutual Legal Assistance Treaties (MLATs)

MLATs are agreements that can be bilateral or multilateral and are mechanisms for formal requests between countries that facilitate the requests and exchange for evidence located in their respective jurisdictions. Given that crimes and offences are no longer territorially bound, the MLATs were envisaged as a process that ensures mutual assistance and cooperation between parties to the treaty in the matters of domestic investigations and legal processes that may involve access to evidence and data stored in the other country’s jurisdiction. (Sinha et al 2019) These are most commonly set up and used to facilitate cooperation for criminal investigations and prosecutions, for civil and commercial matters, MoU’s between the countries are the facilitating mechanism, these will be discussed and analysed in the next section. Under an MLAT, a law enforcement agency in one country can request another country that is part of the agreement, for access to evidence that can be in the form of physical evidence, testimonials, documents and most recently, with the advent of digital technologies and the internet, electronic evidence or data has also been brought under the ambit of MLATs. (Sagar et al 2020) In the absence of data sharing agreements signed at the executive level between countries, MLATs have been relied upon as the mechanism to facilitate cooperative sharing of data in the form of evidence. (Srikumar et al 2019)

Though MLATs can be viewed as a tool for legal cooperation in criminal investigations and has a wide mandate when it comes to the kinds of legal assistance offered, in this section MLATs will be analysed in their efficacy to provide access to data sought by LEAs in the modern cross border data flows ecosystem.

Post the signing of an MLAT between two or more countries, the parties must designate a Central Authority for receiving and handling requests for criminal matters. (Mehta 2020) For India, the Ministry of Home Affairs (The Internal Security- II (IS-II) division in particular) is the nodal agency for MLAT incoming and outgoing MLAT requests. At present, India has signed MLATs with 40 countries including the US, EU, UK, Russia, Singapore amongst others, with the latest one being signed with Maldives in 2019.[24] Should the need arise for access to data from countries that do not have an MLAT with India, in addition to the informal direct data request to service provider discussed in the previous section, the Ministry of Home Affairs makes requests to other country's governments through the consular/diplomatic channel on the basis of guaranteeing reciprocity to the other government.[25] When such cases arise and diplomatic channels are utilised, the Ministry of External Affairs of India is also involved in the process.[26] Information regarding the exact role of the MEA in such cases and sharing of responsibilities with the MHA are not available in the public domain.

The process of requests through MLAT

In the case of an MLAT request from India to the US the following steps are followed.

a. The Indian Investigation agency must first make an MLAT request with the MHA which is the designated central authority.
b. The MHA then reviews the request and then relays it to the US Department of Justice's Office for International Affairs.

[24] https://cbi.gov.in/MLATs
[25] https://mea.gov.in/mutual-legal-assistance-in-criminal-matters.htm
[26] Ibid

c. The US Department of Justice after reviewing the request and finding it in order will forward the request to a US prosecuting attorney.
d. The attorney will then place the request before a US Federal Judge for review.
e. If the federal judge finds that the request abides by US legal requirements such as the presence of a substantive cause for the request, the judge will then issue a directive to the firm to produce the documents, physical evidence or data requested.
f. The evidence produced by the firm is sent to the US DOJ again to ensure that the production and sharing of such information and evidence in the particular case will be in accordance with US laws and regulations.
g. The DOJ can then share the same with the MHA who would eventually relay it to the Indian LEA that initiated the request.

Issues identified

Though the MLATs have been found to be a beneficial mechanism in facilitating cross border law enforcement cooperation in cases of transnational characters. Particularly in the money laundering cases or corruption committed by companies through their foreign branches, the mechanism has given teeth and reach to the LEAs of one country to seek the cooperation of another country's LEA and get access to evidence that has proved key to initiate extradition proceedings against fugitives that have fled the jurisdiction of the first country. They enable cooperation between the LEAs of countries that otherwise have no other means to do so. (Mehta 2020) MLATs have also been one of the first international frameworks that create a privileged relation between 2 countries in the area of Law Enforcement by being a legally binding obligation to extend assistance that makes the mechanism a more stable and reliable alternative. (Sagar et al 2020) However, **in the particular context of LEAs access to data in other countries, the efficacy of the MLATs has been questioned while highlighting the inefficiencies of the system.**

MLATs were first introduced in the pre-internet era where the cooperation sought was more for physical evidence such as documents seized from the individual in another country and to seek seizure of property, freezing of bank accounts or handing over the custody in extradition cases. But, as we have noted, with the evolution of cyberspace, the nature of criminal activities online has changed and hence the needs of the LEAs have shifted majorly from requiring physical evidence to requiring access to data held by firms abroad. As more and more investigations require access to data, the traditional MLATs have been found to be inefficient in handling the quantum of requests for electronic evidence given that even domestic investigations are now compelling the investigating agencies to file MLATs. Due to its formulation in the pre-data era, the provisions of the MLATs in general do not specify the different categories of data such as differentiating between content and non content data that leads to a lack of clarity on the terminology and different interpretations by stakeholders. For instance, in the India US MLAT in operation, the scope of application that decides the level of cooperation does not specify what form of data and digital communications - cloud data, meta data, content data, machine data and machine to machine communications which hampers the process. (Sinha et al 2018) Several studies have pointed to the extremely time-consuming nature of the MLATs. Given the number of stakeholders involved and each step involving a subjective interpretation and determination (which is a largely opaque process) by different bodies, leads to an extended timeline anywhere between 10 months and 2 years for processing of the requests and the required data reaching the Indian LEA. (Parsheera and Jha 2020; Sinha et al 2019; Srikumar et al 2020; Burman 2020) Such a timeline is especially problematic in investigations requiring digital evidence since the lack of access to data blocks the entire investigation. Certain principles like dual criminality pose a challenge to the process. Under this, the country that has been requested via MLAT, may state that they will cooperate only if the offence for which the data is sought is recognised as an offence under its local laws. The provisions in other countries that notify the data subject of another government's data access request and provides for appealing against it in the local courts, where on one hand can be seen as a good safeguard for user privacy and rights online, further adds to the potential of delays in the process. (Sagar et al 2020) Another key issue at hand is that data being stored in multiple copies on servers in different countries, the determination of 'where the data is located' is a complex if not impossible exercise. The sharding process creates discrete packets of data that only make sense as information when assembled, this then poses an issue to the LEAs to determine which jurisdiction to send the data to. Given that MLATs exist only with certain countries and the ubiquitous flows of the data across borders, this poses a limitation of the efficacy of the MLATs for LEAs. The practice right now is to send it to the country where the company handling the data is incorporated, but as we have seen before, the companies often argue that the data is with their subsidiary in another country and hence cannot comply even with the MLAT due to technical difficulties such as only the subsidiary having the access controls over the data in question, thus the MLATs do not address the key issues on data and jurisdiction in its provisions which is a major detriment for access to data by LEAs. Outside of the US and the EU, the lack of designation of the central authorities for coordinating requests from India also poses a significant issue. On the side of the requesting authorities, a significant number of MLAT requests have been found to be turned down on the ground that the requests are poorly drafted and do not include the necessary details such as the law of the host country being invoked along with supporting details for US legal authorities to determine probable cause. The interviews reflected that this is largely attributable to the lack of training and capacity on the part of the Indian LEAs.

8.3 Data localisation as the proposed solution?

We have seen through the above analysis that access to data stored in other jurisdictions is a legitimate issue faced by the Indian LEAs and merits attention for resolution. Proponents of data localisation zero down on the data being in another jurisdiction as the key cause of the issues faced by LEAs and propose that by mandating localised storage of data within India, the LEAs will be able to maintain control over the data for regulatory purposes and reduce their reliance on cumbersome mechanisms and the discretion of other countries in trying to access data and running investigations. However, this research finds that the arguments of using data localisation to enable better access to LEAs are misguided. Firstly, we must take note of the fact that from a technical viewpoint, data localisation is a redundant measure as the mere local storage of data does not rule out the cooperation that is required from the firm controlling the data who is required to extract and assemble the data from its servers. Arguments were made that in the absence of such voluntary cooperation, data localisation will help legally compel the firms to hand over the data since a copy will be stored on Indian territory. However, we have already seen how the core issue in inability to access data by Indian LEAs is the lack of exerting jurisdiction over the foreign entities and how data localisation does little to resolve the conflict of laws. Even if data is stored on Indian servers, the blocking statutes of other countries like the ECPA of the US will still limit the reach of the Indian LEAs and will in no way reduce the reliance on the existing mechanisms of MLATs or LRs. The data localisation requirements will also not solve the issue of access to data of non Indians stored in servers abroad. This is an issue that warrants consideration since the data regarding cyber criminals targeting Indian citizens and thus important for the investigation will still be outside of the reach of the Indian LEAs and the only recourse available will be the formal instruments like MLATs in place. In the case of firms that operate from non US territories and who do not have similar blocking statutes, the localised storage of data may enable a wider and speedier access for the LEAs but there is little evidence before the practical implementation to suggest better compliance by these non US entities. (Sinha et al 2019; Burman 2021) But we have seen that the bulk of the cross border data flows and storage is handled by firms incorporated in the US and hence in practical terms the utility of data localisation is unfounded. Additionally, through our analysis of the mechanisms in operation, we can ascertain that the issue does not lie in the location of storage of the data but instead on the inefficiencies that exist in the current mechanism. Data localisation mandates do not find any use in improving upon these inefficiencies. For instance, we have seen that MLATs and LRs are extremely cumbersome in nature but mandating localised storage does not provide any measures that improve the speed of access. Next, the inefficiencies arise from the complicated and subjective procedures that have been found to be opaque, involving a large number of stakeholders which need structural reforms and are not assisted by localisation requirements. There are issues of administrative and technical capacity in the Indian LEAs which leads to faulty and incomplete formulation of the requests that are then turned down. Lastly, there are technical difficulties in the processes that localisation does not solve, one of them being the issue of access to unencrypted data from the service providers. (Burman 2019; Seth 2019) Firms have been found to turn down requests from Indian agencies citing that the technologies they employ do not allow them to access the end-to-end encrypted devices or content of communications. This is particularly the case with Apple and Whatsapp when requesting for content. In order to resolve this, experts have posited the requirement for an independent legal requirement that mandates the companies to maintain keys and processes that allow the decryption for lawful access to data, such a law is currently in consideration in India.

In conclusion, data localisation requirements by themselves do not resolve the issue of access to cross border data by Indian LEAs. Instead, a more structured and targeted response to the concerns and difficulties faced by the Indian LEAs in access to data warrants reforms in the current mechanisms along with a new stance shifting away from localisation on how to facilitate cooperation for law enforcement purposes in the context of cross border data flows.

8.4 Way forward for improving access for LEAs

This paper recommends a 2 step approach for improving the overall framework in India for improving LEA access to data stored abroad. The solutions are in the form of a graded approach that starts from internal reforms and goes till the priorities at the international scale.

Internal - MLAT reforms

The analysis in the preceding sections shows that there is an urgent need to introduce reforms in the current mechanisms that facilitate access to data stored abroad for Indian LEAs. The MLAT is the most widely used mechanism for this and has structural and internal capacity issues that make the process inefficient. The following are the reforms suggested for MLATs-

1. **Investing in and building internal capacity of Indian LEAs**
    a. The first step on the Indian side of things should be to rectify that shortfalls in the technical capacity and training that leads to poorly drafted and submitted requests which consequently get held up in scrutiny or rejected. The MHA can review the legal and technical requirements of all the countries with which India holds MLATs and then issue a model template for filing requests for each of

these countries. This will ensure that the Indian LEAs have ready reference documents to refer to which will help them put together the necessary documents required by the other country for facilitating the request.

b. Next, the technical capacity of the officers involved in the process must be improved through training. This should operate at the level of the MHA since it is the designated coordinating body, the central LEAs such as NIA, CBI, ED and the state police officers who file such requests while investigating crimes. Adequate allocation of resources both financial and to ramp up administrative capacity must be made by the MHA for this purpose.

c. Taking note of the fact that the MHA and the central LEAs are better equipped and resourced to handle the complicated MLAT process compared to the state police authorities and taking cognisance of the fact that a growing number of domestic investigations also require for state police officers to file MLAT requests, more attention should be paid to developing and augmenting the capabilities of the state police for MLATs. This paper suggests that state level coordinators must be designated by the MHA who can then coordinate the establishment of specialised departments in the state police with the requisite technical and cyber legal expertise. For this the Indian policy makers can emulate the role played by the IPCC of the CBI for LR requests. The coordinator and the department can then advise the state police officers in framing the MLAT requests and coordinating its approval with the MHA. This is to ensure that between the formulation of the request by the state investigators and the review by the MHA, a layer of expertise is present which irons out the shortcomings and speeds up the process.

The next area of reforms should be the process and structure of the MLATs that are currently in operation and these reforms should be the guide for future MLAT negotiations.

Structural reforms to the current process

1. **Stipulating time bound action** - One of the most pressing issues has been the cumbersome time consuming determinations which is further exacerbated by the number of stakeholders involved in the vetting process. It is recommended that for India, the Central Government should, after a comprehensive review, mandate the time period within which each stakeholder must follow through on their scrutiny and submit the status. This is to ensure a time bound process within India.
2. **Digitising the process -** The current practice is for the state police investigators to post their requests to the IS-II division at the MHA which also responds with their

observations on paper. This is an extremely time consuming process and also adds uncertainty on the part of the investigators as they have to channel their queries through written requests. The MHA should set up a centralised secure portal online and digitise the process of receiving requests from the LEAs. The portal can also display the status of the request based on the action that has been taken within the MHA. This will not only optimise the process but also make it more transparent and accountable.

3. Taking the digitisation idea forward, the MHA should initiate discussions with the coordinating agencies of other countries to shift to a secure digitised channel for communications instead of relying on the paper trail which is the norm at present.
4. **Establish consultative channels -** There must be a channel where the central authorities from the two countries can discuss their concerns and take the opinion in case any MLAT requests are found to be deficient instead of rejecting the requests that delays the overall process further. Experts have argued in favour of making provisions for a 'cyber legal attache' in the diplomatic missions to handle bilateral data sharing requests for law enforcement purposes. This would be along the lines of the office of a Defence Attache which has a specific mandate for defence cooperation between the countries. A specialised office such as this can also play a constructive role in expediting the process.

External - Negotiating direct data sharing agreements

A key takeaway from the interviews conducted with stakeholders is that the most suitable long term solution for resolving the issues of LEA access to data in a holistic manner is for India to enter into bilateral and multilateral data sharing agreements at the executive level. The executive level agreements will help towards establishing a coherent framework for data sharing which is built upon a set of agreed upon principles and safeguards. The agreements provide for a space of constructive interactions between the key law enforcement stakeholders of both countries that helps in developing an understanding of the needs and priorities along with expectations of each jurisdiction with regards to law enforcement access to data in their jurisdictions. By doing so, the agreements also play a role in mitigating cases of conflict of law and jurisdictions that are rooted in unilateral assertions of one's data protection laws over another country, often seen as infringing on the other country's sovereignty. One of the fundamental issues has been the diverging nature of data governance frameworks and varying interpretations on consent, probable cause for accessing data for criminal investigations, establishing a nexus between the third country and the service provider's data in determining whether the request should be honoured and hence executive direct data access agreements present a unique opportunity for the partial alignment of such diverging frameworks for enabling effective cooperation of both countries in matters concerning access to data for law enforcement purposes. Direct data agreements between countries have also been found to significantly reduce the number of stakeholders and judicial and regulatory subjective determinations given that the agreement addresses key issues regarding lawful access to data and adds legitimacy to the requests from both sides. Such bilateral and multilateral agreements are also viewed as less restrictive measures when compared to data localisation laws with significantly less compliance and regulatory costs for the economy while also serving the utility in addressing concerns of law enforcement agencies. When judging the access to data for law enforcement purposes, both the speed and scope are key determinants and direct data agreements have been posited as the most effective framework for cross border data access based on these metrics. (Burman 2021) There are some key examples of executive direct data agreements that can serve as a reference- The CLOUD Act of the US which allows for executive agreements with other countries for law enforcement data access and the EU E-Evidence Directive that facilitates cross border data sharing for criminal investigations.

Clarifying Lawful Overseas Use of Data (CLOUD) Act of the United States

The CLOUD Act finds its genesis in the Microsoft Ireland vs US case that has been discussed in the previous section on conflict of jurisdiction. The Act was signed into a law in 2018 and amends the Stored Communications Act of the US for facilitating access to foreign data for law enforcement agencies of the US. Under the act, the US LEAs can unilaterally compel the data controllers incorporated in the US to provide access to data held by them irrespective of the location of its storage. Secondly, it also makes provisions for the US to enter into executive agreements with other countries for facilitating access to data held by US Service providers for foreign LEAs. In order to enter into an executive agreement under the act, the Attorney General will make an assessment of the Indian legal and procedural framework and determine if it meets certain preconditions such as compliance with rule of law, adherence with international human rights obligations and that such access to data will not be used to target US citizens. Another precondition is that the country requesting the should commit to free flow of data. (Parsheera and Jha 2020) The CLOUD Act is of particular significance to the Indian context on the second feature of the bill. India can initiate a negotiation of entering into a direct data executive agreement which will then play a pivotal role in ironing out the current inefficiencies of the system to access data. Post the agreement, Indian LEAs will be able to unilaterally send their requests to Service providers of the US to hand over data under their control irrespective of its location of storage. The agreement also leads to a relaxation in the application of the ECPA blocking statute and does away with the US judicial determination of probable cause. The incoming requests to the US will not be subject to any review after the agreement with only the service providers being able to appeal against any such request from another country, the details of how such an appeal will function however is not spelt in the law. (EPIC 2019) However it must be noted that the agreement under the CLOUD Act calls for a review of the request by an independent authority, court or magistrate in the country initiating the request. Further, the agreement under the act has a broad scope of application covering access to all kinds of data including content and subscriber data, this was earlier limited to meta data that was held on the servers of the country making the request. Thus, we can see that an executive data access agreement with the US serves the interests of the law enforcement agencies of India as both the scope and the speed of access to data stored with the US based service providers (the most significant for India) are enhanced.

However, on the Indian side, some key reforms in the existing Indian laws on government access to data are warranted in order to satisfy the preconditions set by the US. The current provisions of the PDP such as Section 35 which gives the Central Government the power to exempt any body in India from the obligations under the bill based on its discretion that it is necessary for strategic or trade purposes have raised issues on the lack of any oversight over government activities when dealing with Indian personal data and undermining the privacy safeguards laid down by the Bill. This can potentially cause India not to fit in the criteria for regard for online privacy and human rights. Secondly, the agreement warrants a commitment to free flow of data which is in contravention with the data localisation mandates being introduced in India. Further, the requirement for an independent authority like a judge or magistrate to review the request is not provided for in current Indian law as LEA officers send requests directly as per Section 91 of the CrPC. (Parsheers and Jha 2020) Experts also argue that any agreement that India enters into must be carefully negotiated while making sure that Indian priorities and interests are well represented and accommodated in the negotiations rather than just ascribing to the norms dictated by another government that will prove to be counterproductive in resolving the systemic issues of LEA access to data.

9. The Economics of Data Localisation

One of the more hotly contested issues arising out of mandating localisation of data in India has been its potential impacts on the Indian economy in general and the Indian digital economy in particular.

As has been highlighted in the process tracing for the evolution of Data Sovereignty in India and the economic objectives under the localisation policy, the recent push for localised storage of data reflects the sentiment of the policymakers to pursue a digital industrial policy that is premised upon giving the local digital businesses the competitive push to drive their capacity to innovate digital services and products and thereby expand their footprint and business opportunities. (CUTS 2020) This has further been based on the thinking that localised storage of data is required to enable access to valuable data for driving growth in the domestic digital businesses and check the monopolisation and monetisation of Indian personal data by the global tech giants that has caused this skewed ecosystem in the first place. Where on the one hand the disadvantages faced by the Indian companies and startups against the global tech giants and companies from developed nations that have capitalised on the first mover advantage merits attention and policy recalibration, whether data localisation is the appropriate tool or policy to bring about that recalibration and balance to the digital economy ecosystem warrants a deeper look at the potential costs and benefits arising from the adoption of the policy.

The Justice BN Srikrishna Committee report has posited the requirement of a data localisation policy to achieve the following objectives for the Indian digital economy-

1. Growth of the domestic data driven businesses by enhancing their productivity and competitiveness by providing them access to data.
2. Correct the imbalances arising out of data monopolisation by large technology corporations.
3. Fostering a robust AI and innovation industry.
4. Increasing investments in technology and fast tracking the development of the data centre sector.

This chapter evaluates the efficacy of data localisation in achieving its stated economic objectives while also analysing the additional economic implications for the Indian economy. The **key research question** for this chapter was - “What are the key economic implications of Data Localisation for the Indian economy?”

An analysis of the interviews conducted with key stakeholders and secondary data from studies conducted on the economics of data localisation laws, the following trends emerge that exhibit the potential economic impacts of mandation data localisation requirements.

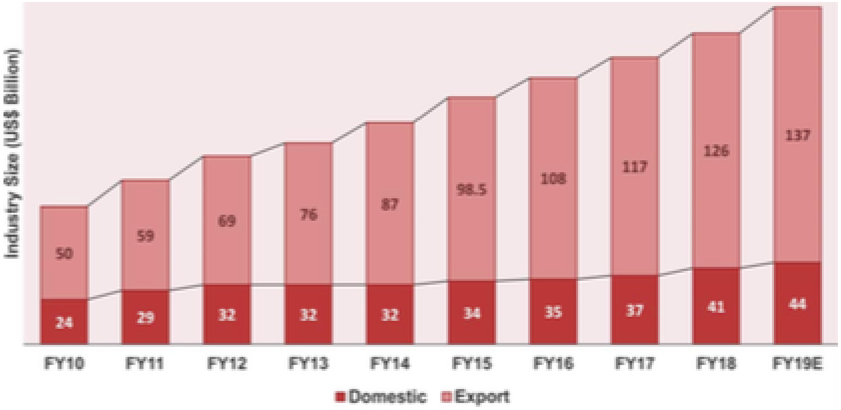
9.1 Impact on digital trade

Cross Border Data Flows have transformed trade at the global scale. Trade that was until just two decades ago dominated by the flow of tangible goods has increasingly come to be characterised by the flow of services and more prominently digitally enabled goods and services that are built on data flows across countries. Digital trade has created global markets by connecting economies using the internet and data flows which has led to the growth of digital economies that benefit from new market opportunities, transformative business processes and fostered data driven innovation that has created several new digitally enabled products and services and diversified consumer choice. A review of literature shows that one of the arguments made against data localisation laws and restrictions is that it affects the digital trade between countries negatively which in turn impacts the Economy since digital trade in goods and services have come to occupy a prominent share in the contribution to value creation in economies. Several studies by think tanks and industry bodies such as ITIF, ECIPE, ICRIER, IAMAI and CUTS have conducted quantitative estimations on the impacts of data localisation at a macro countrywide and have posited the idea that data localisation is detrimental to digital trade and GDP of modern data driven economies. However, an analysis of the methodology followed by these studies along with the assumptions and variables used shows that the factors considered are often disconnected directly from data localisation. For instance, the studies quote the growth in the international bandwidth and penetration of data and digital technologies have digitised businesses and improved connectivity and hence led to the growth of digital trade and then argue that localisation mandates impact the free flow of data which limits digital trade. However, localisation restrictions do not impact the growth of internet bandwidth or the spread of data. Additionally, the blanket argument that digital trade is impacted by data localisation takes a myopic view of the variation in data localisation requirements as not all data localisation laws impose a complete ban on transfer and movement of data across borders. Indian data localisation requirements are also conditional data flow requirements that permit the transfer of sensitive personal data via certain prescribed mechanisms. Thus in the Indian context, the findings of these studies must be considered cautiously. While investigating the link between data localisation and digital trade further, some interviews revealed that the Digital services exports by the IT-BPM industries in particular might get negatively impacted that will carry repercussions for the Indian economy as the IT-BPM industry in India is a major contributor to the GDP and has established its dominance as a global leader in exporting digital goods and services which accrues spillover benefits to the Indian economy.

A finer look at the impacts on the IT-BPM industry

India has benefitted by participating in the digital trade channels and by actively harnessing the opportunities has emerged as a prominent global leader of IT-BPM services. (CUTS 2020) A study by the Think Tank Dialogue estimates that close to 60% of the global companies are currently being serviced by Indian BPOs using digitally enabled services and business solutions. The RBI also highlights that the Indian IT BPM industry accounts for 55% of the global outsourcing market in services. It is pertinent to note that the growth of the IT-BPM industry in India and on the global scale has been largely driven by the export of digital services by the industry.

Figure 12: The Size of the Indian IT-BPM industry by domestic and exported digital services

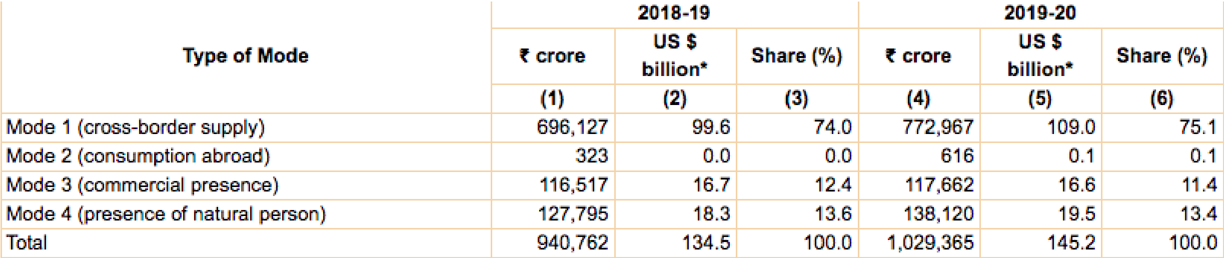


Source : Indian Brand Equity Foundation

We can see from the data above that the share of the digital services exports in the IT-BPM industry has seen a steady rise over the last 10 years and is the major contributor to its revenue. The following statistics also highlight the importance of the digital services exports to the Indian economy. Digital exports by the IT-BPM industry termed as ‘Software Services’ under the Economic Survey for FY 2019-20 was the largest component of the Total exports in Services at 43.70%. The IT-BPM industry is also a significant contributor to the Indian GDP with an estimated contribution of 8% to the GVA calculations for the Indian economy in FY20. (Indian Economic Survey 2020) An econometric study by the think tank CUTS on the direct correlation between digital services exports and the GDP yielded a statistically significant result suggesting a positive correlation. According to the findings of the study, a 1% increase in the digital services exports can potentially raise the Indian GDP by 0.02%. (CUTS 2020) Digital services exports is also the second largest category in overall exports for India with an estimated value of USD128 Bn in the FY 2019-20 and with a projected potential of reaching USD 197 Bn in the next 10 years. (Hinrich Foundation 2019) Further, the value of the digital trade for India has been projected to touch USD 512 Bn by the year 2030, growing 14 times over its current valuation with more than 1/4th of the value being driven by digital services exports. (CUTS 2020)

It is also important to note here that the digital services as per an RBI survey titled “Computer Software and Information Technology- Enabled Services Exports: 2019-20” , the digital services are exported using 4 main modes of which cross border supply of digital services exports has the lion’s share of a staggering 75%.

Figure 13 : Mode of export of digital services



Type of Mode	2018-19			2019-20		
	₹ crore	US $ billion*	Share (%)	₹ crore	US $ billion*	Share (%)
	(1)	(2)	(3)	(4)	(5)	(6)
Mode 1 (cross-border supply)	696,127	99.6	74.0	772,967	109.0	75.1
Mode 2 (consumption abroad)	323	0.0	0.0	616	0.1	0.1
Mode 3 (commercial presence)	116,517	16.7	12.4	117,662	16.6	11.4
Mode 4 (presence of natural person)	127,795	18.3	13.6	138,120	19.5	13.4
Total	940,762	134.5	100.0	1,029,365	145.2	100.0

Source : RBI

Thus we can see from the above that free cross border data flows have enabled the growth of digital services exports and thereby contributed to the growth of the IT-BPM industry and the Indian economy. From this it might seem that data localisation restrictions that inhibit cross border data flows will negatively impact this value chain in a cascading manner. However, it is important to understand that the composition of such digital services exports from India shows that the Indian companies process data of citizens of other countries while providing services such as medical transcription and documentation, back end business processes, supply chain and inventory management, all of which involves the importing of data from other countries (foreign businesses that have outsourced these functions to Indian BPOs will transfer data) and processing it in India to offer business solutions and services. Thus the Indian IT-BPM industry is primarily involved in the processing of data that belongs to citizens of another nationality which do not fall under the data localisation requirements of India that are limited to Indian personal data. Thus, localisation rules in India will not impact the ability of the Indian firms to continue with their outsourcing services or limit IT exports in any manner.

The only scenario in which data localisation requirements of India can negatively impact the digital trade (particularly the digital service exports) is when other countries take retaliatory measures against India and impose similar restrictions that then inhibits the flow of foreign data to Indian companies. Recent trade negotiations for the RCEP and the G-20 Osaka Track exhibited how certain countries like the US and other predominantly developed nations argued in favour of maintaining free cross border data flows and termed localisation to be a protectionist measure and a trade barrier. The major reason for terming localisation a trade barrier is because it limits the operations of the foreign firms when dealing with Indian personal data and also imposes significant costs by mandating the use of India data centres, maintaining separate IT infrastructure for Indian data amongst others. This can be seen as impacting the growth that these companies derived from mining Indian data and processing it which also accrued benefits to the home economies of such companies such as the US. Thus, there are potential scenarios where other countries can impose retaliatory data flow restrictions to India analogous to how tariffs are imposed in trade wars. In this situation, the flow of data to Indian companies will get restricted which in turn will disrupt the IT-BPM industry's business models and processes and consequently impact the Indian economy. Based on econometric estimations by CUTS International, retaliatory data flow restrictions by other countries can potentially lower digital services exports from India between 10% and 19%. As a consequence of which, given that there is a positive correlation between the digital services exports and the GDP, the Indian GDP can potentially decline between 0.2% to 0.34% which translates to losses of USD 19 Bn to USD 36 Bn to the Indian economy. (CUTS 2020)

9.2 Economic growth and Data Localisation

The key rationale behind governments mandating localisation for economic growth lies is that localised storage of data will provide better access for domestic firms that are otherwise at a disadvantage due to data monopolisation by certain foreign firms along with improving their competitiveness, efficiency and innovation capabilities. The following sections analyse these claims in the Indian context.

Costs for businesses

There is a unanimous agreement on the fact that the introduction of data localisation requirements in India will impose costs across on all stakeholders in the economy. The Justice BN Srikrishna Committee also takes cognisance of this consequence but argues that costs accompany any regulatory intervention and thus the increase in costs for businesses should not affect the consideration of data localisation in India. The committee also posits that 'given the size of the Indian market, the benefits arising from data localisation will outweigh the costs incurred in data processing.' However, this line of thinking does not take into account the fact that there are several costs other than those involved in localised processing that will arise from regulatory compliance requirements and that have been found to have a varied impact across the Indian digital economy.

This research identifies costs incurring in 2 broad categories - direct and indirect- from the introduction of data localisation.

Direct costs

These costs are largely compliance costs that will incur from the changes the companies will have to introduce. Firstly, the firms dealing with data will have to invest in creating data centres in India exclusively to handle the storage of Indian personal data that they collect or may choose to contract their data storage and management requirements to an Indian data centre service provider. These are significant costs as investing in creating data centre infrastructure is an extremely resource and capital intensive exercise and will only be an option limited to a few major firms with the requisite capabilities. The other option of contracting with Indian players is also not a lucrative option since the data centre market in India is still nascent having been privatised only in 2005. There is a general perception that the quality and cost effectiveness of the data centre services of Indian players is inferior as compared to the other global providers, especially cloud data service providers such as Microsoft Azure, Amazon Web Services and Google who also dominate the current data storage market. Additionally, the number of players in the Indian data centre market is limited thus leading to a possibility of non competitive pricing. However, since most of the infrastructure is still in development and the fact that different firms use the services of data centres in different ways, it is not possible to estimate the exact cost parity between Indian data centre providers and foreign firms that are largely Cloud Service Providers. A study by the Indian Council for Research on International Economic Relations estimated that the operational costs of firms could rise by close to 10% by shifting to Indian data centres from their current models of data storage which were largely found to be making use of foreign players.

The compliance costs also manifest in the form of investing in IT assets and specialised teams that will be required for the separate storage and processing of Indian personal data from the other data sets. A key point to note here is that a majority of interviewees expressed concerns over the difficulties that organisations will face in separating the data. Firms today both large and small are dealing with mammoth amounts of data on a daily basis with data belonging to different categories and from different locations being combined to form ‘high value data sets’ that are complex in nature that help businesses in data analytics. However, the separation of Indian data from these data sets will require ‘data mapping’ which is an expensive and highly technical process that will impose monetary costs along with time delays in operations of the firms. The forced splitting of data sets might also lead to errors in computing and data analytics. Most firms will have to restructure their businesses and in particular their data collection, management and storage processes along with how they currently run data analytics and share data that will be a complex exercise and entail significant investments into new areas and costs from shifting assets.

It is important to note here that the larger businesses will be better positioned to absorb the costs of compliance. Several data driven giants such as Jio, Phone Pe, Paytm in India along with the big tech companies like Google, Amazon, Facebook, Microsoft command the resources to establish their own data centre infrastructure. Startups and SMEs on the other hand do not have the kind of resources required for in house IT storage and management and will have to contract service providers from India. Given that these compliance costs will accompany the localisation policy, the government can make the transition smoother by prescribing a suitable cooling off period after due consultation with all players within which the compliance and shift can take place. Doing so will serve a dual purpose of ensuring an amicable time bound compliance with the requirements while also removing uncertainty of penalties on the firms if their compliance status is arbitrarily scrutinised.

Indirect costs

There are also indirect costs for businesses associated with complying with data localisation requirements. The efficiency of the firms gets impacted negatively, this is because by shifting data storage to localised or Indian data centres, the firms lose out on several key features that are currently provided by foreign cloud data storage service providers. Cloud storage is more lucrative for both large and small companies alike due to its flexibility and large array of storage options, data management products and services that they are able to offer. Because these Cloud Service Providers (CSPs) have a large number of servers and data centres at their disposal, they are able to make different permutations of resources to offer a wide choice to suit the requirements and financial limits of each business. The range of products and services offered by Indian data centres in general have been found to be of a lower quality with fewer options available to the firms, this in turn impacts the ability of the firms to make efficient use of the data with them. CSPs also offer a higher scalability in terms of data storage. For instance, if a firm requires more data storage facilities on account of an expanding business or due to mergers, CSPs are able to cater to this surge in the least possible time without requiring any additional infrastructure. A CSP like Google can simply allocate a few servers from each of its data centres connected on their unified network in order to make up for the demand, in the case of India however till the localised cloud services develop to a large enough network, the localised data centres will be slower in responding to the increased demand due to constrained resources (servers) at their disposal. Thus, these factors help businesses in streamlining their operations while making use of the sophisticated products and services to run analytics and derive insights that lead to value creation. The lack of such features and benefits with Indian data centre providers is likely to impact the efficiency of business operations. It is also important to note that these costs are not borne just by data driven businesses but also by more traditional sectors of the economy such as manufacturing and logistics industries that are now increasingly reliant on the suite of customised and cost effective services that are accessed through Cloud data storage providers.

In the context of efficiency, one of the arguments made against localisation is that it will increase network latency (delay in access to data from the data centre) in India. However, data travels over the internet according to the Open Shortest Path First (OSPF) policy where the data routers on the networks will push the data through the particular network that will take the shortest time to reach the destination. Given that the Indian data localisation policy does not place any restrictions on the movement of internet traffic across networks, firms will not face an issue of network latency. Businesses may also incur an indirect cost in terms of opportunity costs of investments. Investments especially in the case of startups that would be used for business expansion and new ventures may get diverted to cover the costs of business restructuring and shifting to localised data infrastructure. A study by the European Centre for International Political Economy also estimated that the new regulations on data localisation in India will reduce the Total Factor Productivity of Indian firms while incurring losses of 1.35% in the communications sector, 0.50% in the IT-BPM services sector and 0.20% in the digital finance and insurance sector respectively. (ECIPE 2014)

An indirect cost of localisation emerging in other countries

Startups and SMEs in particular have benefited from the liberal cross border data flows and have been able to expand their businesses to new markets and customers in different geographies making use of the global internet architecture. A scenario where data localisation restrictions are imposed in foreign countries that mandate the use of data centres localised within their country instead of Google cloud data storage services that was enabling them to service these markets, the Indian startups may find it difficult to invest in localised data centres of the other country and potentially lose market access to it.

Market Competition

Data localisation has been touted to reduce the inequalities that exist in the digital economy particularly on the accessibility of data which is concentrated in the hands of a few large corporations who were early movers in the ecosystem and developed and scaled their data collection capabilities over the years. However, these players have been accused of monopolising data to drive growth for their businesses and the benefits of this accrues to their home countries. Data localisation by itself does not correct the network effects and market concentration of data and does not lead to better access of data by the Indian firms. Local storage requirements are complied with by these large corporations by setting up their own data centres in the country but the data they collect is still under their control. Experts have argued that a separate legal requirement will be essential for ensuring that large data fiduciaries share data collected by them with other firms to allow equitable use of the data in the economy. Recent policy proposals such as the draft E-commerce policy, National AI Strategy by NITI AAYOG and the GI CLOUD MeghRaj initiative have posited the idea of anonymising the data sets with large technology companies which can then be shared with startups and SMEs. (Centre for Internet and Society 2019) Some proposals under the E-commerce policy for facilitating data access are to share data with startups that meet a baseline criteria such as minimum turnover and business presence. The AI strategy by NITI AAYOG envisions the creation of an AI marketplace at the national level which would facilitate a more transparent price discovery process while establishing a public portal for sharing of data between players for the healthy adoption of the technology. (NITI AAYOG 2018) Where on one hand these proposals do work towards addressing the concerns of imbalance in the markets due to market concentration of data in the hands of a few which in turn affects capabilities of firms, there are certain issues with the implementation. Media and Technology policy firm Medianama in its recommendations to the DPIIT outlined 2 key issues[27] -

1. The firms that collect data from users will be bound by their terms of service and use of data that might prohibit them from sharing it with third parties.
2. The firms also have vested IP interests in the data sets which are used for analytics.
3. Forcing companies to share data that is used primarily for improving their services and differentiate them in the market place owing to the unique use of the data, might make it difficult for them to remain competitive in the market.

We must also take note of the fact that competition in the digital markets operates differently from the traditional markets in the offline world. Anti competitive behaviour is also exhibited in other ways by hostile takeovers and acquisitions of startups by large technology corporations, offering services for free owing to the network effects that discourages startups or manipulating consumer choice by favouring a few products and firms on the platform as was witnessed in the case of Amazon India favouring some select traders on the platform. Thus, in order to effectively address the issue of market concentration and correct the imbalances, policies to incentivise data sharing amongst firms can be considered rather than taking a heavy handed approach of forcing them to. However, it must be noted that mandating or incentivising the sharing of anonymised data sets would still fall short of the goal of stimulating the domestic firms and promoting growth since there’s a fundamental difference between the data driven firm getting access to personal data that they can analyses in different ways tailored to their business needs and objectives and the large anonymised and aggregated data sets that might becomes available to them. Additionally, to holistically address concerns of imbalance between

[27]

firms in the digital markets, the competition policy must be updated in order to respond proactively to the anti competitive behaviour centered on data in the Indian markets by a few firms.

The costs that accompany localisation requirements negatively impact the efficiency and productivity of the firms which then translates into higher operational costs which are eventually passed on as higher prices and declining profits, thus making the firms less competitive. Hence, competition in the digital markets is not a function of an improvement of a firm's competitiveness but is instead attributed to the additional costs being imposed on the foreign players that brings very minimal parity. The high compliance and operational costs also act as market barriers for smaller firms and SMEs to enter and sometimes may even force businesses who find the additional expenses on IT infrastructure as infeasible, out of the market thereby negatively impacting competition and instead bolstering the position of the few large technology firms even more. The market barrier argument extends to foreign startups that offer their products and services in the Indian market. Consumers in India have benefitted from the large number of choices of services and products offered online made possible by the internet and the firms making use of free flow of data to customise their services for the Indian consumers. (CUTS 2019) Requirements to store data on Indian servers will require such startups to invest in contracting with Indian data centre service providers and if found to be unfeasible economically or on the front of efficiency and quality of services, the firms may be compelled to stop offering services in India. Along similar lines, it has been argued that data localisation measures will drive out most of the foreign firms. It must be noted that the larger companies and especially the big tech players are highly unlikely to exit the Indian market which presents a massive user base and revenue opportunities along with the prospects of an untapped market growing as more people come online in the near future. Thus, it may be argued here that data localisation requirements in India are indeed acting as a lever of control on the large technology corporations by pushing them to invest in local data infrastructure (that at the end of the day is beneficial for the data centre market in India) and imposing costs on their data extraction activities, which also falls in line with the objective of Data Sovereignty where the governments are argued to have a sovereign right to control the activities centered around the resource of data.

Innovation

The Justice BN Srikrishna committee listed the growth of the innovation ecosystem in India as one of the benefits of data localisation for the Indian economy. In particular, the committee cited the example of the AI driven growth of industries in China and the US that is argued to be enabled by access to huge volumes of data under the control of the companies incorporated in these countries. However, interviews with key stakeholders reflected that while access to data is important for training of AI algorithms that in turn drive the development of new products and solutions, the volume of data is not the key factor responsible for the development of the AI ecosystem. Data is essentially used as an input in AI systems which are made up of algorithms being developed for different purposes. The algorithm is 'trained' using the data sets wherein the algorithm unearths all the possible permutations and combinations of using the data for different purposes which then leads to analytics tools making use of the algorithm to derive insights. In this process, the more complex the data set, the better the algorithm gets trained and hence the insights are of a higher quality and wider utility. The construction of complex datasets is dependent on data being accumulated and allowed to flow freely across borders. Data localisation, by restricting the flows of data can potentially hamper the construction of these complex data sets that will inhibit the development of effective algorithms and hence affect the quality of products and services built on the platform. Infrastructure is another key enabler for the AI ecosystem. The development and running of the algorithms requires huge computational power that is catered for by the cloud computing and data storage services for reasons of scalability discussed before. In addition, a lot of the platforms that provide access to tools and services for AI development are foreign based web services. However, firms will not be able to leverage the computational power of the CSPs or the web based platforms of foreign companies as the complex data sets that they will be using will include a mix of Indian personal as well data collected from other geographies. The use of complex data sets is not an issue so long as Indian personal data does not leave the Indian territory as part of the larger data set. This essentially implies that for using data sets with an Indian personal data component, the local data centre facilities will have to be used but whether Indian data centres will have the requisite server capacity to cater to the specialised needs of AI systems and applications is questionable and needs further research. The development of AI serviceable platforms is also in its very early stages in India and does not provide the same features and functionalities as the foreign platforms. Therefore, we can see that the firms involved in AI development in India essentially face an opportunity cost while developing and training their algorithms. One the one hand they can use the proven and flexible computing infrastructure power of the CSPs and foreign AI development platforms with datasets without Indian data since using these services involved such data leaving Indian territory. However, the algorithms that are trained with data sets exclusive of Indian data will have a limited utility and application to solve issues in the Indian context thereby undermining the benefits of innovation for India. On the other hand, complex data sets with an Indian component may be used for training algorithms within India but the lack of features and requisite power will hamper the process of development of the algorithm and may inhibit the realisation of its full potential. Other emerging technologies such as Blockchain, Big Data and Internet of Things (IoT) are by their very nature decentralized technologies that develop in a geographically agnostic manner. Blockchain for instance is built on a decentralised network of databases distributed across multiple geographies to build a 'chain' that then records data in an anonymised way in one of the data bases (block). The draft National Strategy on Blockchain introduced by the MEiTY in India in January 2021 has highlighted the benefits of transparency, efficiency and security in business operations and utility in improving functionality of e-governance and service delivery across sectors in India. However, the draft also mentions that the data localisation policy will place limitations on the development and deployment of blockchain since personal data cannot leave Indian territory and the use of blockchain will inadvertently include nodes (databases) in other territories. Blockchain also saves a copy of the data on each node and the development of strong blockchains that require a diverse and distributed network of databases will be inhibited by localisation requirements. Internet of Things also relies on collecting data from devices from across the globe which are then used by the parent companies for analysis (using the company's own or outsourced servers that can be located anywhere in the world) which then leads to an improvement in services and development of new more advanced products. Since IoT devices such as heart rate trackers and fitness bands collect data from Indian citizens that fall under Sensitive and Critical personal data, the IoT technology firm's operations of collecting and analysing data will face similar limitations as that faced in the development of AI algorithms due to an opportunity cost.

Innovation in an economy is also driven by the growth of knowledge based industries and services. These industries which are primarily consulting firms and Research and Development institutions are increasingly reliant on sharing and collaboration of information that is built on free cross border flow of data. The seamless sharing of information enables new insights and yields innovations and solutions. The restrictions posed by data localisation will inhibit Indian researchers from sharing their data with counterparts in foreign universities and research institutions. This is particularly relevant for small and medium scale research projects and individual researchers since the current conditional data flow mechanisms prescribed in the PDPB 19 only provides for instruments that can be negotiated at a much larger scale with significant expenses. Thus, data localisation carries negative implications for the growth of the Indian innovation ecosystem. But given the importance of these emerging technologies to modern economies with scholars positing the idea that they will be the key drivers of the fourth Industrial revolution, the government must take measures that safeguard the development and growth of the technology ecosystems in India from the negative consequences of data localisation requirements. This paper recommends 2 approaches that may be considered to balance data localisation with the development of emerging technologies in India-

1. The government should consult the industry bodies and players engaged in the development of the technologies to gain a more holistic understanding of their requirements for cross border data flows. Based on this, some relaxations on restrictions may be considered for these industries.
2. The second approach that the government can take is to use partial adequacy decisions to enable the movement of cross border flows of data between specific industries in countries. Partial adequacy decisions are used to facilitate cross border movement of data for specific purposes between countries. For instance, the UK has given a partial adequacy decision to the US for the healthcare sector where firms in both countries can freely transmit healthcare data between them and make use of resources provided by service providers of the other country. A similar partial adequacy decision may be considered for the AI and IoT industries in India and the US that will enable the use of computing power and access to sophisticated AI development platforms provided by US based firms.

From the analysis above we see that the policy of data localisation has a limited utility in achieving its stated economic objectives of spurring innovation, improving market dynamics and competitiveness of firms while also imposing additional costs that act as market barriers, raise operational costs and cause a significant investment in business restructuring. However, it is unlikely that data localisation requirements will be rolled back given that it is helping achieve a commercial objective of data sovereignty wherein the government aims to assert some control over the data collection and processing activities of the big tech. In this sphere, data localisation has demonstrated its utility by bringing these firms to the negotiating table with the Indian government which can be seen by the intense lobbying efforts for concessions in data localisation requirements. These large corporations are also unlikely to exit the Indian market given the mammoth user database and business opportunities that the Indian markets provide. Data localisation requirements have also pushed big tech companies to invest in data infrastructure in India that has brought in significant amounts of FDI in the data infrastructure markets of India and promoted growth. Thus, despite its misalignment with the stated economic objectives of national economic growth, data localisation is likely to stay in the PDPB 19.

10. An assessment of the Conditional Data Flow Regime for India

The ecosystem created by the free and liberal flow of data across borders has generated a mix of advantages and disadvantages. Where on the one hand there are significant economic benefits in the form of scaling up of digital trade and enhanced productivity, innovation and competitiveness of the stakeholders in the Indian digital economy. On the other hand, the data flows raise some serious and valid issues in the areas of security and privacy of personal data, national security and law enforcement access to data across borders which have been analysed thoroughly in the previous sections. While it was found that the efficacy and utility of data localisation measures proposed for India to mitigate such concerns has been limited, it is highly unlikely that the policy stance would change and hence at present, data localisation will be a part of the Indian data governance framework. However, any holistic and balanced data governance framework when deciding on the 'how' and 'what' of regulating data flows must seek to strike a balance between the costs and benefits arising from the free flow of data. This is particularly applicable in the Indian context as well given that the Indian digital economy has gained significantly from the benefits of international data flows and the economic implications of localisation cannot be overlooked. The policymakers have taken cognisance of the fact that they need to balance the objectives as has been echoed in the report by the Justice BN Srikrishna Committee, where it states that

> 'It is essential to ensure that the interests of effective enforcement of the law, economic benefits to Indians need to be core to any proposed framework for cross-border transfer. However these must not unjustifiably impede international flow of personal data, which itself is beneficial in many ways for Indians.'

The question that then arises is how to strike a balance in this ecosystem of cross border data flows. The solution has been manifesting in the form of 'conditional data flow regimes' that are premised on certain preconditions relating to the safety of data and applicability of safeguards that must be fulfilled before data is allowed to flow to other countries. Several countries like Australia, China, The EU and the US have been using different mechanisms to allow the flow of data across borders while placing suitable restrictions. In the Indian context as well, provisions have been included in the draft of the Personal Data Protection Bill 2019 to facilitate a conditional flow of data across borders. Under chapter 7 titled 'Restrictions on transfer of personal data outside India' in the draft of the Personal Data Protection Bill of 2019, the conditions for transfer of **sensitive personal data** outside the territory of India (for the purpose of processing and while maintaining one live copy on an Indian server) are as follows -

5. The data may be transferred outside India where the explicit consent is given by the data principal for such a transfer and where,

6. The transfer is in accordance with a contractual agreement or intra-group scheme that has been pre-approved and certified by the proposed Data Protection Authority. Further the approval of the contractual agreement and intra group scheme shall be contingent upon them including provisions such as -
    a. Ensuring the effective protection of rights of the data principals that have been outlined in the relevant sections of the PDPB19.
    b. That the data fiduciary involved in the transfer of data to another entity will bear the liability for any non compliance with a provision/ safeguard under the contract/scheme.
7. The third approach is that of adequacy assessments and certifications for other jurisdictions. According to the text of the PDPB19, 'the Central Government after consulting the DPA may allow the free flow of data to another jurisdiction that has been approved' on the basis of its finding that -
    a. The data transferred will be subject to an adequate level of protection, with due regard to the applicable laws and international agreements.
    b. The transfer will not affect the enforceability of relevant laws by the authority with the appropriate jurisdiction.
8. Under section 34, subsection (1) clause (c) - the authority may approve the transfer of sensitive personal data for 'any specific purpose'.

While for **Critical Personal Data** that has been mandated to be processed exclusively within Indian territory, there are certain provisions that allow for its cross border transfer. They are as the followings-

4. The critical personal data may be transferred to any person or entity that is engaged in the provision of health or emergency services.
5. Where such a transfer[28] is necessary for action to fulfill conditions listed under Section 12[29] under chapter 3 that deals with the 'Processing of Personal Data without Consent'.
6. Where the transfer of such data is in accordance with the adequacy determination by the Central government as highlighted above and where such a transfer (in the opinion of the Central Government) does not affect the security and strategic interests of the country .

As we can see, the conditional flow regime is premised upon the flow of personal data being permitted only to a limited number of circumstances. An analysis of the preconditions of the clauses shows that in practice, there are 3 broad mechanisms that can be used to facilitate cross

[28] Any transfer under this clause shall be notified to the DPA within a period specified by the subsequent regulations.

[29] The provisions that allow for non consensual processing under Section 12 have been included in the Appendix.

border data flows while being in compliance with data localisation requirements. These mechanisms are

1. Model/Standard Contractual clauses (SCCs) that can be used for transfers between 2 firms in different jurisdictions.
2. Binding Corporate Rules (BCRs) that can be used by a group of companies (subsidiaries under an MNC in different countries) for transfer of data amongst them.
3. Transfers on the basis of Adequacy determinations and certifications to other jurisdictions.

Transfers after obtaining explicit consent of the data principals. One-off exceptions which permit the flow of data based on the discretion of the Central Government.

These alternatives have largely been adapted from the EU GDPR which also advocates for a conditional flow of data across borders subject to adequate levels of protection being guaranteed to the EU citizen's data. The underlying principle of approaches is that before the transfer of data to another country, an assessment must be made to ascertain if that country will be providing safeguards and adequate level of protection to the data being transferred. The 'adequacy' in practice has largely been centered on whether the levels of protection in the importing country are comparable to those offered to the data in the exporting country. Mechanisms such as SCCs and BCRs rely on the principle that the onus is placed on the entities involved in the transaction of data to ensure that an adequate/similar level of protection is accorded to the data right from its collection, transit across borders and processing in another jurisdiction. The mechanism of Adequacy decisions on other jurisdictions operates at a country wide level where countries that are deemed adequate are put on 'whitelists' and all types of data transfer are then allowed between entities in the 2 countries without any further prior authorisation. Additionally, in the adequacy decision model the onus is not on the transferor entities but instead on the Executive authorities of the countries in consultation with an expert body.

The first two approaches, that of Standard/Model Contractual clauses and Binding Corporate Rules have been advocated for by the Justice Srikrishna Committee as the primary pillars of the framework regulating cross border flows of personal data of Indian citizens. 'The entity led transfers facilitated will be the primary method for ensuring equivalent protection to Indian data flowing abroad.' (Justice Srikrishna Committee 2019) In their assessment of the adequacy determinations mechanism, the committee highlights that there are concerns regarding the lack of capacity of the Indian data regulator (the Data Protection Authority) along with the enforcement burden make it less suitable as compared to the entity led alternatives for data transfers. However, the committee also reasons that the adequacy determinations are the mechanism that allow for the role of the sovereign in permissibility of data transfers and ensuring that the data flows to only those jurisdictions that the sovereign, in its opinion has found to be providing a similar/adequate level to protection to Indian personal data. Further, the committee opined that the sovereign must play a constructive role in framing the regulatory preconditions for transfer of Indian personal data safely abroad. Thus, though there are practical difficulties revolving around capacity and administrative burden on the DPA, adequacy determinations have been included as the secondary mechanism in India's conditional flow regime.

Further, even if another country fails to get an adequate determination from the Indian government, the firms can still exercise their autonomy in making use of the contracts and the rules to continue their operations centered on data transfers. This will ensure that a harmonious balance is maintained between the mechanisms and the stakeholders (namely the central government and the data controlling entities) and also maintain the regulated flow of data across borders.

This chapter would be conducting a cost benefit analysis of the mechanisms of SCCs and BCRs with an objective to determine the efficacy of the approaches in regulating cross border data flows for India. The objective of undertaking this exercise is to highlight the key issues that arise in the practical implementation of these instruments which can serve as a reference for Indian policymakers when formulating the structure and contents of these instruments under the PDP Bill 2019.

Additionally, a case study analysis of the EU Adequacy Decisions model has been employed for analysing the adequacy assessments approach, wherein the guiding principles, steps followed and the experiences from implementing such an approach have been analysed.

10.1 Standard Contractual Clauses

Standard contractual clauses are legal instruments that are used by data fiduciaries in one country for facilitating cross border data transfers. They are in essence a model document outlining the obligations of the entities involved in the exchange of data along with other rules that will govern the flow of data. These obligations and rules that are in the form of clauses in the model document then need to be mandatorily included in all private contracts that entities in different jurisdictions may create for the exchange of data between them. (OECD 2020)

The concept of Standard Contractual Clauses was first introduced in the EU in the form of the Council of Europe Model Contracts to ensure Equivalent Data Protection in the context of Cross Border Data Flows. These clauses were revised by the EU Commission and under the Directive 95/46/EC and introduced 2 sets of Contractual clauses - Those between Data Controllers (outside the EU) and those Between Data Controllers and Data Processors. (outside the EU) The contractual clauses subsequently underwent amendments in 2004 and most recently in 2020. Since their introduction, several countries around the world have adopted the mechanism and framework introduced by the EU, albeit with minor changes to suit their particular interests and contexts.

There are 2 major categories of Standard Contractual Clauses that are commonly found in the frameworks by different countries-

1. **Data Controller to Data Controller contracts** - These contracts are used when a firm from one country acts as a Data exporter and transfers data to another form that is a Data importer who then uses/processes the data for their own objectives. Post the transfer here, the data is fully in control of the importing company.
2. **Data Controller to Data Processor contracts** - These contracts are used when a firm exports data to another firm to carry out processing activities using the data for the former. Here the importing firm only has access to data so long as they are carrying out the specific requirement based processing on behalf of the exporting firm. Common examples here include the processing of medical imaging scans by third parties, payroll administration and management of staff records by outsourced service providers.

Contents of the Model Contracts

An analysis of the contractual clauses formulated in different jurisdictions reflects the following common elements-

1. Description of the data transfer including details such as the data subjects/principals involved, categories of data, separate mention if any sensitive data (under the definition of the laws of the transferor jurisdiction) is part of the transfer, purpose of the transfer.
2. Obligations and responsibilities of the data exporter, data importer and the sub processes involved in the transfers of data.
3. The laws that will be applicable to the transfers. The country in which the data exporter is incorporated/established is the ones whose laws govern the stakeholders.

4. The particulars of what will be considered as a breach of obligations by the data importers and the situations in which the data exporter is under obligation to suspend the data transfers until rectification or terminate the contract.
5. Mechanisms for complaints by data principals, the recourse available and provisions for dispute resolution.

Obligations

Since the mechanism of SCCs is heavily dependent on the compliance of the entities involved in the exchange, it is pertinent to look at the kind of obligations that are included in these contracts to ensure that the data is subject to safeguards and adequate protection while being transferred. The **EU SCCs have been found to be the most comprehensive in outlining the obligations of the different stakeholders in cross border data transfers**. The obligations are as below-

1. **Data exporter** - The data exporter is the entity that controls and transfers data outside the territory of the country. Their obligations include -
    a. That the data transferred to the data importer is processed and used only for the reasons stipulated in the clauses and in accordance with the safeguards enumerated therein.
    b. The data exporter shall make reasonable efforts to determine if the data importer is able to satisfy the legal obligations under the clauses.
    c. The data exporters hold the primary responsibility for any data breach along the data value chain. This is due to the fact that the data subject may invoke their 'third party rights' and hold the exporter liable for any breach or harm that occurs to the data by the data exporter itself, the importer or by the subprocessor.
    d. The data exporter must ensure that the data importer and the subprocessor provide an adequate level of protection to the data transferred to them.
    e. Maintain a record of the SCCs including the subprocessing agreements that may be enacted by the data importer.
2. **Data importer** - The data importer is the entity that receives data and is engaged by the data exporters for processing data on its behalf. The obligations include-
    a. To incorporate appropriate technical and organizational measures to accord a suitable level of protection to data from unauthorized access and exploitation.

b. The data importer is liable to the data exporter for any breach of data by itself or by the subprocessor they have contracted. Additionally they are also liable in the case that they fail to provide an adequate level of protection[30] in the opinion of the data exporter's assessment.

c. The data importer must inform the exporter of any contract they form with a subprocessor. The contracts with the sub processors shall impose the same obligations as were imposed on the importer.

d. To include third party rights in their subcontracts so as to make the subprocessing entity also liable for action by the data principal in the event of a breach. They are also obligated to offer choice to the data principal for the dispute resolution which might be litigation or mediation.

e. The data importer is also obligated to inform the exporter in writing, whenever they receive a legally backed request for disclosure of data[31] by the law enforcement agencies or public authorities.[32]

f. Data Breach notifications - The importer is also mandated to submit information to the relevant authorities on incidents on any data breaches, unauthorised or accidental access to data that they have imported.

As we can see, the model contracts place a wide variety of obligations on all entities that are involved in the transfer of data. The mechanism primarily uses the principle of accountability and responsibility on the part of the firms for ensuring the protection of data. The firm that is collecting data within the country and then transferring it abroad is the one who is primarily responsible for due diligence before the data flows to another jurisdiction and even has a wide mandate of responsibilities after the data has been transferred. Thus, the accountability at all points in the data value chain are held by the exporter either directly or indirectly.

A reason for concentrating these obligations on the exporter is that they are based out of the jurisdiction of the host territory and hence directly under the mandate of the local data protection laws. On the other hand, the mandate of the data importer and the subprocessor are largely centered on maintaining transparency and timely reporting of the status of protection of data in its processing. It is by extension through the data exporter that the data importer and

[30] Here 'adequate level of protection' is a subjective term and it has been noted that it's assessment is based on its comparison with the safeguards that the data exporter is mandated to offer to the data by virtue of the data protection laws that are applicable on the data exporter.

[31] Only applicable for data that has been imported and under the control of the firm or the subprocessor contracted by them.

[32] This is done so because the law enforcement agencies will not be a party to the contract and hence won't be obligated to ensure the same safeguards as the data importer or the sub processor. This would undermine the privacy of the user data and also render the main objective of the contract - that data should enjoy the same protection across borders- will become redundant.

subprocessor have the obligation to make provisions so as to comply with the legal safeguards accorded to the data in the host country. In the Indian context, the firms importing data from India will have to make sure that the safeguards listed in the PDP Bill 2019 such as -purpose limitation, storage limitation, securing rights of the individuals - are complied with and provided to the data in the transfer.

Role of the Data Protection Authorities

When it comes to formulating the model contracts, the norm followed is that the Data Protection Authorities in these countries either frame the contractual clauses themselves or formulate the guidelines on the specific provisions that must be included in the contracts. In the case of India, the Justice Srikrishna Committee report has stated that the Indian DPA will be responsible for formulating the model contractual clauses. Additionally, the DPA in India will also be responsible for carrying out periodic audits of the data exporters to assess their data management activities and compliance. It must be noted that the EU SCCs make an explicit provision for the data importers and sub processors to also be subject to audit by the host country's regulatory body. The Indian DPA will also have the responsibility of carrying out periodic reviews of the contracts submitted to them while also updating the model contracts suitably to accommodate the changing business environment and technology processes of data transfers.

Having seen how SCCs operate and the role of different stakeholders, we now turn our attention to the benefits and costs arising from the use of SCCs for data transfers.

Benefits

1. SCCs are legally backed instruments and the growing recognition of its utility in data transfers amongst countries is propelling its adoption especially with a rise in data localisation requirements. This is so because the SCCs add certainty to the business environment while enabling the continuity of data flows and business activities while the firms comply with the localisation requirements.
2. The data is accorded an adequate level of protection at all points in the data value chain.
3. It helps in establishing a degree of compatibility between different data protection regimes even in the absence of bilateral/multilateral data sharing agreements of favourable adequacy determinations.
4. Promotes accountability on the entities involved in the transfer and transparency in the data flows.

5. They can be implemented fairly quickly at a relatively low cost compared to other alternatives. Additionally, they can be incorporated into existing commercial contracts between entities operating in different countries.
6. It allows for flexibility to introduce new clauses and arrangements/safeguards as the landscape evolves. This also permits clauses for specific data types and sectors which might have different needs.

Costs

1. In mandating the disclosure of the categories of data in the transfers the SCCs do not account for the complex nature of data. Data points are found in hybrid data sets and to ascertain which exact data points fit under what categories is a subjective and open ended exercise that can lead to ambiguity in disclosure. A consequence of this will be legal repercussions for the data exporter.
2. The volume of data that is routinely transferred between entities is also too large to be declared in SCCs separately or even accurately predicted since changing business needs also alters that kind and volume of data that is transferred.
3. The data exporter has extensive obligations to conduct a due diligence of the measures undertaken by the data importer and of the legal environment on data protection in the country where the data is being transferred. In addition to this, they have to constantly monitor the status of compliance of the importer with the contractual obligations and take suitable measures in the form of prescribing additional safeguards or in some cases suspending or terminating data flows if it finds that the data is not getting adequate safety. These have been found to be extremely cumbersome and significantly raises the legal and compliance costs for the exporter due to the reliance on third party legal consultation services even for large companies. Studies have found that SMEs and startups are likely to be severely impacted as they do not have legal expertise available in house to carry out these obligations. These costs are also recurring given that the nature of assessments is an ongoing process.
4. For companies that are complex in structure and deal with a wide variety of data, mandating SCCs may involve restructuring or renegotiating their existing commercial contracts to imbibe the data protection obligations. This will be a significant cost as even though SCCs are quick to adapt, the bulk of the costs come from negotiating and drafting the contracts between parties.
5. There are instances where the data importer will be subject to disclosure of data to the law enforcement agencies or state authorities of that country. This has been flagged as an issue since these authorities are not party to the contract and hence have no obligations regarding safeguarding the data, let alone according to the standards of the

exporting country. This has also been highlighted as a limitation of SCCs utility in ensuring safety of data in data transfers.

6. Taking note of the issues above, post the invalidation of the EU-US Privacy Shield on grounds of EU data being susceptible to US surveillance laws post export, SCCs have added clauses that call for the data exporter to insert additional safeguards to protect data from state interference. **Though there is still ambiguity regarding what these additional safeguards should be, the research has identified 2 broad prescriptions given for these-**
    a. The data exporter should in conjunction with the data importer ascertain which, if any, binding data disclosure laws the importer firm is subject to. Additionally on the question of government surveillance, the data exporter should assess the measures taken by the importing firms to prevent unauthorised surveillance.
    b. The data exporter may also include safeguards in the form of additional technical requirements such as stronger encryption for the data importer.

10.2 Binding Corporate Rules

The second mechanism advocated by the Justice Srikrishna Committee for conditional data transfers is Binding Corporate Rules. These are essentially intra-group schemes that can be adopted by a group of companies for ‘inter se’ transfer of data amongst entities within the group. (Srikrishna Committee Report 2019) In essence, a company located in India will be able to use the BCRs to transfer data to its subsidiaries in other countries even without an adequacy decision or data sharing agreement existing between the countries. The rules act as a policy for the group of companies that, similar to SCCs, outline the data security practices and protocols that must be followed while transferring data between entities. BCRs thus demonstrate that the organisation as a whole has put in place adequate safeguards to protect data as it is transferred between parts of the same organisation. (Cory et al 2020) Additionally, they also ensure compliance with the local laws and adequate protection to data prescribed by the exporting country. They are uniform in application once formulated and binding on all entities of the corporate group. (Asian Business Law Institute 2020)

Contents of Binding Corporate Rules

BCRs are formulated by the group of companies and then placed before the Data Protection Authorities to carry out an adequacy assessment of the measures and obligations adopted, laws and regulations applicable and whether the affiliates in the third country will be able to provide an adequate level of protection for data. Due to this, literature or copies on BCRs used by companies are not available in the public domain. Thus, for the purpose of this research the framework of BCRs formulated by the Article 29 Data Protection Working Party of the EU and the updated BCRs under the EU GDPR have been used as a reference in understanding the contents of the rules.

It must be noted that even under the directives issued by the Article 29 Working Party, there are no model rules that have been prescribed, instead a framework of principles and compliance have been listed, which may be incorporated into the rules formulated by companies in different documents and forms. (PwC 2018)

The following are the guiding principles for BCRs prescribed by the Article 29 WP of the EU -

1. The BCRs must include safeguards in line with the core data protection principles that the data enjoys in the home jurisdiction. In the case of India these will be purpose and storage limitation, lawful access to data amongst others.
2. The group structure must be declared including details on the entities as part of the group and covered by the BCRs.
3. The BCRs must be legally binding and governed by the law of the host country. It should also list the obligations and responsibilities of each member of the group for securing data with adequate safeguards. Some of the common obligations include data breach notifications and declaration of the security measures undertaken.
4. The entity that is located in the host country is made responsible for the acts of the other group members across jurisdictions. It is this entity that is primarily responsible and is mandated to also take corrective measures in the case of a data breach and is liable to pay compensation for such breaches that might occur under any of the members.
5. Additionally, provisions should be made for the members to demonstrate their compliance with the rules and the laws applicable by means of audits and inspections.
6. The BCRs must include provisions for establishing cooperation between the Data regulatory authorities and all the entities of the group.
7. There must be provisions regarding the handling of complaints and list the third party beneficiary rights of the data principals.

Benefits of using BCRs for data transfers

1. BCRs are of particular significance to multinational companies with several subsidiaries spread over multiple countries. Given the rise of data driven businesses, BCRs help in

the continuity in operations of data transfers while in compliance with local data localisation restrictions.

2. Post implementation the maintenance of BCRs have been found to be more streamlined as compared to model contracts as the regulatory approval is a one time requirement and only significant changes to the group structure need to be updated with the concerned Data Protection Authorities.
3. They provide a higher degree of autonomy to the group of companies in determining their rules for governing data transfers and according security to it. The groups can satisfy the principles discussed above in ways that suit their business operations as opposed to the largely rigid template of the model contracts.
4. Since the adequacy determination of the level of safety provided by the BCR entities in other jurisdictions is made by the Data regulatory authorities as opposed to the data exporter, the BCRs are considered to be more stable mechanisms. Since the regulatory authority is part of the review and approval process, it is unlikely to find instances where the authority would place restrictions on the mechanism. (Feiler and Seinen 2020)

Costs

1. BCRs have been found to be more expensive requiring a significant amount of upfront investment to be made.
2. They are also time consuming. According to a study by Allen and Overy, estimated the time taken for the finalisation and approval of a BCR to be between 11 months to 2 years. The long and unpredictable processing can be attributed to lack of resources, technical capacity or staffing at the Data Protection Authorities.
3. The transfers find utility only with multinationals and their subsidiaries in other countries owing to the resources and time that is required to get them approved. (Feiler and Seinen 2020)
4. BCRs do not allow for transfers to other corporate groups which is a practical difficulty with how modern business operate. For instance, joint ventures between different corporate houses cannot make use of BCRs for data transfers inter se.
5. The requirement for companies to formulate training programs for the employees who have access to data and are involved in its processing and having to dedicate a specialised section of the staff to liaise with the Data Protection Authorities, oversee the compliance of the firms and handling complaints have been found to be administratively cumbersome by companies.

Analysis

Having analysed the mechanisms that have been prescribed for facilitating data transfers, we now turn our attention to their adoption in the Indian context. Firstly, given the nature of the mechanisms, the large corporate groups and multinationals are more likely to make use of the BCRs as even though it incurs a significant investment, it is a one time expense and gives them greater autonomy in determining how they want to structure rules for their specific business structure while also undercutting the need for a large number of agreements. The smaller entities such as startups and SMEs are more likely to adopt the SCCs given the lack of other alternatives. Secondly, all the stakeholders will be incurring costs arising from the compliance, transparency and reporting obligations that exist in both mechanisms. The firms, both large and small will also be incurring expenses on creating capacity in house to ensure the compliance and handling the responsibilities mandated. The magnitude of these costs is in turn dependent on a number of factors such as the framing of the procedures for reporting to the DPA, the capacity that exists within the DPA to carry out its supervisory functions. Whether the DPAs prescribe a cooling off period between the enforcement of localisation and assessing compliance will also be a significant factor because post the enforcement of data localisation, a large number of firms of all sizes and from all sectors will be resorting to either of these mechanisms to maintaining continuity in their data flows thus leading to a possibility of an overburdened DPA at the start. Lastly, special attention must be paid to the role of Indian Data Protection Authority in the context of these mechanisms being implemented. As has been outlined in the sections above, the DPA will have a wide mandate of responsibilities in different roles such as framing of contracts, approving rules, conducting adequacy assessments, actively exercising supervision over the processes and the stakeholders for compliance, enforcing directives to take corrective measures and acting on complaints submitted by the data principals in the event of mishandling of data and data breaches. The Indian DPA will also be in a unique position where it can innovate new provisions that mitigate some of the costs that accompany these mechanisms such as allowing for Joint Ventures to use BCRs or allowing processors to use SCCs between them. Though these sets of responsibilities are by no means exhaustive, they demonstrate the administrative burden and technical challenges that must be addressed by suitably providing enough resources, powers and expertise through careful staffing to the Indian DPA. The exact details on the structuring of these mechanisms in India and the role of the Indian DPA in exercising its functions with respect to these data transfer mechanisms have not been notified in the PDPB 19 but the concerns highlighted serve as a reference point for what the policymakers should make provisions for pre-emptively so as to ensure a smooth facilitation of the prescribed mechanisms and a smooth transition to the localisation regime.

Thus, in the particular context of India the entity led transfers through SCCs and BCRs will be useful in the short to medium term to ensure that data flows are not disrupted with the introduction of data localisation requirements and the firms involved in the collection and transfer of data across border can continue to do so while complying with the localisation requirements by making use of these contracts. In the longer run, the policy stance is in favour of an adequacy determinations led regime that reduced the compliance and transaction cost for entities (arising out of the enforcement of obligations under the contracts) while also giving the executive a key role in ensuring the safety of data in transfers to other countries.

10.3 Adequacy decisions framework

Adequacy decisions are a tool or a mechanism that is gaining traction around the world to facilitate the cross border transfers of data in an environment increasingly characterised by more data flow restrictions and data localisation mandates. The development of this mechanism can be attributed to the fact that there was an increasing call for protecting data in cross border data flows beyond one's territory while also finding a way to ensure continuity of data flows for business purposes. Hence, adequacy decisions were first introduced by the EU under the EU Directive in the 90's and consequently updated post the introduction of the EU GDPR in 2018. Under the adequacy decisions model of data transfers, a country makes an assessment of the level of protection that another country will provide to its data if it is transferred there. In doing so, if the assessment finds that the level of protection is adequate and comparable to the safeguards that is provided to data in the first country, the second country is then given a positive adequacy decision. Based on this, data can then flow freely between the two countries without requiring any additional safeguards or authorisations from regulatory authorities or the executive. Adequacy decisions in essence help the countries to identify and greenlight other countries for permitting data transfers and ensure that the data of its citizens is protected by the standards of data protection they deem to be adequate. (McCann et al 2020)

Different countries have adopted the adequacy decisions framework with changes to suit their context. However, adequacy decision frameworks are made up of 2 broad components- what principles and criteria are used to assess the adequacy along with the procedure through which the decision will be made. (Weber 2013)

This research undertook a case study analysis of the adequacy decision frameworks of the EU to gain in depth insights on the guiding principles, procedures while ascertaining the strengths and weaknesses of the framework that would help in determining the key focus areas for policy makers for developing an Indian adequacy framework. The decision of selecting the EU model for the case study was based on the considerations that the EU pioneered the concept and has been making use of since the EU Directive of 1992 with amendments over the years upto the introduction of the EU GDPR. The EU model is also seen as the most comprehensive framework which has been the template that other countries have emulated with modifications to suit their contexts and objectives. The framework has also been applied widely and actively by the EU over the years to whitelist other jurisdictions.

Case Study - EU Adequacy Decisions Model

Guiding principles

Article 45 of the EU GDPR titled 'Transfers on the basis of adequacy decisions' is the basis for adequacy decisions and outlines the principles and procedures that must be followed by the EU while making adequacy determinations and decisions. According to the Article, the following elements form the basis for determining the adequacy of another country in providing data protection to EU data that is transferred there. Section 2 under Article 45 of the GDPR and the relevant recitals under numbers 103-105 states that 'When assessing the adequacy of the level of protection, the EU Commission, shall in particular take note of the following elements' -

a. The respect for the rule of law and regard to international standards of human rights and fundamental freedoms granted by the laws of the country.
b. General and sectoral laws on data protection with a special focus on the safeguards and security measures for data by specifying the obligations rights, recourse mechanisms and judicial redress available to the data subjects. In addition the material and personal scope of the laws is considered along with the types of data and processing activities that are allowed and what limits are placed.
c. The safeguards are in turn compared to the EU standard of data protection such as storage and purpose limitation, lawful access to data to determine their adequacy.
d. The provisions for onward transmission of data received from other jurisdictions is assessed. This is done to ensure that EU data transferred is limited to the jurisdiction that is greenlighted by the mechanism.
e. Existence and the functioning of one or more independent supervisory authorities with individual oversight and enforcement resources.
f. The laws guiding the public access to data held by companies under the country's jurisdiction and the processes and limitations placed therein.
g. The international commitments and obligations of the country arising out of its participation in multilateral and regional agreements particularly concerning the flow and protection of data.

In addition to these criteria, an analysis of the EU adequacy decisions given to other countries (which reflects the practical implementation of the adequacy decision model) shows that factors such as the relations with the other country- both political and commercial along with the extent of personal data flows and general reputation of the country on privacy and data protection matters are considered.

Procedure of Adequacy determinations

The procedure and the stakeholders involved in EU framework of adequacy decisions are as follows-

1. The European Commission which is the executive body that is responsible for proposing legislations and implementing decisions for the EU has the powers under Article 45 of the EU GDPR to make adequate determinations for data transfers to other countries. It is the primary body responsible for carrying out a detailed assessment of the country making use of the principles and practical considerations that have been listed above.
2. Post the stage of investigations, the Commission consolidates its findings and opinions/recommendations in a proposal.
3. The proposal is then sent to the European Data Protection Board (EDPB) for its opinion. The European Data Protection Board is an independent body whose mandate is to ensure the effective compliance and consistent application of the provisions of the GDPR in legislations and orders formulated by the executive bodies of the EU. It is a body made up of representatives from the Data Protection Boards from all EU countries.
    a. The EDPB must be provided with the materials, evidence and the relevant correspondence that were used by the EU Commission to arrive at the decision listed in the proposal.
    b. The EDPB is also involved in any investigation/review process or revocation regarding the adequacy decision for a third country.
4. Post the scrutiny and the approval by the EDPB (reflecting the consensus of representatives of the EU countries) the Commission can then adopt the decision and issue directives for the implementation of the decision for the other country.
5. There is also a provision in the EU where the EU parliament may request the Commission to amend or withdraw its decision accorded to a third country on te=he grounds that the act exceeds the powers provided in the regulation. [33]

[33] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

6. The Commission is also responsible for undertaking periodic assessments of the status of compliance and adequacy provided by countries that have received a favourable decision. This must be carried out every 4 years or at an earlier time due to situations like changes to the data protection laws and regulations in the third country.

Analysis of the practical implementation and use of Adequacy decisions for data transfers

The use of adequacy decisions in enabling conditional data transfers to other countries has exhibited benefits such as providing a country level assessment to be made for safeguarding data that is transferred. The country level decisions also play a role in reducing the compliance burden of firms significantly as it eliminates the need to to negotiate and implement contracts. The mechanism provides stability and creates a safe business environment that is relatively free from the risk abrupt disruption of data flows as was seen with the invalidation of the EU-US Privacy shield. The utility of the mechanism also lies in the fact that it enables the government of a country to carry out assessments and exercise their sovereign power rather than delegating it to companies who may not be able to sufficiently assess the fine points of the data protection framework of another country.

However, an analysis of the EU adequacy decisions handed out to other countries also exhibits the following drawbacks and inefficiencies that are important to take note of -

1. Despite being operational for close to 3 decades now, till date only 12 countries have obtained positive adequacy decisions by the EU. Out of the EU's top 40 trading partners as well, only 3 have obtained adequacy decisions. This sluggish uptake highlights that most countries have been able to operate without seeking adequate decisions and that firms over time have adjusted to making use of the model contractual agreements and rules for facilitating data transfers.
2. Though the guiding principles are general in nature, the requirement for adequacy essentially entails how comparable the safeguards for data in the third country are with EU standards that have been deemed to be too high. There is also a general ambiguity with the mechanism due to the interchangeable use of terms such as ‘adequate’ ‘equivalent’ and ‘similar’ in comparing the level of protection of the third country which adds to subjectivity and uncertainty.
3. The EU does not publish its negative adequacy decisions and there's also no transparency on what factors were responsible for the lack of a favourable adequacy decision. Though the principles guiding the determinations have been clearly laid down, they are not exhaustive in nature and the practical implementation documents show that political and trade relations and significance also play a role in the decisions. This is

problematic since the mechanism can become polarised by tensions in the political climate and end up acting as a trade barrier.

4. The inclusion of these additional factors has also led to the inconsistent application of the adequacy model. As an example, the EU adequacy decision published for New Zealand mentioned that concerns were expressed over the conditions for onward transfers in the country. However, a favourable adequacy decision was still granted by overlooking this gap citing that it is unlikely that large volumes of EU data will be transferred to the country due to its relatively isolated geographical location and nature of trade relations with the EU. This is a major concern since the basic guidelines for assessing adequacy were overlooked.
5. The model entails a significant administrative burden with the requirement of advanced technical capacity and legal resources for conducting a thorough assessment of the data protection frameworks of other countries. The periodic nature of assessments further add to this.

10.4 Way forward for the Indian Adequacy Decisions Framework

Using the above findings on inefficiencies of the adequacy model as a reference and taking into account that the current policy stance (as reflected in the Justice BN Srikrishna Committee report) favours the use of the adequacy decisions mechanism for India, the research recommends the following measures for the development of the Indian adequacy assessment framework-

1. The Indian model for adequacy decisions should not try to import its principles of data protection to other countries as is done by the EU in looking for an alignment between the laws of the two jurisdictions. Instead the model should determine adequacy on the basis of similarity of the substantive principles of data protection and safeguards provided by the other country instead of focusing on how similar or aligned the exact provisions in the law of the other country are with the Indian laws. This accommodates the fact that different countries may take different approaches and measures to provide a similar protection level to data.
2. The Indian PDP Bill has outlined that the Central Government in consultation with the DPA will be responsible for carrying out the adequacy determinations. Given the highly complex and technical nature of adequacy assessments, the resources of both the government department coordinating the assessment and the DPA will have to work in tandem and the exact roles and responsibilities must be notified for a smooth functioning between the two. Whether the observations/recommendations of the DPA will be binding on the Central Government is also something that must be addressed.

3. Provisions should be made to ensure that the DPA in particular is adequately staffed and has the requisite technical, legal and administrative resources to carry out its role in the determinations.
4. The process should be made transparent and in case findings suggest that a positive adequacy decision cannot be accorded to the country, a consultative channel must be engaged to take up the specific points of concerns that are limiting a favourable decision.
5. Given that the capacity to conduct these assessments will develop gradually over time, in the short and medium term, partial adequacy decisions can be made for strategic sectors such as healthcare, finance and emerging technology industries that will ensure the continuity of data flows and businesses while also reducing the compliance burden on the firms in these industries from relying on SCCs and BCRs.

11. Conclusion

Expanding and contextualising the debate on data localisation shows that even though there are legitimate concerns that manifest in the form of disadvantages faced by a country like India in an ecosystem characterized by free cross border data flows, the dominant factor that is driving localisation in India is the concept of Data Sovereignty. The research findings presented in the chapters on security and law enforcement posit that data localisation by itself has limited utility in according better security to data, improving the national security posture or enabling better access to data for Indian LEAs. On the contrary, localised storage of data increases the vulnerability of data to cyber threats by concentrating it in one geography and does not resolve the conflict of law, reduce dependency on or improve the inefficiencies of the existing mechanisms for LEA access to cross border data. However, even in light of these shortcomings, it is highly unlikely that data localisation requirements will be removed from the PDPB 19 by the Joint Parliamentary Committee studying it. This is so because the slew of recent policy proposals in different sectors and statements by the government officials and ministers clearly indicates that the priority for the Indian policy makers is to exert sovereign control over data and the changing perceptions and recognition of data as a national resource with strategic and commercial value which must be protected by storage within Indian boundaries play a pivotal role arguing in favour of retaining the data localisation requirements in the Indian data governance framework being set up by the PDPB 19. Additionally, it must be noted that data localisation, where on one hand imposes significant costs on the stakeholders and also hampers competition and innovation in the economy, has also made gains by furthering the commercial objectives of Data Sovereignty by imposing costs over the data extraction activities of the large technology corporations and imposing compliance requirements that bring them to the negotiating table, as has been the norm with several closed door representations have been made by the Big Tech firms to the JPC to lobby for a dilution in localisation requirements. This must be taken note of as one of the key concerns to the sovereign authorities of modern governments is the unchecked power and influence of such big tech firms, which is where localisation now acts as a lever of some control over their activities. The localisation requirements have also compelled the large technology companies to invest in building local data storage infrastructure that has brought in significant investments and technology transfer gains for the Indian data centre markets still in their nascent stages. Thus, going forward, data localisation will be implemented as a means to achieve Data Sovereignty but must be augmented with additional policy measures that fill the gaps in achieving the stated objectives, since the objectives are valid and present a policy challenge to be addressed, but where data localisation by itself exhibits limited utility and falls short of fulfilling them.

12. Policy Recommendations

This section consolidates and presents the policy recommendations proposed by this study to augment the current data localisation framework for India.

1. The Ministry of Electronic and Information Technology, Government of India which is the nodal agency for the implementation of the PDPB must notify the exact types of data that fall under the categories of Sensitive Personal Data and Critical Personal Data. Doing so will clarify the scope of the bill and will also act more certainty to the business landscape that can then plan the steps to be taken for compliance.
2. **On the conflict of jurisdiction** - The Joint Parliamentary Committee studying the Bill should consider expanding the scope of the PDPB 19 by including a provision that extends its application on the basis of nationality of the data subject and not just on the principle of territoriality that reflects in the current provisions for scope and applicability of the Bill. This will ensure that the safeguards are provided to data of all Indian citizens by virtue of their nationality and not limited to data that is collected or processed within India. This will also accord a stronger position to Indian courts in questions on conflict of law where the nationality of the Indian data subject can be quoted to assert jurisdiction over the data regardless of where they are and where their data was collected.
3. **On Law Enforcement Access to Data** -The issue of access to data by Indian LEAs lies in the structural inefficiencies of the existing mechanisms such as MLATSs and the shortfalls in the internal capacity of the LEAs. Hence, internally, reforms are required in order to bridge the gaps in capacity and optimise the mechanism of MLATs -
    a. **Internal capacity reforms**
        i. The MHA can review the legal and technical requirements of all the countries with which India holds MLATs and then issue a model template for filing requests for each of these countries. This will ensure that the Indian LEAs have ready reference documents to refer to which will help them put together the necessary documents required by the other country for facilitating the request.
        ii. The technical capacity of the officers involved in the process must be improved through training. This should operate at the level of the MHA since it is the designated coordinating body, the central LEAs such as NIA, CBI, ED and the state police officers who file such requests while investigating crimes. Adequate allocation of resources both financial and

to ramp up administrative capacity must be made by the MHA for this purpose.

iii. State level coordinators must be designated by the MHA who can then coordinate the establishment of specialised departments in the state police with the requisite technical and cyber legal expertise. For this the Indian policy makers can emulate the role played by the IPCC of the CBI for LR requests. The coordinator and the department can then advise the state police officers in framing the MLAT requests and coordinating its approval with the MHA. This is to ensure that between the formulation of the request by the state investigators and the review by the MHA, a layer of expertise is present which irons out the shortcomings and speeds up the process.

b. Structural reforms to MLATs

i. **Stipulating time bound action** - One of the most pressing issues has been the cumbersome time consuming determinations which is further exacerbated by the number of stakeholders involved in the vetting process. It is recommended that for India, the Central Government should, after a comprehensive review, mandate the time period within which each stakeholder must follow through on their scrutiny and submit the status. This is to ensure a time bound process within India.

ii. **Digitising the process -** The current practice is for the state police investigators to post their requests to the IS-II division at the MHA which also responds with their observations on paper. This is an extremely time consuming process and also adds uncertainty on the part of the investigators as they have to channel their queries through written requests. The MHA should set up a centralised secure portal online and digitise the process of receiving requests from the LEAs. The portal can also display the status of the request based on the action that has been taken within the MHA. This will not only optimise the process but also make it more transparent and accountable.

iii. Taking the digitisation idea forward, the MHA should initiate discussions with the coordinating agencies of other countries to shift to a secure digitised channel for communications instead of relying on the paper trail which is the norm at present.

iv. **Establish consultative channels -** There must be a channel where the central authorities from the two countries can discuss their concerns and take the opinion in case any MLAT requests are found to be deficient instead of rejecting the requests that delays the overall process further. Experts have argued in favour of making provisions for a ‘cyber legal attache’ in the diplomatic missions to handle bilateral data sharing requests for law enforcement purposes. This would be along the lines of the office of a Defence Attache which has a specific mandate for defence cooperation between the countries. A specialised office such as this can also play a constructive role in expediting the process.

4. In the long term, India should focus on establishing direct data sharing agreements at the executive level with other countries and regional groupings. The executive level agreements will help towards establishing a coherent framework for data sharing which is built upon a set of agreed upon principles and safeguards and increase the speed and scope of accessing data across borders for the Indian LEAs.
5. **On Costs imposed on businesses** - Given that the compliance costs will accompany the localisation policy, the government can make the transition smoother by prescribing a suitable cooling off period after due consultation with all players within which the compliance and shift can take place. Doing so will serve a dual purpose of ensuring an amicable time bound compliance with the requirements while also removing uncertainty of penalties on the firms if their compliance status is arbitrarily scrutinised.
6. **On checking the monopolistic practices of Big Tech in the markets**-
   a. In order to effectively address the issue of market concentration of data and correct the imbalances, policies to incentivise data sharing amongst firms can be considered rather than taking a heavy handed approach of forcing them to.
   b. To holistically address concerns of imbalance between firms in the digital markets, the competition policy must be updated in order to respond proactively to the anti competitive behaviour centered on data. This takes into consideration that competition in the digital markets operates differently from the traditional markets in the offline world. Anti competitive behaviour is also exhibited in other ways by hostile takeovers and acquisitions of startups by large technology corporations, offering services for free owing to the network effects that discourages startups or manipulating consumer choice by favouring a few products and firms on the platform
7. **On promoting Innovation** - This paper recommends 2 approaches that may be considered to balance data localisation with the development of emerging technologies in India-

a. The government should consult the industry bodies and players engaged in the development of the technologies to gain a more holistic understanding of their requirements for cross border data flows. Based on this, some relaxations on restrictions may be considered for these industries.

b. The second approach that the government can take is to use partial adequacy decisions to enable the movement of cross border flows of data between specific industries in countries. Partial adequacy decisions are used to facilitate cross border movement of data for specific purposes between countries. For instance, the UK has given a partial adequacy decision to the US for the healthcare sector where firms in both countries can freely transmit healthcare data between them and make use of resources provided by service providers of the other country. A similar partial adequacy decision may be considered for the AI and IoT industries in India and the US that will enable the use of computing power and access to sophisticated AI development platforms provided by US based firms.

8. **On the conditional data flow mechanisms -**

   a. An appropriate cooling off period must be provided for the businesses to operationalise and implement SCCs and BCRs rather than mandating a strict compliance from the onset of the Act.

   b. **Standard Contractual Clauses** - Processor to Processor data transfers must be permitted using SCCs.

      i. Given that startups in India will be primarily dependent on SCCs out of the two short term mechanisms, appropriate financial incentives must be provided to enable them to comply with the restrictions while remaining operational. These incentives can be a part of the wide range of offerings under the Startup India Scheme.

   c. **Binding Corporate Rules** - Joint Ventures must be allowed to use BCRs for transfer of data between separate business entities that belong to the same venture.

   d. **The Adequacy Decisions model** -

      i. The Indian model for adequacy decisions should not try to import its principles of data protection to other countries as is done by the EU in looking for an alignment between the laws of the two jurisdictions. Instead the model should determine adequacy on the basis of similarity of the substantive principles of data protection and safeguards provided by the other country instead of focusing on how similar or aligned the exact provisions in the law of the other country are with the Indian laws.

This accommodates the fact that different countries may take different approaches and measures to provide a similar protection level to data.

ii. Given the highly complex and technical nature of adequacy assessments, the resources of both the government department coordinating the assessment and the DPA will have to work in tandem and the exact roles and responsibilities must be notified for a smooth functioning between the two. Whether the observations/recommendations of the DPA will be binding on the Central Government is also something that must be addressed.

iii. Provisions should be made to ensure that the DPA in particular is adequately staffed and has the requisite technical, legal and administrative resources to carry out its role in the determinations.

iv. The process should be made transparent and in case findings suggest that a positive adequacy decision cannot be accorded to the country, a consultative channel must be engaged to take up the specific points of concerns that are limiting a favourable decision.

v. Given that the capacity to conduct these assessments will develop gradually over time, in the short and medium term, partial adequacy decisions can be made for strategic sectors such as healthcare, finance and emerging technology industries that will ensure the continuity of data flows and businesses while also reducing the compliance burden on the firms in these industries from relying on SCCs and BCRs.

Appendix

Interview Guide

1. Has the Indian stance on Data Flows become more protectionist in your opinion?
2. Given that India has been a beneficiary of the liberal data flows regime, what factors are driving the agenda to now regulate and limit data flows by localised storage?
3. What have been the key factors behind the emergence of the Data Sovereignty ideology in India that reflects in the latest data governance policy proposals?
4. What are the national security concerns arising out of free cross border data flows?
    a. Follow up - What has India’s experience been?
5. Does data localisation reduce the dependency on undersea cable infrastructure?
6. Does data localisation improve the cybersecurity environment provided to data?
7. Between centralised storage and decentralized storage over cloud networks, which method is more preferable to secure data?
8. Does localised storage of data reduce the risks of foreign surveillance by other countries and organisations on Indian data?
9. What are the challenges faced by Indian law enforcement agencies when trying to access data stored abroad?
10. What are the existing approaches to exercise jurisdiction in cyberspace?
11. Does data localisation resolve the conflict of law question that arises from a free flow of data across the servers spread across the world?
12. In your opinion, is a data nationality centered approach to extending jurisdiction better than the present territorial approach of the Indian PDPB 19.
13. What are the gaps and inefficiencies that exist in the current mechanisms to facilitate access to cross border data by Indian law enforcement agencies?
14. Does data localisation reduce the dependency on mechanisms such as MLATs and Direct data requests to Cloud Service Providers by storing data locally?
15. How does data localisation impact India’s digital trade prospects?
16. In what form are the compliance costs of data localisation likely to manifest?
17. Proponents of data localisation argue that it enables better access to data for domestic firms, but given that even if it is localised it will still be their proprietary data and under their control. What are your thoughts on this?
18. How feasible is data mapping for different kinds of organisations for compliance purposes?
19. What are your thoughts on a marketplace for personal data in India?

20. Will data localisation play a role in reducing market data monopolies of Big Tech firms and spur competition?
21. What are the impacts of regulating data flows on the growth of innovation?
22. Given that technologies such as Blockchain and IoT are decentralised in nature and make use of resources spread across countries for optimised operations, how will data localisation impact their growth?
23. Experts have argued in favour of localising data to develop an AI economy citing the example of the US and China where they control massive amounts of data. Is volume of data the principal determining factor behind the growth of an AI economy?
24. Are data sets that combine diverse information more valuable for training algorithms than data from a particular geography?
25. Will AI algorithms trained on Indian data have limited utility in application?

References

Aaranson, Susan. 2019. 'Data is a development issue'. *CIGI papers* 223.

Albright Stonebridge Group. 2015. 'Data Localisation : A challenge to global commerce and the free flow of information.'

Asian Business Law Institute. 2020. 'Transferring Personal Data in Asia : A path to legal certainty and regional convergence.'

Bauer, Matthias et al. 2016. 'Tracing the economic impacts of regulations on the free flow of data and data localisation'. *Global Commission on Internet Governance paper series.* 30. pp. 2-14.

Basu, Arindrajit et al. 2019. 'The Localisation gambit : Unpacking policy measures for Sovereign control of data in India'. *Centre for Internet and Society working paper series.*

Burman, Anirudh and Upasana Sharma. 2021. 'How would Data Localisation Benefit India?'. *Carnegie India working paper series*. Pp. 7-24.

Burman, Anirudh. 2020. 'Will India's Proposed Data Protection Law Protect Privacy and Promote Growth'. *Carnegie India working paper series*. pp. 16-28.

Casalini, Francesca and Javier Lopez Gonzalez. 2019. 'Trade and Cross Border Data Flows'. *OECD Trade Policy Papers*. 220.

Chander, Anupam and Uyen P Le. 2014. 'Breaking the Web : Data localisation vs the Global internet'. *UC Davis Legal Studies Research Paper series*. 2014-1 (378). pp- 28-42.

Cory, Nigel., Ellysse Dick and Daniel Castro. 2020. 'The Role and Value of Standard Contractual Clauses in EU-US Digital Trade'. *Information Technology and Innovation Foundation Working Paper.*

Cory, Nigel. 2017. 'Cross Border Data Flows : What are the barriers, and what do they cost?'. *Information Technology and Information Foundation working paper.*

Cory, Nigel. 2020. 'The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade'. *Information Technology and Innovation Foundation working paper.*

CUTS. 2020. *Data Localisation : India's Double edged sword?.* CUTS international : Jaipur.

Daskal, Jennifer. 2016. 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues'. *Journal of National Security Law and Policy*. 8 (3).

Duggal, Pavan. 2019. 'Data Localisation : A review of proposed data localisation legislation in India with learnings for the United States'. *Data Catalyst policy brief.*

French, C., Brad Carr and Clay Lowery. 2020. 'Data Localization : Costs, Tradeoffs and Impacts across the Economy'. Washington DC : Institute for International Finance.

Ferracane, Martina and Erik Van der Marel. 2018. 'Do Data Policy restrictions inhibit trade in services?'. European Centre for International Political Economy.

Future Agenda. 2018. ‘ Data localisation’. *Delivering value through data paper series.*

Goenka, Vinit. 2019. *Data Sovereignty : The Pursuit for Supremacy*. New Delhi: Penman Books.

GSMA. 2018. *Cross Border Data Flows : Realising the benefits and removing barriers*. London.

Hicks, Jacqueline. 2019. ‘Digital colonialism’: Why countries like India want to take control of data from Big Tech’. (https://theprint.in/tech/digital-colonialism-why-countries-like-india-want-to-take-control-of-data-from-big-tech/298217/) (posted on 29th September 2019) (accessed on 24th December 2020)

Hoglund, William. 2018. ‘Exporting data protection law : The extraterritorial reach of the EU GDPR’. Umea University.

International Institute for Finance. 2019. *Data Flows across borders : Overcoming data localisation requirements.*

Joshi, Divij. 2020. ‘Interrogating India’s Quest for Data Sovereignty’. *Seminar India.* 731.

Kathuria, Rajat et al. 2019. ‘Economic implications of Cross Border Data Flows’. *ICRIER and IAMAI working paper.*

Komaitis, Konstantinos. 2017. ‘The wicked problem of data localisation’. *Journal of Cyber Policy.* 2373-8898. pp- 3-12.

Kovacs, Anja and Nayantara Ranganathan. 2019. ‘Data Sovereignty of whom? Limits and suitability of sovereignty frameworks for data in India’. *Data Governance Network Working Paper Series*. 3.

Kuner, Christopher. 2011. ‘Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future’. *OECD Digital Economy Papers*. 187 :pp. 14-25.

Kuner, Christopher. 2015. ‘Data Nationalism and its discontents’. *Emory Law Journal Online*. 64 (2089).

Lessig, Lawrence. 2006. *Code 2.0*. New York : Basic Books Publishers.

Martin, Nicholas et al. 2019. ‘How Data Protection Regulation affects startup innovation’. *Information Systems Frontier*. 21:1307.

Mattoo, Aditya and Joshu P Meltzer. 2018. ‘International Data Flows and Privacy : The Conflict and its Resolution’. *The World Bank Policy Research Working Paper*. 8431.

McCann, Duncan, Oliver Patel and Javier Ruiz.2020. ‘The costs of Data inadequacy’. UCL European Institute.

McKinsey Global Institute. 2016. *Digital Globalisation : The New Era of Global Flows*.

Meltzer, Joshua. 2020. ‘Cybersecurity, Digital Trade and data flows’. *Brookings Global Economy and Development Working Paper*. No. 132. Pp. 12-30.

Ministry of Electronics and Information Technology, Government of India. 2019. 'The Personal Data Protection Bill 2019'.
(http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)
(accessed on 10th January 2021)

Ministry of Electronics and Information Technology, Government of India. 2018. 'A Free and Fair Digital Economy : Protecting Privacy, Empowering Indians'. Committee of Experts under the Chairmanship of Justice BN Srikrishna. (https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf) (accessed on 10th October 2020)

Mitchell, Andrew and Neha Mishra. 2019. 'Regulating Cross Border Data Flows in a Data Driven World : How WTO Law can contribute'. *International Journal of Economic Law.* 22(3).

Mohanty, Bedavyasa and Madhulika Srikumar. 2017. 'Hitting Refresh : Making India US Data Sharing work'. *ORF Special Report*. 39.

Molinuevo, Martin and Simon Gaillard. 2018. 'Trade, Cross Border data and the next Regulatory Frontier : Law enforcement and data localisation requirements'. *World Bank Group MTI practice notes.* 3.

NITI AAYOG. 2018. 'National Strategy for Artificial Intelligence'. Discussion Paper. https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf (Accessed on 15th February 2021)

OECD. 2020. *Mapping Approaches to Data and Data Flows*. Saudi Arabia.

Omidyar Network. 2020. *Unchecked Power : The root of Big Tech issues.*

Pai, Siddharth. 2020. 'Data Nationalism could hobble the world's progress'. (https://www.livemint.com/opinion/columns/data-nationalism-could-hobble-the-world-s-progress-11595259439395.html) (posted on 20th July 2020) (accessed on 10th January 2021)

Parmar, Sushma Devi. 2015. 'Cybersecurity in India : An evolving concern for National Security'. Central University of Gujarat.

Parsheera, Smriti and Prateek Jha. 2020. 'Cross Border Data Access for Law Enforcement : What are India's strategic options?'. *Carnegie India working paper.* pp - 5-15.

Pepper, Roberts, John Garrity and Connie LaSalle. 2016. 'Cross Border Data Flows, Innovation and Economic Growth'. *The Global Information Technology Report.* Pp. 1-9.

Pisa, Michael and John Polcari. 2019. 'Governing Big Tech's pursuit of the Next Billion Users'. *Centre for Global Development Policy Paper* 138.

Rizvi, Kazim, Rohan Seth and Madhav Sharma. 2018. 'Data Localization in a Globalised world : An Indian Perspective.' New Delhi : The Dialogue.

Sargsyan, Tatevik. 2016. 'Data Localisation and the Role of Infrastructure for Surveillance, Privacy and Security'. *International Journal of Communication*. 10 (2221-2237).

Shah, Reema. 2015. 'Law Enforcement and Data Privacy : A forward looking approach'. *The Yale Law Journal.* 125(3).

Shipley, Carrie. 1984. ‘Transborder Data Flows in the Developing World : A Question of Balance’. *Journal of Applied Communications*. 67 (4). pp.15-25.

Srikumar, Madhulika et al. 2019. ‘India US data sharing for law enforcement : Blueprint for reforms’. *Cross Border requests for Data Project by Georgia Tech Institute.*

Singh, Parminder. 2018. ‘Data localisation : A matter of rule of law and economic development’. *IT for Change Policy Brief.*

Sinha, Amber et al. 2018. ‘Cross Border Data Sharing : A study in processes, content and capacity’. *Centre for Internet and Society Working Paper*. Pp. 22-34.

Taylor, Richard. 2020. ‘Data localisation : The internet in the balance’. *Telecommunications policy.* 44. pp. 6-9.

Tehrani, Pardis. 2018. ‘Cross border data transfer: Complexity of adequate protection and its exceptions’. *Computer Law and Security Review*. 34.

United Nations Conference on Trade and Development. 2016. *Data Protection Regulations and International Data Flows : Implications for Trade and Development*. New York : United Nations Publishing. pp.- 8-37.

United Nations Conference on Trade and Development. 2019. *Digital Economy Report 2019-Value Creation and Capture : Implications for Developing countries*. New York : United Nations Publishing. pp. 84-95.

U.S Chamber of Commerce and Hunton and Williams LLP. 2014. ‘Business without Borders : The importance of Cross Border Data Transfers to Global Prosperity’. Washington DC.

Velasco, Cristos., Anna Maria Osula and Julia Hornle. 2016. ‘Global Views on Internet Jurisdiction and TransBorder Access’. *New Journal of European Criminal Law*.

World Economic Forum. 2020. *A Roadmap for Cross Border Data Flows : Future Proofing Readiness and Cooperation in the New Data Economy.* Switzerland.

Woods, Andrew. 2018. ‘Litigating Data Sovereignty’. *The Yale Law Journal*. 128(328).